



“Access denied”? Barriers for staff accessing,
using and sharing published information online
within the National Health Service (NHS) in
England: technology, risk, culture,
policy and practice

Catherine Mary Ebenezer

Submitted in partial fulfilment of the requirements

for the degree of Doctor of Philosophy

Information School, University of Sheffield

November 2017

Abstract

The overall aim of the study was to investigate barriers to online professional information seeking, use and sharing occurring within the NHS in England, their possible effects (upon education, working practices, working lives and clinical and organisational effectiveness), and possible explanatory or causative factors.

The investigation adopted a qualitative case study approach, using semi-structured interviews and documentary analysis as its methods, with three NHS Trusts of different types (acute - district general hospital, mental health / community, acute – teaching) as the nested sites of data collection. It aimed to be both exploratory and explanatory. A stratified sample of participants, including representatives of professions whose perspectives were deemed to be relevant, and clinicians with educational or staff development responsibilities, was recruited for each Trust. Three non-Trust specialists (the product manager of a secure web gateway vendor, an academic e-learning specialist, and the senior manager at NICE responsible for the NHS Evidence electronic content and web platform) were also interviewed. Policy documents, statistics, strategies, reports and quality accounts for the Trusts were obtained via public websites, from participants or via Freedom of Information requests. Thematic analysis following the approach of Braun and Clarke (2006) was adopted as the analytic method for both interviews and documents. The key themes of the results that emerged are presented: barriers to accessing and using information, education and training, professional cultures and norms, information governance and security, and communications policy.

The findings are discussed under three main headings: power, culture, trust and risk in information security; use and regulation of Web 2.0 and social media, and the system of professions. It became evident that the roots of problems with access to and use of such information lay deep within the culture and organisational characteristics of the NHS and its use of IT. A possible model is presented to explain the interaction of the various technical and organisational factors that were identified as relevant. A number of policy recommendations are put forward to improve access to published information at Trust level, as well as recommendations for further research.

Acknowledgments

This research was supported by a University of Sheffield Faculty Scholarship.

I am hugely grateful to my supervisors Professors Peter Bath and Stephen Pinfield, for their expertise, patience and support. I owe considerable thanks also to Drs Barbara Sen and Paula Roberts for their specialist input, support and encouragement, to Christine Ellis of CHE Secretarial Services for her fast and accurate transcribing of recorded interviews, to the university library staff who have rapidly and efficiently processed my numerous document supply requests, to Dr Christina Silver of the University of Surrey whose NVivo workshop I attended, and to Matt Jones for his diligent and efficient administration throughout my time at the Information School.

I am bound to mention my partner Dr Janette Allotey, retired within the last few years from her work as Lecturer in Midwifery at the University of Manchester. She strongly encouraged me initially to undertake a PhD, and has been there for me in the bad patches, where I have benefited from her own experiences both as a student and as a supervisor. Also she has uncomplainingly borne far more than her fair share of work in cooking, shopping and maintaining our house and garden, enabling me to give the time required to the thesis.

I am indebted also to the many interview participants who gave up their time, to the librarians at Trusts T1 and T3 who assisted in arranging interviews, to the professional associates and former colleagues, Linda Mace-Michalik, Helga Perry, Tricia Wells, Rachel Steele and John Blenkinsopp, who corresponded with me and provided me with feedback on early drafts, and to Dr Sarah Hargreaves, who provided me with invaluable guidance on viva preparation. I am grateful in particular to Alan Ryan of NHS England for inviting me to participate in the NHS Technology Enhanced Learning Hub project; to Dr Hazel Roddam of the Allied Health Research Unit at the University of Central Lancashire, for her invitation to present my findings at a meeting of the Cumbria and Lancashire Allied Health Professionals Research Network; and to the research coordinator at Trust T3 for inviting me to present my findings at a local research meeting, thereby putting me in contact with an e-learning specialist who became a key informant (T4-22).

Finally I must mention the non-human members of the household: our cat Ziggy ("Zigzags") for his companionship while I was analysing data and writing, and our lurcher Marcus ("Mr Hound") for our daily walks in the nearby fields, which provided me with much-needed exercise and diversion.

Table of contents

Title page	1
Abstract	2
Acknowledgements	4
Table of contents	6
List of figures	14
List of tables	15
Glossary of abbreviations and acronyms.....	16
Publications	20
Chapter 1. Introduction.....	21
1.1 Structure	21
1.2 The research problem.....	21
1.3 Rationale and motivation for the research	22
1.4 Background and context	23
1.4.1 Overall structure and operation of the NHS	23
1.4.2 Policy drivers for access to published information	27
1.4.3 NHS IT strategies and developments	28
1.4.4 Information governance and security in the NHS	31
1.4.5 NHS libraries and e-library initiatives.....	36
1.4.6 NHS e-learning developments	40
1.4.7 Health informatics professions	43
1.5 Aims and objectives of the research	45
1.6 Research questions	46
1.7 Possible outcomes/benefits of the study	47
1.8 Structure of the thesis	48
1.9 Summary and conclusion	48
Chapter 2. Literature review	49
2.1 Introduction	49
2.2 Search strategy	49
2.3 Scope and limits of the review	50
2.4 Information behaviour	53
2.4.1 Introduction and terminology	53
2.4.2 Theories of information behaviour	56
2.4.3 Multi-professional studies	58
2.4.4 Studies of doctors	59
2.4.5 Studies of nurses	64
2.4.6 Studies of health service managers	67
2.4.7 Summary and synthesis	69

2.5 Organisational cultures and subcultures	70
2.5.1 Theories of organisational culture	70
2.5.2 Occupational cultures and subcultures	70
2.5.3 Information technology staff subculture and attitudes	71
2.5.4 Inter-professional conflicts: professional jurisdiction	72
2.5.5 The NHS as an organisation	74
2.5.5.1 Introduction	74
2.5.5.2 Public distrust, risk and regulation	76
2.5.5.3 Staff engagement, organisational values and organisational trust	77
2.5.6 Theories of organisational power	81
2.5.6.1 Kanter's theory of structural power and empowerment	81
2.5.6.2 Clegg's circuits of power theory	83
2.5.7 Summary	86
2.6 Information security and cybersecurity threats	87
2.6.1 Definitions	87
2.6.2 Web-based cybersecurity threats	89
2.6.3 User behaviour and web-based cybersecurity threats	93
2.6.4 Web-based cybersecurity threats: counter-measures	97
2.7 Risk in information security and cybersecurity	101
2.7.1 Theories of risk; factors influencing risk assessment	101
2.7.2 Risk assessment, risk management and organisational trust in information security	107
2.7.2.1 Introduction	107
2.7.2.2 What constitutes risk management in cybersecurity / information security?	108
2.7.2.3 Assessment and analysis of cybersecurity / information security risks	110
2.7.2.4 Characteristics of cybersecurity / information security risk perception and decision-making	111
2.7.2.4.1 IT professionals	111
2.7.2.4.2 End-users	115
2.7.3 Measures against inappropriate web use	117
2.7.3.1 The problem	117
2.7.3.2 Measures against inappropriate web use: deterrence	118
2.7.3.2.1 Acceptable use policies	118
2.7.3.2.2 Security education, training and awareness	120
2.7.3.3 Measures against inappropriate web use: detection	121
2.7.3.4 Measures against inappropriate web use: prevention	122

2.7.3.4.1 Web filtering: technologies	122
2.7.3.4.2 Web filtering technologies: impacts upon information seeking	125
2.7.4 Summary and synthesis	129
2.8 Diffusion of innovations	131
2.8.1 Rogers' theory of diffusion of innovations	131
2.8.2 Innovation and risk	136
2.8.3 IT consumerisation	137
2.8.4 IT and organisational culture: IT-culture conflict	138
2.8.5 Diffusion of information technology innovations within the NHS	129
2.8.6 Summary and synthesis.....	143
2.9 Overall summary	143
Chapter 3. Methodology and methods	147
3.1 Introduction	147
3.2 Methodology / philosophy of social science	147
3.2.1 Introduction	147
3.2.2 Positivism	149
3.2.3 Interpretivism	150
3.2.4 Critical theory	152
3.2.5 Critical realism	154
3.3 Research approach and design	160
3.4 Research process overview	165
3.5 Data collection	165
3.5.1 Interviews: introduction	166
3.5.2 Interview questions	168
3.5.3 Interview piloting	171
3.5.4 Interviewee sampling and recruitment	172
3.5.5 Interviewing style and approach	175
3.5.6 Conduct of interviews.....	176
3.5.7 Recording and transcription of interviews	176
3.5.8 Documents.....	178
3.6 Data analysis	179
3.7 Interpretation and explanation of findings	181
3.8 Specific quality issues.....	181
3.8.1 Introduction: quality and validity in qualitative research.....	181
3.8.2 Number of interviews conducted	181
3.8.3 Audit trail	182
3.8.4 Member checking	182
3.8.5 Triangulation	183
3.9 Position of the researcher.....	183
3.10 Ethics	185

3.11 How results are reported:	186
3.11.1 Preliminaries	186
3.11.2 Structure	188
3.12 Summary	190
Chapter 4. Findings: background and organisational context	191
4.1 General information about the Trusts	191
4.1.1 Introduction	191
4.1.2 Policy and regulatory environment	193
4.1.2.1 National events and policy initiatives	193
4.1.2.2 Organisational performance	195
4.2 Information resources	196
4.2.1 Introduction	196
4.2.2 Library services	196
4.2.3 Intranets	199
4.2.4 Business intelligence services	200
4.2.5 MIDatabank	201
4.3 Education and training	201
4.3.1 Education and training priorities	201
4.3.2 Academic and research links.....	202
4.4 Trust IT services	203
4.4.1 Strategic and operational priorities	203
4.4.2 Outsourcing	206
4.4.3 Internet connectivity and wireless networks	206
4.4.4 Secure web gateways	207
4.5 Information governance	209
4.5.1 Information governance structures	209
4.5.2 Information governance working relationships	212
4.5.3 Sources of professional information and guidance	215
4.5.4 Decision making, tasks and priorities	216
4.5.5 Internal and external assessments	222
4.6 Summary	223
Chapter 5. Findings: barriers to information seeking, use and sharing.....	224
5.1. Introduction	224
5.2 Trust IT infrastructures and their management	226
5.2.1 The requirement to use encrypted portable media and devices	227
5.2.2 Network access, availability and performance	228
5.2.2.1 Authentication and access management	228
5.2.2.2 Remote access	229

5.2.2.3 Access to systems across organisational network boundaries	229
5.2.3 “Legacy” software	230
5.2.4 System policies and permissions	230
5.2.5 Availability of PCs in clinical areas	231
5.2.6 Access to approved storage	232
5.2.7 Email	232
5.2.7.1 Webmail	232
5.2.7.2 Email attachments	233
5.2.7.3 Spam filter and data loss prevention false positives	234
5.3 Published information resources	235
5.4 E-learning	239
5.5 Web 2.0 and social media	239
5.6 Mobile devices	240
5.7 Summary	242
Chapter 6. Findings: education and training arrangements.....	246
6.1. Introduction	246
6.2 IT infrastructure	246
6.3 Published information resources	252
6.4 E-learning	253
6.4.1 Drivers for the growth of e-learning	253
6.4.2 Timeline and development of e-learning within each Trust	253
6.4.3 Scope and utilisation of e-learning	254
6.4.4 Learning management systems	255
6.4.5 Non-technical problems with e-learning	255
6.5 Web 2.0 and social media	256
6.6 Mobile devices	257
6.7 Summary	259
Chapter 7. Findings: organisational dynamics and professional cultures	261
7.1 Introduction	261
7.2 IT infrastructure	261
7.2.1 IT strategies	261
7.2.2 Procurement of hardware	262
7.2.3 Organisational interface with IT departments	263
7.2.3.2 Introduction.....	263
7.2.3.2 Perceived technical adequacy and scope	264
7.2.3.3 Perceived accessibility and usability	264
7.2.3.4 Timeliness of response	265
7.2.3.5 IT department resources	265
7.2.3.6 Perceived quality of communications	266
7.2.3.7 Perceived alignment with service business needs and priorities	266
7.2.3.8 Perceived cultures and attitudes	266

7.2.3.9 Overall perceived quality of service	269
7.3 Published information resources	269
7.4 E-learning	274
7.4.1 Cultural and behavioural attitudes relating to use of IT	274
7.4.2 Staff attitudes to e-learning	276
7.5 Web 2.0 and social media	277
7.6 Mobile devices	279
7.7 Summary	283
Chapter 8. Findings: information governance and security	283
8.1 Introduction	285
8.2 Acceptable use policies	285
8.3 Monitoring	289
8.4 Endpoint security	291
8.5 Access to published resources	291
8.5.1 Frequency / extent of website blocking experienced	291
8.5.2 What was blocked?	293
8.5.3 Responses to encountering blocked websites	296
8.5.4 Effects of website blocking	300
8.5.5 Awareness of national measures	302
8.6 Information governance and education	303
8.7 Use of mobile devices	304
8.8 Summary	304
Chapter 9: Findings: Web 2.0 and social media	307
9.1 Introduction	307
9.2 Web 2.0 and social media	307
9.2.1 Social media policy in relation to media strategies	307
9.2.2 Blocking of Web 2.0 and social media applications.....	313
9.2.3 Staff perceptions of Web 2.0 / social media use and related policies.....	313
9.2.4 Corporate uses of Web 2.0 and social media	318
9.2.4.1 Drivers	318
9.2.4.2 Patterns of Web 2.0 and social media use	320
9.3 Mobile devices	321
9.4 Summary.....	322
Chapter 10. Findings: synthesis of results by Trust.....	324
10.1 T1.....	324
10.2 T3.....	349
10.3 T4.....	350

Chapter 11. Discussion and interpretation.....	354
11.1 Introduction	354
11.2 Proposed theoretical model	356
11.3 Power, culture, trust and risk in information security	358
11.3.1 Introduction	358
11.3.2 Blocking of websites	359
11.3.3 Mandatory use of encrypted portable media	368
11.3.4 Empowerment, engagement and access to information	370
11.3.5 Information security / governance risk	371
11.3.6 Impact of information governance / information security incidents	373
11.4 Approaches to innovation	373
11.5 Professional jurisdictions, professional projects	378
11.6 Summary	382
Chapter 12. Conclusion and recommendations	382
12.1 Introduction	382
12.2 Overall conclusions	382
12.3 Extent to which overall research aim has been met.....	384
12.4 Extent to which the research objectives have been met	385
12.5 Limitations of the study	387
12.6 Contribution to new knowledge	389
12.7 Recommendations for further research	391
12.8 Recommendations for practice.....	394
12.9 Conclusion	397
References	401
Appendices	483
Appendix A: Main search statements	484
Appendix B: Information behaviour of health care staff.....	490
Appendix C: Studies of other groups of health care staff.....	491
Appendix D: Web-based security threats.....	492
Appendix E: Ethics documents	496
E.1. Proposal for research ethics review	496
E.2 Information School Research Ethics Panel: Letter of Approval	504
E.3 Research ethics review outcome	507
E.4: Participant information sheet and consent form	508
Appendix F: Interview guides	511
F.1 Information technology staff (version 3.11)	511
F.2 Information governance staff (version 1.2).....	515
F.3 Library / information managers (version 2.0).....	516
F.4 Communications staff (version 2.0).....	518

F.5 Training and development staff (version 3.0)	519
F.6 Human resources managers (version 1.0).....	521
F.7 Clinical staff (sample – nursing version 1.11).....	522
F.8 NICE manager (version 1.0)	524
Appendix G: HSCIC model Internet use policy	525
Appendix H: Mobile phones and infection control	532
Appendix J: Correspondence from NICE re: browser versions	533
J.1. Internet browser survey of link resolver and knowledge base administrators	533
J.2 Letter from NICE to NHS IT managers	542
Appendix K: The ISMS plan-do-check-act cycle	544
Appendix L: Precision (specificity) and recall (sensitivity) of web filtering	547
Appendix M: Usability problems with mobile apps for accessing e-content.....	549
Appendix N: Summary of responses: access to YouTube / streamed services query.....	550
Appendix P: Information security and cybersecurity measures compared.....	551
Appendix R: Examples of data analysis matrices	552

List of figures

Frontispiece: Tag cloud from Mendeley bibliography manager.....	5
Figure 1.1 Structure of the NHS in England	26
Figure 1.2 Integrating approaches of clinical governance.....	28
Figure 2.1 Literature review thematic map	51
Figure 2.2 Wilson’s updated model of information behaviour.....	57
Figure 2.3 Proposed model : the effect of empowering behaviours on work engagement / burnout	80
Figure 2.4 Relationships between job resources, job demands, burnout and engagement.....	82
Figure 2.5 Representing the circuits of power.....	85
Figure 2.6 Cybersecurity vs. information security and critical infrastructure protection.....	88
Figure 2.7 Proportion of malicious URLs by subject – random URL sample	92
Figure 2.8 Proportion of URLs by subject – all malicious URLs	93
Figure 2.9 Triunal model of cybersecurity vulnerability	98
Figure 2.10 Cultural prototypes and their perspective on risk	105
Figure 2.11 Social amplification of risk	109
Figure 2.12 Blocking of access to e-resources in NHS libraries.....	127
Figure 2.13 Diffusion curve for an interactive innovation.....	132
Figure 2.14 Decision-making processes in innovation.....	134
Figure 2.15 The innovation process in an organisation.....	135
Figure 2.16 Annual expenditure per employee on information and communication technology in the United Kingdom in different economic sectors, 2000.....	141
Figure 2.17 Social media in medicine hierarchy of needs pyramid.....	142
Figure 3.1 Unstructured research method with weak domain-specific theory (Type III)	160
Figure 3.2 Research process flowchart with key to symbols	167
Figure 3.3 Research process Gantt chart	169
Figure 4.1 Background and organisational context	192
Figure 5.1 Overview thematic map	225
Figure 5.2 Barriers to information seeking and use.....	226
Figure 6.1 Education and training arrangements.....	248
Figure 7.1 Organisational dynamics and professional cultures.....	262
Figure 8.1 Information governance and security.....	287
Figure 9.1 Communications policies and practices.....	309
Figure 11.1 Factors determining access to published information within the NHS.....	355
Figure 11.2 Likelihood of reporting blocked websites.....	362

Figure 11.3 Locked-down access to “closed build” PCs and external Internet.....	366
Figure 11.4 Re-thinking circuits of power in acceptable use enforcement.....	369
Figure 11.5 Proposed mechanism of effect of access to information on organisational effectiveness.....	371
Figure K.1 BS ISO/IEC 27001 major process step: PDCA cycle.....	544
Figure K.2 Risk treatment cycle	545
Figure L.1 Confusion matrix.....	547
Figure L.2 ROC curve for content classifier.....	548

List of tables

Table 2.1 Doctors’ preferred sources for information seeking	62
Table 2.2 Studies of malware risk in relation to web browsing behaviour	95
Table 2.3 Technical and social information security counter-measures	99
Table 2.4 Epistemological approaches to risk in the social sciences	102
Table 2.5 Web filtering accuracy	125
Table 2.6 The theory of IT-culture conflict as related to social media applications.....	139
Table 3.1 Stratified ontology of critical realism.....	154
Table 3.2 Types of interview questions	168
Table 3.3 Differing roles of staff groups ... online published information	170
Table 3.4 Interview themes and sub-themes	171
Table 3.5 Interview participants within Trusts by job category.....	189
Table 3.6 Non-Trust participants	190
Table 3.7 Thematic map colour code.....	190
Table 4.1 Trust background information 2014-15.....	194
Table 4.2 Selected Trust performance measures 2013-15	198
Table 5.1 Access to Web 2.0 applications.....	243
Table 5.2 Access to social media applications.....	244
Table 10.1 Summary and comparison of findings by Trust	326
Table B.1 Information behaviour of multi-professional groups of health care staff: primary research	491
Table P.1 Information security and cybersecurity measures compared	551
Table R.1 Results matrix outline as at 28/01/15	552
Table R.2 Example of an individual matrix cell	557

Glossary of abbreviations and acronyms

A&E	Accident and emergency
ADSL	Asymmetric Digital Subscriber Line – <i>a broadband technology</i>
AHP	Allied health professions
ANT	Actor network theory
Athens	<i>(AuTHENTICATION System): a third-party (EduServ) authentication system used by the NHS to provide access to commercially provided electronic content. Now OpenAthens, the technology of which is compatible with Federated Access Management open standards</i>
AUP	Acceptable use policy
BCS	British Computer Society
BCS ASSIST	Association for Informatics Professionals in Health and Social Care
BNF	British National Formulary
BYOD	Bring Your Own Device
CAMHS	Child and adolescent mental health services
<i>C. diff.</i>	<i>Clostridium difficile</i> – a hospital-acquired infection
CBT	Cognitive-behavioural therapy
CAQDAS	Computer-assisted qualitative data analysis
CCG	Clinical Commissioning Group
CD	Compact disc
CERT	<i>CERT Division: concerned with computer security; part of Carnegie Mellon University's Software Engineering Institute</i>
CILIP	Chartered Institute of Library and Information Professionals
COBIT	<i>Originally stood for: Control Objectives for Information and related Technology</i>
CQC	Care Quality Commission
CRIS	Computer Radiology Information System
CSU	Commissioning Support Unit
CVE	Common Vulnerabilities and Exposures
DH	Department of Health
DLP	Data loss prevention
DMA	Digital Maturity Assessment
DNS	Domain name server
DOI	Diffusion of innovations
DVD	Digital Versatile Disc
EBP	Evidence-based practice

e-LfH	e-Learning for Healthcare – <i>a Health Education England programme</i>
eduroam	<i>International wireless network for higher education, further education and research, authenticated by institutional credentials</i>
EPR	Electronic patient record
ESR	Electronic Staff Record
Fed-IP	Federation for Informatics Professionals in Health and Social Care
FoI	Freedom of information
FT	Foundation Trust
FTP	File Transfer Protocol
<i>GIG Cymru</i>	<i>Gwasanaeth Iechyd Genedlaethol Cymru = NHS Wales</i>
GMC	General Medical Council
GPSoC	GP Systems of Choice
HCPC	Health and Care Professions Council
HDAS	Health Databases Advanced Search
HEE	Health Education England
HICF	Health Informatics Career Framework
HR	Human resources
HSCIC	Health and Social Care Information Centre
HTML	HyperText Markup Language
IAPT	Improving Access to Psychological Therapies
ICO	Information Commissioner’s Office
ICMM	Informatics Capability Maturity Model
iCSP	<i>Online forum for members of the Chartered Society of Physiotherapy</i>
IDS	Intrusion Detection System
IES	Institute for Employment Studies
IGT	Information Governance Toolkit
IHRIM	Institute of Health Records and Information Management
IMTG	Information Management and Technology Group
iOS	<i>The mobile operating system used in Apple mobile devices (iPhone, iPad)</i>
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information technology
ITDA	IT Department Accreditation Scheme
ITIL	<i>Formerly IT Infrastructure Library - a best practice framework for IT services</i>
IUE	Information use environment
JANET	Joint Academic NETwork - <i>the UK universities network</i>
JRE	Java Runtime Environment

KSF	(NHS) Knowledge and Skills Framework
LAN	Local area network
LETB	Local Education and Training Board
LGBT	Lesbian, gay, bisexual and transgender
LKSL	Library and Knowledge Services Leads
LIS	Library and information science (or studies)
LMS	Learning management system
Mac OS	<i>The operating system used in Apple Macintosh computers</i>
MDM	Mobile device management
MoM	Map of Medicine
Moodle	Modular Object-Oriented Dynamic Learning Environment – <i>an open-source VLE</i>
MRSA	Methicillin-resistant <i>Staphylococcus aureus</i>
N3	<i>The NHS wide area private network</i>
NCC	National Core Content
NeLH	National electronic Library for Health
NIB	National Information Board
NIMM	National Infrastructure Maturity Model
NPM	New Public Management
NICE	National Institute of Health and Care Excellence
NLH	National Library for Health
NHS	National Health Service
NHSIA	NHS Information Authority
NIB	National Information Board
NLMS	National Learning Management System
NMC	Nursing and Midwifery Council
NPfIT	National Programme for IT in the NHS
NTF	Nursing Technology Fund
OLMS	Oracle Learning Management System (= NLMS)
OpenAthens	<i>see under Athens, above</i>
OPP	Obligatory passage point
OWASP	Open Web Application Security Project
P2P	Peer-to-peer
PACS	Picture Archiving and Communications System
PII	Person-identifiable information
PIN	Personal identification number
PDA	Personal digital assistant
PDF	Portable document format

PHE	Public Health England
PWU	Personal web use
RSS	Rich Site Summary <i>OR</i> RDF Site Summary <i>OR</i> Really Simple Syndication
R&D	Research and development
RIPA	Regulation of Investigatory Powers Act (2000)
ROC	Receiver Operating Characteristic
s.d.	= <i>sine dato</i> – no date
SEO	Search engine optimisation
SETA	Security education, training and awareness
s.l.	= <i>sine loco</i> – no place
SIEM	Security Information and Event Management
SIRI	Serious Incident Requiring Investigation
SIRO	Senior Information Risk Owner
SFIA	Skills for the Information Age
SHALL	Strategic Health Authority Library Leads
SoMe	Social media
STM	Scientific, technical and medical
SWG	Secure web gateway
TDAG	Technical Design Authority Group
TEL	Technology-enhanced learning
TMSA	Transformational Model of Social Activity – <i>Roy Bhaskar’s approach to the issue of agency and structure in social theory</i>
TOE	Technology-Organisation-Environment
UKCHIP	United Kingdom Council for the Health Informatics Professions
URL	Uniform Resource Locator
USB	Universal Serial Bus – <i>an interface standard for computer peripherals</i>
UTM	Unified Threat Management
VRE	Vancomycin-resistant enterococci
VLE	Virtual learning environment
VDI	Virtualization Desktop Infrastructure – <i>a Microsoft virtualisation technology</i>
VoIP	Voice over IP
VPN	Virtual private network

Publications

Research findings have been published as follows:

Ebenezer, Catherine

Nurses' and midwives' information behaviour: a review of literature from 1998 to 2014
New Library World 116(3/4) 2015 155-172

Ebenezer, Catherine

Access to and use of Web 2.0 and social media applications within the NHS in England: the role and impact of organisational culture, information governance, and communications policy
Presentation given at annual research afternoon of Trust T3, February 2015

Ebenezer, Catherine

Access to and use of Web 2.0 and social media applications within the NHS in England: the role and impact of organisational culture, information governance, and communications policy
Presentation given at iFutures conference, University of Sheffield, 7th July 2015. At <https://www.researchgate.net>

Ebenezer, C., Bath, P.A., & Pinfield, S.

"Access denied"? Managing access to the World Wide Web within the National Health Service (NHS) in England: technology, risk, culture, policy and practice. In P.A. Bath, H. Spring, & B. Sen, (Eds.). *Health informatics for enhancing health and well-being*. Poster presented at ISHIMR 2015: The 17th International Symposium on Health Information Management Research, June 24th-25th 2015, York, UK (p. 287-288). York and Sheffield: York St. John University and University of Sheffield

Ebenezer, Catherine

Social media applications within the NHS: role and impact of organisational culture, information governance, and communications policy
Presentation given at meeting of Council for Allied Health Professions Research (CAHPR) Cumbria and Lancashire AHP Regional Hub, October 2015. At <http://www.slideshare.net/ebenezer/cm/social-media-applications-within-the-nhs-role-and-impact-of-organisational-culture-information-governance-and-communications-policy/>

Ebenezer, Catherine; Bath, Peter A; Pinfield, Stephen

"Access denied?" Managing access to the World Wide Web within the NHS in England: technology, risk, culture, policy and practice
Presentation given at CILIP Health Libraries Conference, Scarborough, 15th-16th September 2016. At http://www.cilip.org.uk/sites/default/files/documents/catherine_ebenezer_0.pdf

Chapter 1. Introduction

1.1 Structure

This thesis is concerned with investigating the major organisational and technical factors involved in barriers to professional information seeking, use and sharing within the NHS in England. The introductory chapter (1) begins with a brief statement of the research problem (1.2) followed by a brief personal reflection on the researcher's motivation for undertaking the work (1.3). This is followed by background and context information (1.4) across seven main areas: structure and operation of the NHS (1.4.1), policy drivers for access to published information (1.4.2), NHS IT strategies and developments (1.4.3), information governance and security (1.4.4), NHS libraries and e-library initiatives (1.4.5) NHS e-learning developments (1.4.6), and the current state of the health informatics professions (1.4.7). The chapter continues with a statement of the aims and objectives of the research (1.5), of its research questions (1.6), and of its possible outcomes and benefits (1.7). The structure of the thesis as a whole is set out (1.8). The summary and conclusion (1.9) leads on to the following chapter.

1.2 The research problem

A multiplicity of policy drivers supported access to information resources by NHS staff for professional purposes. These included the NHS Constitution, clinical governance and quality frameworks, and professional standards, which are discussed below in Section 1.4.2.

However, widespread and persistent anecdotal reports from library and training staff working in NHS settings in England, discussed on the LIS-MEDICAL mailing list (Blenkinsopp, 2008b) indicated the existence of a variety of barriers to professional information seeking, use and sharing, and to teaching and learning, apparently presented mostly by information governance, information security or other information technology policies and practices.

These barriers, arising primarily at the level of individual Trusts rather than nationally,¹ included the blocking of individual websites or categories of websites, and infrastructure and system policy

¹ Throughout the thesis, capitalisation of the initial 'T' is used to distinguish references to NHS bodies from references to 'trust' as an interpersonal or organisational disposition.

barriers to the use of particular content types and applications. The material blocked sometimes included e-journal content purchased nationally or locally. PC hardware and software that could not support media types required within e-learning, lack of system permissions to download some types of material (such as podcasts) and slow network performance also presented problems. For students on brief placements, training requirements for network access could be difficult to fulfil in a timely fashion. Significant impediments thereby appeared to be presented to information seeking, to the teaching of students on placement, and to professional e-learning and updating. Limited access to the most current and up to date professional health information and, consequently, to the practice of evidence-based health care, in both clinical and managerial contexts, thereby appeared to result, presenting potential risks to the quality of health services and clinical care provided within the NHS. In particular the blocking of various Web 2.0 and social media applications, as was common in many NHS Trusts, as indicated within the discussions of the Library and Knowledge Services Leads (LKSL) Information Management and Technology Group (IMTG) and in posts to the LIS-MEDICAL mailing list, seemed to leave information professionals, clinicians and managers with substantially reduced capacities for professional networking and information sharing (Blenkinsopp, 2008a).

While it is acknowledged that computer literacy deficits are a contributory factor to wider problems relating to innovation in NHS IT (see below, Sections 2.8.5, 6.4.5, 7.1), it should be noted that the impacts of information literacy or computer literacy deficits, and of resource issues (e.g. resulting in subscription-based or pay-per-view content being unavailable) upon access to published information (Rowlands, Nicholas, Brown, & Williams, 2011), while important to professional learning within the NHS, are outside the scope of this research. (Within the NHS, some of these problems were mitigated to some extent: health professionals used mediated search services and document supply services provided by NHS libraries as well as carrying out their own searches (Brettle, Hulme, & Ormandy, 2007)). Wider socio-political aspects of “access to information”, as comprehensively reviewed by McCreddie and Rice (1999a, 1999b), are also not considered.

1.3 Rationale and motivation for the research

From March 2008 until May 2012 the researcher worked within the NHS as library manager of a mental health Trust in the north east of England, where she was a regional representative on the then national Strategic Health Authority Library Leads Information Management and Technology Group (IMTG) and a member of her Trust’s research governance group. Within her own Trust she frequently encountered obstacles to information seeking, use and sharing of the kind described above (Sections 1.2, see also Section 3.9). As a service to the health library profession and a

contribution to the quality of library and information services and of clinical care, to which she had been committed throughout her librarian career, it seemed important to her to investigate the root causes of these barriers to information seeking and to present her findings to the relevant professional bodies, in the hope and expectation that beneficial changes might result to policy and practice.

1.4 Background and context

1.4.1 Overall structure and operation of the NHS

The National Health Service of the United Kingdom (NHS) came into existence on 5th July 1948. It offers comprehensive, free and universal entitlement to medical care to all UK residents, which is funded almost entirely on taxation and based solely on clinical need, although some charges are made for prescriptions and for dental and optical services. It covers physical and mental health, learning disabilities, primary care services, and ambulance services, but not social care, for which responsibility was transferred in 1974 to local authorities; it is funded by them and privately via means-tested systems of access. The NHS is one of the United Kingdom's largest employers. In 2014, the NHS in England employed a total of 1,187,606 staff (NHS Choices, 2016). The Department of Health's total managed expenditure on NHS services in 2014-15 was £115,802 billion (Department of Health, 2015a).

Responsibility for health services is devolved and accountable to the national administrations of the countries of the UK: the Welsh Government (NHS Wales / *GIG Cymru*), the Scottish Government (NHS Scotland), the Northern Ireland Executive (Health and Social Care in Northern Ireland: HSCNI). The United Kingdom Government is responsible for the NHS in England via the Department of Health (DH). While the regulation of individual clinicians is managed on a UK basis, these different national NHS bodies operate independently, with different organisational forms, regulatory bodies, and IT infrastructures, including digital libraries. In particular those of Wales and Scotland do not operate an internal market, whereas those of England and Northern Ireland do. Since 2013, NHS services in England have not included public health, which under the terms of the Health and Social Care Act 2012 became the responsibility of local authority public health boards accountable to Public Health England (Kaehne, 2014). The overall structure of the NHS in England is shown in Figure 1.1 below.

The governing principles of the NHS in England are set out in the NHS Constitution, first published in 2009 on the recommendation of the Darzi review, *High quality care for all* (Darzi, 2008), and

subsequently amended. Its declared aim and purpose are as follows: “It sets out rights to which patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with responsibilities, which the public, patients and staff owe to one another to ensure that the NHS operates fairly and effectively.” (Department of Health, 2015b, p. 2). It covered basic principles, values, and the rights and responsibilities both of patients and the public and of staff.

NHS primary care is delivered by a variety of independent contractors. These include general practitioners (GPs), dentists, pharmacists and optometrists. GPs usually work in practices as part of a team which includes other clinical and administrative staff. General practitioners act as gatekeepers to secondary care and other services via a system of referrals. General practice organisations manage their own IT infrastructures within an overall national procurement framework, GP Systems of Choice (GPSoC)². In 2016, there were 7,616 GP practices in England.

The main organisations responsible for providing other health services (including acute general and specialist care, community health services, mental health and learning disabilities services, and ambulance services) within the NHS in England are NHS Trusts. The NHS Trust as an organisational form developed from the introduction of the internal market and purchaser-provider split into the English NHS in 1991. Following the establishment of the internal market, “purchasers” (health authorities, as they then existed, and some general practices) were provided with budgets to purchase health services from a range of “providers”. Trusts are public sector corporations serving populations in large catchment areas, each headed by a board consisting of executive and non-executive directors, and chaired by a non-executive director. They compete with each other and with other providers locally within their specialisms for contracts to provide services, via complex processes of competitive tendering.

The Trusts in the study, other than T2, were Foundation Trusts (FTs). FTs, which enjoyed wider autonomy than non-foundation Trusts, mainly of a financial nature, were regulated in respect of their finances and corporate governance at the time of the study by Monitor, while non-FTs were managed by the Trust Development Authority. (The two bodies merged in 2016.) The structure of FTs, which involved local members and elected governors, was designed to encourage accountability to their communities in a more patient-centred NHS. As well as annual reports, they were required

² GPSoC: <https://digital.nhs.uk/article/282/GP-Systems-of-Choice>

to produce annual quality accounts describing their performance against a range of national indicators. All health and social care providers were regulated and licensed in respect of the quality and safety of their clinical services by the Care Quality Commission.

In 2016 there existed 137 acute non-specialist Trusts (including 85 Foundation Trusts); 17 acute specialist Trusts (including 16 foundation Trusts); 55 mental health Trusts (including 43 Foundation Trusts); 34 community providers (11 NHS Trusts, six Foundation Trusts and 17 social enterprises); and 10 ambulance Trusts (including five foundation Trusts)(NHS Confederation, 2016). Some of the non-specialist acute and mental health trusts also provided community health services. Figure 1.1 below illustrates the main lines of accountability and funding responsibility within the structure.

Intrinsic to the operation of the internal market is a procurement function for services known as commissioning, this being “the process of ensuring that care services are provided effectively and that they meet the needs of the population ... a complex process with responsibilities ranging from assessing local population needs, prioritising outcomes, procuring products and services to achieve those outcomes and supporting service providers to enable them to deliver outcomes for individual service users” (Yorkshire and the Humber Joint Improvement Partnership, 2015).

NHS England, which took on full statutory responsibilities in April 2013, had been established primarily as a commissioning body; it was responsible for purchasing primary care services and some other specialised services. Regional teams of NHS England were responsible for the commissioning of services in their respective areas, as well as providing professional leadership in both clinical and non-clinical aspects of health services. The regional teams also commissioned public health programmes, such as immunisation and screening. The majority of hospital and community services were commissioned by so-called Clinical Commissioning Groups (CCGs), which were overseen by NHS England. CCGs, of which there were 212 in 2014-15, were clinically led groups which included all the general practices within their area (NHS Choices, 2016).

The services of Commissioning Support Units (CSUs), which at the time of the study were being established by NHS England as independent business units intended to provide a range of administrative functions, including information governance and IT support, were available to CCGs to support this task. CCGs were not, however, obliged to use them, being free to place contracts with private sector organisations recognised within the national procurement framework. In some instances, CSU functions were subsequently brought in-house by the CCG; in other instances, CSUs

struggled to establish themselves as viable businesses (NHS Commissioning Board, 2011; Thiel, 2013).

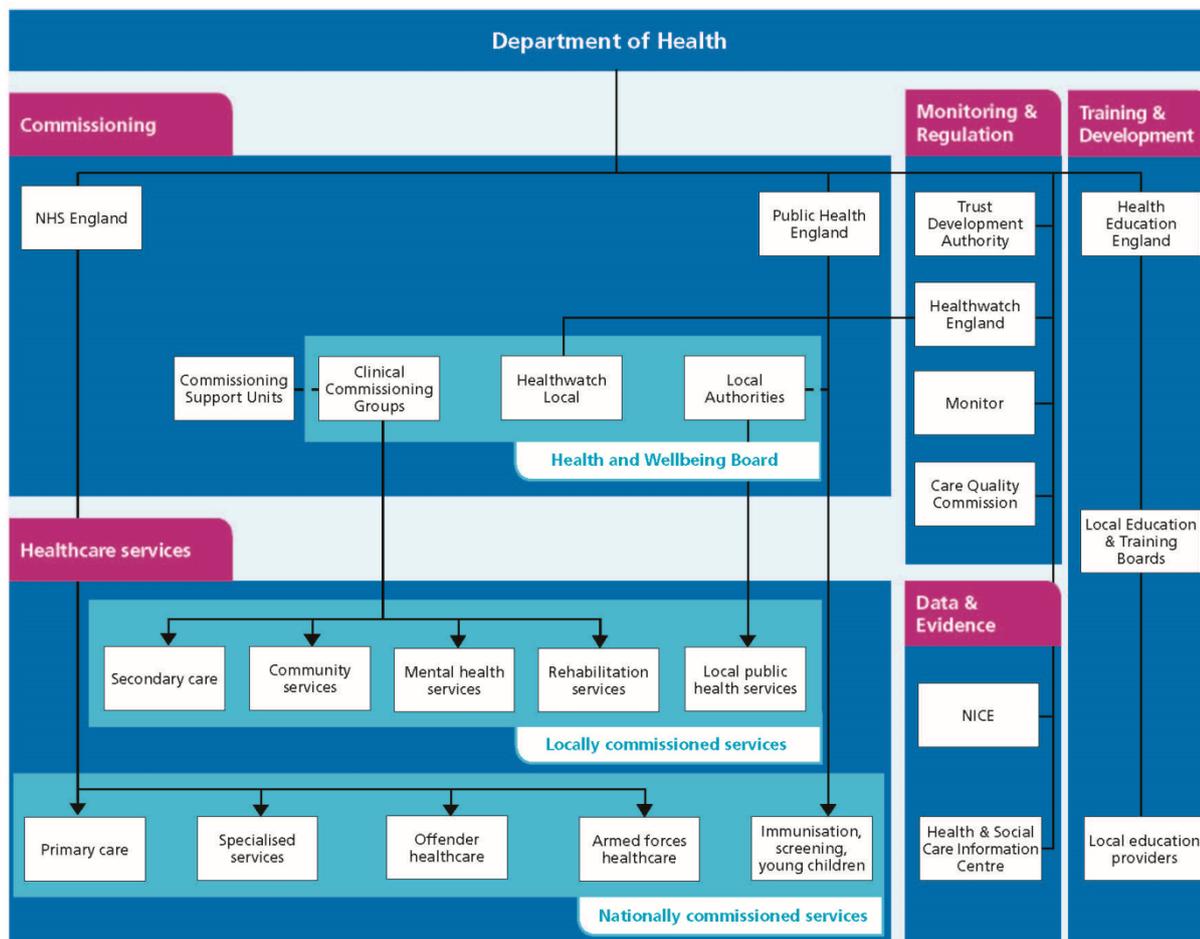


Figure 1.1 Structure of the NHS in England
(NHS Choices, 2016) Crown copyright

1.4.2 Policy drivers for access to published information

It was a principle of the NHS Constitution (Department of Health, 2015) that all staff should have appropriate access to training, support, education and professional development and to resources for the conduct and implementation of research:

“[The NHS] provides high quality care that is safe, effective and focused on patient experience; in the people it employs, and in the support, education, training and development they receive; in the leadership and management of its organisations; and through its commitment to innovation and to the promotion, conduct and use of research to improve the current and future health and care of the population.”

In addition, the NHS pledged to:

“provide all staff with personal development, access to appropriate education and training for their jobs, and line management support to enable them to fulfil their potential”

Under the Health and Social Care Act, 2012 a duty existed on behalf of the Secretary of State for Health to ensure “the use in the health service of evidence obtained from research”. In addition, evidence-based practice and the need to update knowledge and skills featured widely in professional standards documents as requirements for clinical practice and revalidation (Department of Health, 2012a, 2012c; General Medical Council, 2013; Health and Care Professions Council, 2014; Nursing and Midwifery Council, 2008; Royal Pharmaceutical Society, 2014) and in the values statements of individual NHS organisations.

Clinical governance, introduced into the NHS in the late 1990s, has been defined as “the system through which NHS organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care, by creating an environment in which clinical excellence can flourish.” (Department of Health, 1998, p. 116). The policy documents which introduced the clinical governance framework (Department of Health, 1997, 1998, 2000) strongly emphasised the central role of continuing professional development and learning as a means of providing NHS clinical staff in all professional groups with the knowledge to offer the most up to date, effective and high quality care to patients. They also emphasised the incorporation of research-based evidence into clinical practice as a means of facilitating clinical effectiveness, sources for which needed therefore to be accessible to staff (Halligan & Donaldson, 2001; McSherry & Haddock, 1999; Scally & Donaldson, 1998); see under "infrastructure", "culture" and "quality methods" in Figure 1.2 below). The more recent focus on quality governance retains clinical effectiveness as one of its core components (National Quality Board, 2011). Clinical governance is discussed further in Sections 2.5.5.1 and 2.5.5.2 below, in relation to organisational characteristics of the NHS, regulation and public trust.

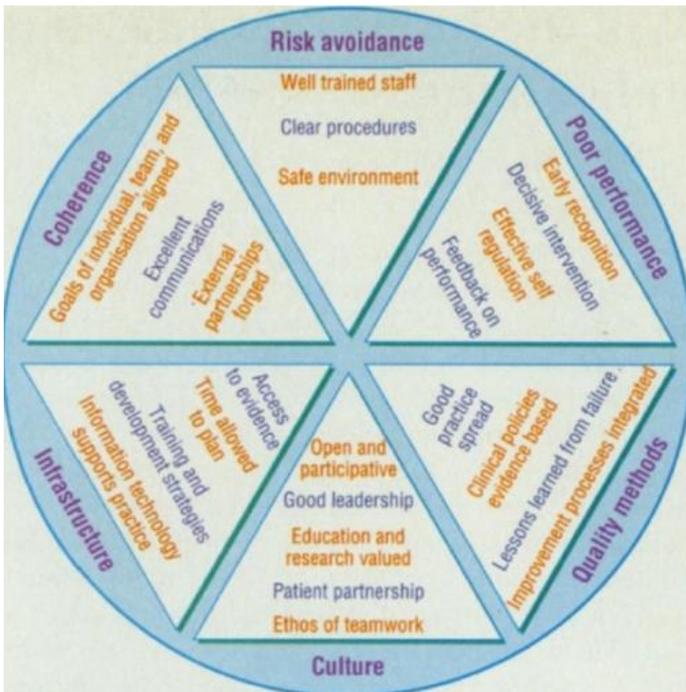


Figure 1.2 Integrating approaches of clinical governance

Sally and Donaldson (1998), p. 82

Reproduced by permission

1.4.3 NHS IT strategies and developments

Part of the background and context of the research concerns approaches within the NHS in England to information technology strategy and information systems implementation in general. Historically this had been a much-contested area; innovations in information technology, although assigned a high strategic priority and large financial investment, had proved extremely difficult to implement (Currie, 2014; Currie & Guah, 2007; Eason, 2007; Greenhalgh & Keen, 2013; Mark, 2007; Sauer & Willcocks, 2007; Takian & Cornford, 2012). Moreover the NHS had tended to oscillate between centralised and decentralised approaches to information systems implementation (NHS England, 2014a; “‘Stars are aligned’ for health IT - Freeman,” 2016). To support its strategic aims, the DH and NHS England from 2012 onwards had introduced competitive bidding processes for national funding to drive information technology innovation: initially the Nursing Technology Fund³ and subsequently the Integrated Digital Care Technology Fund.⁴

³ Nursing Technology Fund: <https://www.england.nhs.uk/digitaltechnology/info-revolution/nursing-technology-fund/>

⁴ Integrated Digital Care Technology Fund: <https://www.england.nhs.uk/digitaltechnology/info-revolution/idct-fund/>

National administrative structures supporting NHS information technology had undergone considerable changes over the preceding decade, associated with the establishment in 2002 and eventual winding-up in 2011 of a major centralised programme known as the National Programme for IT in the NHS (NPfIT). The former NHS Information Authority, established in 1999 following the publication of the strategy document *Information for Health* (NHS Executive, 1998), was abolished in April 2005; its work, including responsibility for the National electronic Library for Health (see Section 1.4.4 below) was divided between Connecting for Health (the agency managing NPfIT), and a newly created Information Centre for Health and Social Care. This latter was subsequently renamed, initially as the Health and Social Care Information Centre (HSCIC), then in July 2016 as NHS Digital. Connecting for Health ceased to exist in March 2013 (Campion-Awwad, Hayton, Smith, & Vuaran, 2014).

At the time of the study, the organisational landscape was continuing to shift and evolve (Heather, 2016b). Information technology within the English NHS was coordinated by the National Information Board (NIB), established in September 2014 by NHS England to succeed the former Informatics Services Commissioning Group which had been established in late 2012. This was a collaborative partnership of representatives from 29 organisations. Its remit was to provide strategy and leadership across health and care organisations on information technology, and to set commissioning priorities for the Health and Social Care Information Centre (National Information Board, 2014a). The NIB was responsible for the publication in November 2014 of the strategy document *Personalised health and care 2020: using data and technology to transform outcomes for patients and citizens* (National Information Board, 2014b) and in July 2015 for the setting out of a series of work streams for NHS IT. These included the conduct of the Digital Maturity Self-Assessment (NHS England, 2016) by Trust IT departments, which assessed aspects of informatics readiness, capability and infrastructure, and development of so-called digital roadmaps by CCGs, both in pursuit of the strategic objective of a paperless NHS by 2020 (NHS Confederation, 2014). In contrast with previous centralised NHS IT strategies, the details of how individual health organisations were to achieve these aims were to be determined locally (National Information Board, 2016). This strategy remained in operation, modified to some degree in its implementation by other initiatives, notably the government's linking of IT funding to Sustainability and Transformation Plans (Whitfield, 2016b) and the recommendations of Professor Robert Wachter's review of NHS IT (Wachter, 2016).

NHS informatics policy documents such as *Liberating the NHS: an information revolution* (Department of Health, 2010) and *The power of information* (Department of Health, 2012d) appeared to manifest a limited understanding, pervasive within the NHS, of the concept of “information” as relating solely to internally-generated data and information, and excluding the exchange of shared experience and knowledge, or externally-published information (Daines, 2011). Some implications of this are discussed below in Section 11.4.

Provision of PC and network infrastructure within NHS Trusts was managed locally, either in-house, via outsourcing arrangements, or a combination of both. NHSmail,⁵ a national web-based email service approved for the sending of patient-identifiable and sensitive information, was available to NHS organisations, though many (including the Trusts in the study other than T2) continued to use domain-based email predominantly. In general (other than eduroam Wi-Fi installations in teaching hospitals) provision of IT infrastructure appeared to be driven by the requirements of clinical and administrative systems rather than those of professional learning. In relation to patient and staff use of mobile devices, the general practitioner Marcus Baw and others in the NHS Hack Day group had established a register of hospitals, AboutMyHospital, offering Wi-Fi access to staff, patients and visitors, which provided a good overview of existing levels of Wi-Fi availability. (NHS Hack Days were weekend events designed to bring together clinicians, software developers, designers and statisticians to create innovative IT solutions to problems besetting the NHS.) Wi-Fi access for clinical staff and patients had become a concern for the group; it had been found that Wi-Fi network access was in some places being reserved for managers and executive staff (Baw, 2013). This led it in May 2013 to create and publish a survey of Wi-Fi availability to staff.⁶ During the course of the research, provision of free Wi-Fi in all NHS buildings became an expressed aim of government policy (see Section 12.8, below).

The potentially adverse impacts of obsolete IT infrastructure on clinical system stability and security were highlighted in two reports on NHS information technology in England published in the summer of 2016. The CQC’s review *Safe data, safe care* (Care Quality Commission, 2016) identified it as a potential security risk. The review recommended that “computer hardware and software that can no

⁵ NHSmail: <https://digital.nhs.uk/nhsmail>

⁶ AboutMyHospital: <http://ec2-54-237-33-114.compute-1.amazonaws.com:8080/ewd/aboutMyHospital/index.html>

longer be supported should be replaced as a matter of urgency.” (p. 5). The Wachter review, *Making IT work* (Wachter, 2016, p. 36) recommended that:

“The new digital strategy for the NHS should involve a thoughtful blend of funding to help defray the costs of IT purchases and implementation, resources for infrastructure (hardware such as monitors and keyboards, network modernisation, wifi) ... The odds of failure will be increased by focusing only on buying and installing IT systems without attending to issues like hardware, network stability and speed, workforce training and development, programme evaluation, and iterative improvements.”

1.4.4 Information governance and security within the NHS

Gartner Research defined information governance as “the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals” (Logan, 2010). In an NHS context it was defined as “a framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service” (NHS Connecting for Health, 2007). Information governance systems and processes in the English NHS, which were highly centralised, encompassed concepts of records management, information security, public accountability and legal compliance (Lomas, 2010). They followed a controls assurance approach, in that they were characterised by “a focus on robust, documented policies and procedures, delivered through accredited processes and systems, by accredited staff” (Haw, Derry, & Gowing, 2006, p. 4). They were intended to ensure necessary safeguards for, and appropriate use of, patient and personal information. They were developed from the work of Caldicott guardians (Roch-Berry, 2003) in response to the increasing risk and complexity of managing person-identifiable information (PII) or other sensitive information in an era of growing dependence upon information technology, in particular electronic patient records (Donaldson & Walker, 2004). A Caldicott guardian was a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing (Department of Health, 1999).

The key statutory requirement for NHS compliance with information security management principles was the Data Protection Act 1998, and in particular its seventh principle: “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data” (Information Commissioner’s Office, 2012). Information security requirements for NHS IT infrastructure were established by the Infrastructure Security Team at the Health and Social Care Information Centre.

The organisational framework for information security within the NHS in England was provided primarily by the document *Information security management: NHS code of practice* (NHS Connecting for Health, 2007), referred to subsequently as the *Code of Practice*. It sat alongside other information governance codes of practice covering confidentiality, records management, and legal obligations. Another important consideration was the eighth principle of the Data Protection Act 1998, which stated that “Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”. At the time of the study the EU-US Safe Harbor Framework⁷ under the provisions of which personal data could be lawfully transferred to and from US companies, had been ruled invalid by the Court of Justice of the European Union (Price & Cook, 2015). A new framework, the EU-US Privacy Shield, had been adopted in its place (Dunn, 2016; Gilbert & van der Heijden, 2016)..⁸

The *Code of practice* specified the development and use of an information security management system (ISMS) as a method of measuring compliance with information security standards, as prescribed in ISO 27001 (ISO, 2013). Within its ISMS, an NHS organisation was required to define the business needs for information security and set these out within a corporate information security policy, to identify and assess the risks to information security, and to establish controls, where necessary, to manage them, including staff training. It was also to identify a risk evaluation method and documentation processes. Other than BS ISO/IEC 27001, NHS organisations were encouraged to make use of other nationally and internationally recognised “best practice” standards, such as ITIL (Cabinet Office, 2011a, 2011b, 2011c, 2011d, 2011e) for infrastructure management and security. The Health and Social Care Information Centre (HSCIC) published detailed technical briefings for IT staff on various technologies. Significantly at the time of the study, preparation of guidance on content filtering “for organisations who wish to deploy or operate content filtering systems” had been stated to be “in progress” since 2013.⁹

The *Code of practice* also prescribed a structure whereby each NHS organisation needed to establish an accounting officer (the chief executive), a senior information risk owner (a board level

⁷ EU-US Safe Harbor Framework: (<http://export.gov/safeharbor/index.asp>),

⁸ Privacy Shield Framework: <https://www.privacyshield.gov/welcome>

⁹ <http://systems.hscic.gov.uk/infogov/security/infrasec/gpg>.

organisational lead for information governance), information asset owners (senior members of staff to whom ownership of assets was assigned) and information asset administrators, who supported the information asset owners and had day-to-day operational responsibility for information risks in their areas. It was thereby made clear that information governance needed to be owned and managed locally, and was not the sole responsibility of information governance or IT staff. All information assets needed to be identified, and information flows described in detail. All NHS staff were required to undertake annual training via e-learning in the basics of information governance via the training tool, and each Trust had a target of ensuring that 95% of staff completed it.¹⁰ Each NHS organisation was required to develop a comprehensive information risk policy, to sit within its overall business risk management framework. The senior information risk owner was responsible for developing and implementing this policy.

The information governance performance of NHS organisations was rated via the Information Governance Toolkit (IGT) (<https://www.igt.hscic.gov.uk>), which set out information governance and security requirements for different types of NHS organisation. The 63 information security assurance requirements within the IGT were drawn substantially from the ISO 27000 series of standards: ISO 27001, ISO 27002, ISO 27005 and associated applicable controls. Other requirements were drawn from the Data Protection Act 1998, the Caldicott report (Caldicott, 1997), and the *Code of practice* itself. However, despite its introduction, the number of NHS data breaches was increasing overall: 7255 were reported between 2011 and 2014, with a 101% increase between 2013 and 2014 (Evans, Maglaras, He, & Janicke, 2016). A senior manager at NHS Digital (formerly HSCIC) suggested in late 2016 that the IGT in its present form was likely to be abolished and replaced (Heather, 2016a).

The then-current state of data protection law and practice reflected heightened public concern following the 2007 loss of CDs in the post by Her Majesty's Revenue and Customs (HMRC) containing the records of 25 million child benefit recipients, and other well-publicised data breaches occurring at the time (Ceeney, 2009; Grant, 2015; Kamath, 2008; Turle, 2009; Watters, 2009). The Information Commissioner's Office (ICO) had the power to issue monetary civil penalty notices of up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6th April 2010 (Information Commissioner's Office, 2010). Short of doing this, the ICO could require the signing of an undertaking on the part of a data controller (generally the chief executive in an NHS Trust) to comply

¹⁰ <https://www.igte-learning.connectingforhealth.nhs.uk/igte/>.

with the seventh data protection principle, in respect of remedying whatever security measures were lacking. The details of such incidents were published on the ICO website, hence adverse publicity and further possible loss of public trust was involved. NHS Trusts were also required to provide information about data breaches in their annual reports (Grant, 2015); Foundation Trusts were required to report IGT scores within their quality accounts (Monitor, 2014). Within an NHS Trust, breaches of the Data Protection Act were classified as Serious Incidents Requiring Investigation (SIRIs)(Health and Social Care Information Centre, 2015a). Trusts were required to report to the ICO via the IGT reporting tool any information governance incident rated at SIRI Level 2 or above (HSCIC, 2013). The staff involved in such SIRIs could face various forms of disciplinary action, including dismissal. For these reasons, information governance tended to be accorded a high strategic priority within NHS organisations, particularly when a data breach had previously occurred; tolerance of information security risks was generally very low (BCS ASSIST, 2012). A high level of fear could be engendered among NHS staff at all levels regarding information governance issues (Caldicott, 2013; Renaud, 2012; Renaud & Goucher, 2012).

One aspect of NHS information security policy that had far-reaching impacts upon information use and sharing was the requirement that all portable media and devices be encrypted. The policy was introduced in early 2008 (Department of Health, 2008) following the HMRC data loss and the subsequent issuing of guidance by the Information Commissioner's Office.¹¹ It was not implemented immediately in all NHS organisations; in the researcher's former Trust, for instance, the requirement to use encrypted USB memory sticks was not brought in until early 2009 following a data breach (3.9), and the process of encrypting the large number of Trust-owned laptops was undertaken during the summer of that year. The requirement applied in practice to laptop computers, tablet computers, mobile phones and USB memory sticks. Encryption standards were prescribed nationally (Department of Health, 2008; Health and Social Care Information Centre, 2015; Wood & Penny, 2012). A national contract existed with McAfee Data Protection for the supply of device encryption, port control, secure content encryption and mobile encryption software, although its use did not appear to be mandatory ("McAfee wins contract for NHS data encryption," 2008).

¹¹ According to Grant (2009), this guidance was issued in early 2008. The original version was no longer available at the time of the study. The most recent version (April 2015) may be found at <https://ico.org.uk/media/for-organisations/encryption-0-0.pdf>

Particular policies governed the use of mobile phones. Their use had formerly been banned entirely within NHS premises on the grounds that mobile signals could interfere with medical devices and equipment. At the time of the study it was still relatively common to see notices in hospital outpatient departments and doctors' surgeries requesting patients not to use them. Since 2009 the use of mobile phones on NHS premises within England had been governed by the policy framework set out within *Using mobile phones in NHS hospitals* (Department of Health, 2009b), as elaborated within more recent Information Governance Alliance guidance (2015). These two documents set out clearly where usage should be prohibited or restricted, and how staff should manage patient usage. However, the use of mobile phones by staff members was not addressed.

The HSCIC, while it provided strategic guidance on the deployment of mobile technologies,¹² did not provide specific security guidance relating to mobile phones. However, the guidance provided by HSCIC on the security of tablet computers was very stringent. Automatic cloud backup was to be disabled. The ability to transfer data from the device to other networks or devices was to be restricted as far as possible to a "whitelist" of permitted destinations. The application suite was to be standardised (unnecessary applications should be removed, and the possibility of re-installing them blocked) and implementation of a virtualisation service considered to ensure that data was not stored on the device. It was thereby implied that access to download sites for applications and files (such as Google Play or the Apple App Store) should also be blocked. Bluetooth had to be disabled, and virtual private network (VPN) connections used to networks; where possible the ability to connect to wireless networks other than those specifically intended was also to be disabled. Tablets were not to be used to store person-identifiable or sensitive information. As with other portable media, they had to have strong encryption enabled by default (see above); the use of a mobile device management (MDM) system was recommended. (MDM systems provide configuration and access controls, and the facility to wipe the device remotely in case of loss or theft.)

Professional associations also issued guidance to their members regarding the use of mobile devices. The Royal College of Nursing discouraged the use of personal mobile devices in the workplace, on grounds of information security and confidentiality, personal safety, and potential costs (Royal College of Nursing, 2012b).

¹² NHS Mobile Working Knowledge Centre: <http://systems.hscic.gov.uk/qipp/mobile>

In the case of social media, the HSCIC, while entertaining website blocking as a possibility, clearly recommended user education rather than technical controls as the main remedy for inappropriate social media use: “Whilst there are technical website filtering controls that could be applied, the main defence against threats associated with blogging and social networking is user awareness related” (Health and Social Care Information Centre, 2012, p. 6). Within health services in England, social media policies and guidelines have been issued by national strategic bodies (e.g. NHS England, 2013), NHS Trusts, regulatory bodies (e.g. General Medical Council, 2013; Health and Care Professions Council, s.d.; Nursing and Midwifery Council, s.d., 2015), professional associations (e.g. British Association of Social Workers, 2012; British Psychological Society, 2012.; Royal College of General Practitioners, 2013; Royal College of Radiologists, s.d.), and trade unions (e.g. British Medical Association, 2011) (*cf.* below, Section 2.8.4). The report of the official investigation into the sexually abusive activities of the late Jimmy Savile on NHS premises (Lampard & Marsden, 2015) set out a requirement for NHS Trusts to formulate a policy regarding the management of access to the Internet and to social media by patients and visitors. This was said to be required in order to address a safeguarding concern, *viz.* “to protect people on their premises from the consequences of inappropriate use of information technology, the internet and social media.” (p. 18). NHS electronic communications and social media policies in relation to information needs have become a focus of discussion by NHS librarians (Elcock, 2016; Rey, 2016); see also Section 5.5.

1.4.5 NHS libraries and e-library initiatives

It is important by way of background to provide some account of initiatives to provide NHS clinical staff with online resources for evidence-based practice and decision-making, as problems were frequently encountered with using these.

The provision of library and information services within NHS organisations was managed and supported at a strategic level by Health Education England (HEE) (Health Education England, 2014). A development framework for library services, *Knowledge for healthcare*, was issued in late 2014 (Health Education England, 2014), according to which “Healthcare library and knowledge services underpin all aspects of the NHS - supplying the evidence base to the service to make decisions on treatment options, patient care and safety, commissioning and policy, and to support lifelong learning, undertake research and drive innovation” (p. 6). The provision of services was coordinated by library leads from each of the 13 HEE Local Education and Training Boards (LETBs), and subject to a national quality assurance framework. Library and information services within NHS organisations could vary greatly in form and means of delivery; they could be provided as standalone services, or

via outsourcing or partnership arrangements with institutions of higher education or with other NHS Trusts. Funding for libraries was complex and often historically based on educational funding streams, with marked inequities between regions, and between the acute and other sectors (Ebenezer, 2000; Robert Huggins Associates, 2005; Hill, 2008; Stewart, 1992). This bore on the level of staff support available for service development and information literacy training, as well as the provision to end-users of subscription-based information resources.

It was common in the later 1990s for NHS libraries to purchase subscriptions to web-based versions of bibliographic databases locally, although a number of regional library services were experimenting with consortial purchasing (Pye & Ball, 1999). The 1998 NHS IT strategy *Information for health* (NHS Executive, 1998) included among its strategic objectives a plan to establish a National electronic Library for Health (NeLH) : “a National Electronic Library for Health including accredited clinical reference material will be established” (NHS Executive, 1999, p. 60). This was intended to provide easy access for clinicians to best current knowledge, and thereby to improve health and health care, patient choice, and clinical practice (Toth, Muir Gray, Fraser, & Ward, 2000), the assumption being that “health professionals have information needs that they themselves recognise and that they will access such information if provided with the means to do so” (Randell, Mitchell, Thompson, McCaughan, & Dowding, 2009). The plans envisaged that NHS librarians would play a pivotal role in the development and delivery of the NeLH's aims and objectives. Included in the proposals was the creation of a series of so-called Virtual Branch Libraries covering specialised areas; these were intended to function as communities of practice (Brice, 2003). The pilot NeLH went live in 2000; it was launched as a full service in the spring of 2003. Available resources included a selection of evidence-based sources authenticated via the Athens system (now OpenAthens), including the Cochrane Library; the range of these increased over time. A subsequent IT strategy document, *Building the information core* (Department of Health, 2001) set NHS Trust IT departments a target for clinical and support staff to be provided with basic email and web browsing services by March 2002, and other staff to have them by March 2003. The NeLH aimed to work in partnership with NHS libraries (Turner, 2004).

The DH's response to the report of the inquiry into paediatric cardiac surgery at the Bristol Royal Infirmary (Department of Health, 2002a), gave impetus to the establishment of a unified, hybrid National Library for Health (NLH) that included a greater amount of centrally-purchased electronic content (Ebenezer, 2005; Herman & Ward, 2004; Isetta, 2008), procurements for which were carried out via the National Core Content project (NCC)(Glover, 2008). A new common interface for

bibliographic databases integrated within the NLH website was implemented in April 2008, initially called Search 2.0, later renamed Health Databases Advanced Search (HDAS) (“Journals and databases,” 2008). The deployment of an NHS-wide link resolver enabled library leads and Trust library managers to purchase additional content to supplement the “core” e-journal and e-book purchases, which could thereby be made available to staff within the relevant Trust(s). However, problems with HDAS (originally known as Search 2.0) had been frequently reported by librarians via the LIS-MEDICAL JISCMail list and elsewhere ever since its launch, including slow response times, non-availability of the service, crashes, anomalous search results, or problems with exporting search results. Even following a major upgrade in June 2012 which had been intended to address the main technical problems, these reports had continued.¹³ For the benefit of library staff reporting service issues, a summary of reported problems with HDAS had been published on the NICE website.¹⁴ As a measure to minimise their impact, access was made available for library staff and end-users to the relevant aggregators’ “native” interfaces as an alternative. In response to the ongoing problems, another major upgrade of HDAS was initiated in 2015 and launched in October 2016.¹⁵

During its ten-year life span, responsibility for the former National electronic Library for Health / National Library for Health transferred between organisations four times: from the NHS Information Authority (NHSIA), to Connecting for Health when the NHSIA was abolished, then to the NHS Institute for Innovation and Improvement before, following publication of the Darzi review (Darzi, 2008), finally transferring to the National Institute for Health and Care Excellence (NICE), albeit in a considerably altered form — i.e. minus its strategy, its Virtual Branch Libraries and its development remit for NHS library services — as NHS Evidence (National Library for Health, 2009). This institutional instability, and the resulting separation of e-library initiatives from other aspects of NHS IT, is of importance culturally and politically, and is discussed further in Section 11.5.

¹³ They are referred to in the minutes of the LKSL Information Management and Technology Group for November 2012:

http://www.libraryservices.nhs.uk/document_uploads/SIMTG/SIMTG_minutes_14_Nov_2012.pdf.

The researcher has been unable to locate the report which was circulated to members of the group.

¹⁴ <http://www.nice.org.uk/about/nice-communities/library-and-knowledge-services-staff/nice-evidence-services-issues>.

¹⁵ <http://labs.nice.org.uk/331-2/>.

From the outset, the third-party authentication service Eduserv Athens (later OpenAthens) was used to authenticate access for NHS staff to e-resources.¹⁶ Eligible staff needed to register individually for OpenAthens accounts using an NHS email address or from a computer within the N3 network. Accounts were issued for a period of two years initially. They could be retained when staff moved to another NHS organisation; users were required to change their account details online to do this. Users frequently contacted library services requiring help with lost usernames or passwords (although an automated password reminder facility was available), with expired accounts, and with problems transferring their accounts. They were also likely to encounter problems with individual resources (see Section 5.3, below). A relatively small proportion of NHS clinical staff registered for OpenAthens accounts; the percentage of an organisation's staff who were active Athens account users was at one stage proposed as a national key performance indicator (Royal Berkshire NHS Foundation Trust, 2014). In the interests of information literacy support, some universities also issued their health sciences students with university OpenAthens accounts; these provided access not to locally purchased material, but solely to the national core content e-resources (University Health and Medical Librarians Group, 2014). Students on placement within the NHS were also eligible to register for local NHS OpenAthens accounts on the same basis as staff, and an individual student was able to hold both types of account; this was another fertile source of confusion. Individuals who were not eligible for a personal NHS OpenAthens account could be offered an access account, enabling them to access NHS e-resources within an NHS library on a walk-in basis.

End-users' difficulties with Athens or OpenAthens authentication were referred to a major library strategy document: "There always seems [sic] to be problems logging into Athens ... and accessing the article is quite confusing." (Health Education England, 2015b, p. 14) This relates to Brennan *et al.*'s finding (2014) that NHS staff and student users perceived the need for usernames and passwords to be a major barrier to accessing information.

At the time of the study, social workers within the UK had available to them an information portal developed by the Social Care Institute for Excellence (SCIE):¹⁷ those employed by local authorities who were working within the NHS had access online to a range of professional journals in social work, authenticated via Athens, as well as to local and national NHS information resources.

¹⁶ Eduserv OpenAthens: <http://openathens.org/>

¹⁷ SCIE: <http://www.scie.org.uk> [retrieved 01/05/2013];

In relation to access to information resources, one of the agreed follow-up actions from the TDAG survey (described below in Section 2.7.3.4.2) (TDAG, 2009b), was the setting-up of a national whitelist of “domains not to be blocked” within the NHS. This whitelist was updated at the group’s meetings, where candidate sites for addition to the list which had put forward by librarians within the members’ geographical areas were discussed and decided upon. The list was maintained as an MS Excel spreadsheet; it was available to download at the (LKSL) website.¹⁸ The successor to the group ceased to exist in March 2015 when LKSG’s subgroups were reorganised to align with the core themes of the *Knowledge for Healthcare* library strategy (Health Education England, 2014); its papers were archived on the site. Subsequently, arrangements were made for the list to be maintained by one of the local OpenAthens administrators. The intention was that library managers should send updated versions of the whitelist to their Trust IT departments as soon as they were published, for the required configuration changes to be made.

1.4.6 NHS e-learning developments

Barriers were also encountered to accessing and using e-learning resources as information sources, so again it is relevant to provide a brief account of NHS e-learning initiatives. At the time of this study, education and training delivered within the NHS could be categorised in terms of 1) professional pre-registration and post-registration training 2) statutory and mandatory training delivered to all Trust staff 3) other Trust-based or externally sourced training relating to organisational learning and staff development needs. Statutory training was that which the Trust was required to provide by law, or where a statutory body had instructed organisations to provide training on the basis of legislation, and was required for all staff groups. Requirements for mandatory training were mainly determined by the individual Trust, but included initial and annual refresher training on information governance for all staff, delivered via e-learning (NHS England, 2014). Mandatory training was concerned with minimising risk, providing assurance against policies, and ensuring compliance with external standards, and was generally specific to roles or departments. The content of statutory and mandatory training had been partly standardised nationally via the North West Core Skills Programme and subsequently the UK-wide Core Skills Framework produced by Skills for Health. The statutory and mandatory training provided by all the Trusts in the study was aligned to varying degrees with the Core Skills Framework.

¹⁸ LKSL: <http://www.libraryservices.nhs.uk/>.

All of these forms of education and training could involve e-learning. On grounds of cost-effectiveness it had become common practice across the NHS to deliver mandatory and statutory training via e-learning, at least in part. The document *Supporting best practice in e-learning in the NHS: a strategic framework* (NHS National Workforce Group, 2005) identified a clear need to establish the wider adoption and deployment of e-learning across health care services. The subsequent report *Modernising healthcare training: e-learning in the healthcare services* (e-mpirical, 2006) outlined a number of recommendations and strategic elements considered essential for the effective management and deployment of e-learning at national, regional and local levels (Bingham & Wright, 2008). It noted that “barriers to access to computers and a supportive learning infrastructure remain and probably represent the biggest barriers to the effective implementation of the use of new learning technologies” (p. 10).

Wright and Bingham (2008) cited the need to meet the DH’s *Standards for better health* (Department of Health, 2009c) and the NHS Litigation Authority’s *Risk management standards* (e.g. NHS Litigation Authority, 2013) as a key driver for the introduction of technology-enhanced learning within the NHS.

The publication of the DH’s *Framework for technology enhanced learning* in November 2011 encouraged the wider adoption of learning technologies given their potential for patient and service delivery, development of the workforce, flexibility for training delivery and cost effectiveness (Department of Health, 2011a). From 2008-2009 onwards, the DH had made significant central investments in e-learning. Significant national initiatives had been put in place to drive forward the e-learning agenda forward within the English NHS, including the e-Learning Repository;¹⁹ the National Learning Management System (NLMS)²⁰, a new module of the national Electronic Staff Record (ESR), designed to enable and track employee access to e-learning); the Skills for Health e-Learning Readiness Toolkit²¹ and NHS Core Learning Unit²²; and the setting up of e-Learning for Healthcare (e-LfH), which develops e-learning content in partnership with medical royal colleges and other professional health care organisations (Bingham & Wright, 2008). In November 2013 the online networking platform My Health Skills was launched as a “platform [for members] to voice opinion,

¹⁹ E-Learning Repository: <http://www.elearningrepository.nhs.uk/>

²⁰ NLMS: <http://www.esrsupport.co.uk/nlms/index.html>

²¹ E-Learning Readiness Toolkit: <http://www.elearningreadiness.org/index.php>

²² NHS Core Learning Unit: <https://corelearning.skillsforhealth.org.uk/local/sfhadmin/login/index.php>

access relevant information, build capability and seek advice from fellow colleagues within the healthcare sector".²³ Latterly e-LfH, which became a part of Health Education England, had planned the creation of a Technology Enhanced Learning (TEL) Hub, a platform designed to be a first port of call for TEL information and resources; it was intended to launch this in 2017.²⁴ The governance structure for e-learning comprised a national E-Learning Strategy Board, the E-Learning Management Group, and the Strategic e-Learning Leads group (Ward, Sutton, Divall, & Hull, 2008). Facilities or guidance for checking the suitability of local PC infrastructure existed for some of this content, e.g. the ESR PC Check,²⁵ and e-LfH's *Technical requirements for accessing all e-Learning for healthcare products* (e-Learning for Healthcare, 2008). In September 2016, e-LfH added the e-LfH Hub to the list of OpenAthens resources to facilitate access for certain professional groups. E-learning encompasses a range of delivery methods and content types, including re-usable learning objects in various formats, virtual learning environments (VLE), learning management systems (LMS), social networking environments and tools including forums, wikis and blogs, audio- and video conferencing, e-portfolios, podcasts, video clips, online simulation and educational gaming (NHS East of England, 2009). Other than "official" NHS e-learning material, a wide range of other e-learning content existed, produced by higher education institutions, professional bodies and publishers, that NHS professionals might have wished or needed to access for professional development purposes; (Childs, Blenkinsopp, Hall, & Walton, 2005). E-learning was also widely used in the pre-registration education of health professionals, creating a need for students on placement to access such content from within NHS networks (Bilham, 2009; Clarke, 2009; Walton, Smith, Gannon-Leary, & Middleton, 2005; Ward & Moule, 2007). As well as carrying out mediated searches and information literacy training, NHS librarians had an important early role in facilitating e-learning at local level, both in terms of strategic planning and particularly through their provision of support to staff accessing e-learning material using library computers; they were well placed to report on problems with PC system or requirements and with network, authentication or usability issues (Beaumont, 2005; Childs et al., 2005; Sutton, Booth, Ayiku, & O'Rourke, 2005).

²³ My Health Skills: <https://www.myhealthskills.com>

²⁴ HEE Technology Enhanced Learning: <https://www.hee.nhs.uk/our-work/research-learning-innovation/technology-enhanced-learning>

²⁵ ESR PC Check: <http://www.esrsupport.co.uk/nlms/pccheck.html>. There were problems with this in practice: see Section 6.2 below.

1.4.7 Health informatics professions

Understanding the organisational aspects of information access issues, which necessarily involves detailed consideration of the systems and processes which support information governance and network security and which enable appropriate access to online resources, requires some background knowledge of the groups of staff who are responsible for them.

Ongoing trends towards the professionalisation of health informatics since the 1990s had been driven by the increasing importance of information systems in the delivery of health care, and, within the NHS, by the increasing importance of inspection and regulation, and the perceived priority of patient safety (Haw et al., 2006). Health informatics was widely considered to be an still-emerging profession, since it faced problems of consistent education, registration and accreditation, both in the UK and elsewhere (Lui, 2013). An umbrella body, the United Kingdom Council for Health Informatics Professions (UKCHIP)²⁶ was created following the publication of the DH document *Making information count: a human resources strategy for health informatics professions* (Department of Health, 2002b); it had the introduction of a requirement for statutory registration of health informatics workers as one of its main aims, placing them it on a par with clinical professionals.

From the perspective of inter-professional relations, information technology, information governance and library / information / knowledge work may usefully be positioned within this overall broad field. Health informatics was defined by the DH as “the knowledge, skills and tools that enable information to be collected, managed, used and shared to support the delivery of healthcare and to promote health and wellbeing” (Department of Health, 2002, p. 3). Overall it was said to be “concerned with the structures and processes, as well as the outcomes involved in the use of information and information and communications technologies (ICTs) within health” (Bath, 2008). Bath identified three main areas within the field, each of which overlaps considerably in scope with the others: medical informatics, health informatics and health information management. Other authors categorised areas within the field differently, e.g. Haw *et al.* (2006) identified six main staff groups: information and communication technology; health records; knowledge management; information management; clinical informatics; and senior managers and directors of service.

²⁶ United Kingdom Council for Health Informatics Professions: <http://www.ukchip.org>. Subsequent references are to the UKCHIP website unless otherwise stated.

The Health Informatics Career Framework (HCIF) developed by UKCHIP (2014) identified a total of eight main areas of work or career pathways within health informatics: knowledge management, information management, information technology, health records and patient administration, clinical informatics, education and training, and project and programme management. The work of health service IT staff, information governance staff and library staff was considered to belong to different pathways (information and communications technology, information management and knowledge management, respectively) within a the wider framework. Information governance was concerned with legal and ethical frameworks for the management and use of information (see 1.4.4 above), and was located within information management as a sub-specialism. Information governance staff working in the NHS were able to become members of the Institute of Health Records and Information Management (IHRIM), which supported staff working within health records, information management, and clinical coding.²⁷ The HICF mapped to other occupational standards and frameworks such as the NHS Knowledge and Skills Framework (KSF) (Department of Health, 2004; NHS Staff Council, s.d.), Skills for the Information Age (SFIA)²⁸ for information technology, and the CILIP Professional Knowledge and Skills Base (CILIP, s.d.). Other than UKCHIP, a variety of professional bodies supported different aspects of health informatics work. These included IHRIM, the British Computer Society specialist group Association for Informatics Professionals in Health and Social Care (BCS ASSIST), and the Chartered Institute of Library and Information Professionals (CILIP). In 2016, UKCHIP, BCS: the Chartered Institute for IT, CILIP and IHRIM announced their intention of creating a new federation for the health informatics profession, to be called the Federation for Informatics Professionals in Health and Social Care (Fed-IP). The proposed Fed-IP was to act as an independent single voice for the profession, and to set and maintain standards of professional competence and conduct for individuals working in health and care informatics, publishing a register of persons who had met the standards. (Federation for Informatics Professionals, s.d.)

Despite efforts to unify these bodies, the professional landscape can thus be seen to be both fragmented and contested, indicating the likelihood of conflict. Since health informatics professionals in the UK worked within an organisational environment (i.e. the NHS) that was subject to the practices of New Public Management, they participated in organisational structures that

²⁷ IHRIM: <http://www.ihrim.co.uk/>.

²⁸ SFIA: <http://scripts.bcs.org/sfiaplus/sfia.htm>

required them to work in accountable and evidence-based ways within strong frameworks of organisational control (Evetts, 2003, 2011; Hunter, 1996; Noordegraaf, 2007, 2013). While the discourse of unity within an overarching professional framework may have been influential at occupational level, the different groups were commonly in competition and conflict at workplace level (*cf.* Johannisson & Sundin, 2007). This issue is discussed further in Sections 2.5.5.1 and 11.5.

1.5 Aims and objectives of the research

The overall aim of the research was to investigate barriers to online professional information seeking, use and sharing occurring within the NHS in England, their possible effects (upon education, working practices, working lives and clinical and organisational effectiveness), and possible explanatory or causative factors.

Its specific objectives were as follows:

- 1) to establish in detail, via investigations carried out at specific sites (Section 3.3), the nature and extent of barriers to accessing to published information online within the NHS in England, related to the functionality of information technology infrastructure or from aspects of policy and practice relating to the use of information technologies;
- 2) to determine the effects that these might be having on professional information-seeking, learning and decision-making in the contexts of clinical and management practice, education and research, and the possible consequences for working practices, for working lives and for clinical and organisational effectiveness;
- 3) to investigate the norms, practices, attitudes and beliefs, values, interests and presuppositions of stakeholder groups regarding information seeking, business need and risk management which might be involved, and the influences they might be exerting on the phenomena identified in 1).

There was a need in particular to focus on investigating an apparent disjunction in the import and effects of regulatory policies and practices in different areas. On the one hand these required that NHS staff should have appropriate access to training, support, education and professional development, and to resources for the conduct and implementation of research, and that clinical and management decisions be made according to the most current best practice evidence. On the

other hand they appeared to result in restrictions on access to, use and sharing of online published information (1.2).

1.6 Research questions

The specific research questions relating to this study are as follows:

RQ1: What limitations currently exist on access to online published information to support professional development, clinical and management decision making, and research within NHS organisations arising from organisational strategies, policies and practices as they are implemented in relation to IT infrastructures and information technology use?

RQ2: What effects do these limitations have on professional information seeking, use and sharing, on the working practices and working lives of health professionals, on the education of students, and on clinical and organisational effectiveness?

RQ3: What are the organisational issues within NHS Trusts (policy drivers, legal and regulatory requirements, organisational values, cultural attitudes and presuppositions, professional norms, and practices) which bear on a) how IT infrastructure enabling access to online published professional information, including e-learning content, is managed, and b) how acceptable use policies, social media policies and web content filtering are implemented? How do these issues interact?

These three questions derive clearly from the objectives of the research as stated above. In terms of Blaikie's (2009) categorisation of types of research questions, RQ1 and RQ2 are "what?" questions, and RQ3 is a "why?" question incorporating two subsidiary questions, a "what?" question relating to the identification of organisational factors, and a "how?" question relating to their interactions. Alternatively, RQ3 may be categorised in Mason's (2002) terms as a combination of developmental puzzle and causal puzzle. In the course of the research, the focus of the questions broadened from an initial concern with information security, professional cultures and risk perception to include a wider range of organisational issues, such as staff engagement, diffusion of innovations and inter-professional conflicts.

There are particular subsidiary questions that need to be addressed in order to clarify issues that arise in consequence of the main questions:

SQ1: What technical or organisational rationales are offered for restrictions on access to information resources, or on the use of technologies supporting professional information seeking, use and sharing?

SQ2: What differing stakeholder perspectives are involved here?

SQ3: How do these stakeholders understand requirements for risk management in information security /cybersecurity and information seeking, in relation to organisational priorities and values?values?

SQ4: What issues for the accessibility of information within the English NHS are posed by current approaches to IT infrastructure management and to information security /cybersecurity risk management?

SQ5: In what ways are mobile devices (laptops, tablets, smartphones) being used by health professionals to access information?

SQ6: How do patterns of such usage relate to professional norms of behaviour?

SQ7: How is the use of mobile devices managed, technically and in policy terms? What support is available for staff using mobile devices professionally?

SQ8: How are individual and corporate uses of social media and Web 2.0 applications managed, technically and in policy terms?

1.7 Possible outcomes/benefits of the study

The purpose of the research was to shed light upon and to generate knowledge of an issue affecting NHS library services, professional educators, and e-learning leads, i.e., that of reported difficulties in gaining access to online resources for information seeking, use and sharing. The study offered a multi-faceted approach to developing a better understanding of the issues; its results were likely to have implications at all levels for professional information seeking, use and sharing, and for teaching and learning within the NHS in England, leading (it is to be hoped) to more effective strategies for improving e-resource access. It was expected also for it to suggest areas for discussion and

negotiation between NHS and higher education library and e-learning leads and those responsible for information technology infrastructure and security policies, at national and local levels.

1.8 Structure of the thesis

The thesis is structured as follows. The introductory chapter (Chapter 1) is followed by the literature review (Chapter 2) and an account of methodology and methods (Chapter 3). The findings are presented in five separate chapters covering each major theme: background and context (Chapter 4), barriers to information seeking and use (Chapter 5), education and training arrangements (Chapter 6), organisational dynamics and professional cultures (Chapter 8), communications policies and practices (Chapter 9), and summarised in Chapter 10. A discussion of the findings, together with a proposed theoretical model of the major operative factors affecting access to published information online, is offered in Chapter 11. Conclusions and recommendations for further research and for policy are presented in Chapter 12.

1.9 Summary and conclusion

This introductory chapter has provided an outline of the research project described more fully in subsequent chapters, and some necessary background on the organisational nature of the NHS and its information technology, electronic library and e-learning services. The aims and objectives of the research and the research questions have been stated. It leads on to a more detailed review of previous relevant research and theoretical frameworks (Chapter 2).

Chapter 2. Literature review

2.1 Introduction

This literature review is thematic in approach and covers the five main areas which were perceived to be most important to the research problem: information behaviour within health services; aspects of organisational culture and behaviour; information governance and security; risk management, and diffusion of innovations. It aimed to identify existing research in these areas, to inform the development and refinement of the research questions and methods, to identify gaps in the literature, and to provide an outline of frameworks or theories which were perceived as relevant to the discussion. The scope and structure are illustrated in Figure 2.1 below. An initial review was carried out to delineate the gap in the literature; this focused substantially on information behaviour, cybersecurity risk management, organisational culture, and social theories of risk. The other material on organisation theory and on the diffusion of innovations was added at a later stage following data collection, in conjunction with work on analysing and theorising the findings. The scope and structure are illustrated in Figure 2.1 below.

2.2 Search strategy

Keyword searches were conducted within relevant bibliographic databases, mainly Web of Science, Google Scholar, Scopus and Primo Central. The King's Fund library database was included in the searches for NHS-related material. Important-seeming references within relevant papers retrieved were followed up, and citation searches were conducted using these databases to identify recent material citing major reviews or particularly interesting primary studies. Where available and when a highly relevant article was found, "related articles" and "cited by" features were used to broaden the searches. The researcher registered to receive tables of contents of relevant journals via JournalTOCs,²⁹ and received notification of other possibly relevant articles via the Mendeley news feed and Google Scholar updates. She also "followed" selected other authors on ResearchGate³⁰ and received advice of their new or updated publications. In order to keep up with policy initiatives, she

²⁹ JournalTOCs: <http://www.journaltoocs.hw.ac.uk/>

³⁰ ResearchGate: <https://www.researchgate.net/home>

also registered to receive a range of online newsletters relating to health service management and health IT.

To identify studies of the information behaviour of health professionals, searches were undertaken also within OVID Embase (which includes MEDLINE records), PsycINFO, CINAHL, and LISTA, limited to 1998 and later. Core journals: *Health Information and Libraries Journal*, *Journal of the Medical Library Association*, *Journal of Information Science*, *Journal of Documentation*, *Information Research*, *Annual Review of Information Science and Technology*, as suggested by Detlefsen (1998), were hand-searched. Other relevant papers were found incidentally. The researcher was aware of Edwards *et al.*'s. (2013) study of NHS health managers' information behaviour, as she had been involved as the facilitator within her Trust for the research it described. References were managed using the Mendeley bibliography manager.³¹

Search statements for the five main areas of the review are given in Appendix A.

2.3 Scope and limits of the review

The central questions of the research relate to five main subject areas:

- 1) The information behaviour of clinicians and managers within the NHS: there was an evident need to scope the nature and extent of their information needs and use in support of clinical practice, teaching and learning, particularly in relation to online sources, in order to gauge the effects of non-accessibility of information. Information behaviour theories were evaluated in terms of possible explanatory frameworks for the effects of barriers to information seeking, use and sharing upon information behaviour (Section 2.4);
- 2) Organisational issues, including organisational culture and subcultures, professions and professionalism, the character of the NHS as an organisation, staff engagement, theories of power and of trust within organisations: these were relevant on account of the significance of professional groups and their subcultures, and of conflicts between them, in NHS organisations, the importance of information technology staff subcultures in some contexts, and the manner in which organisational issues often featured in discussions of aspects of information security (Section 2.5);

³¹ Mendeley: <https://www.mendeley.com>

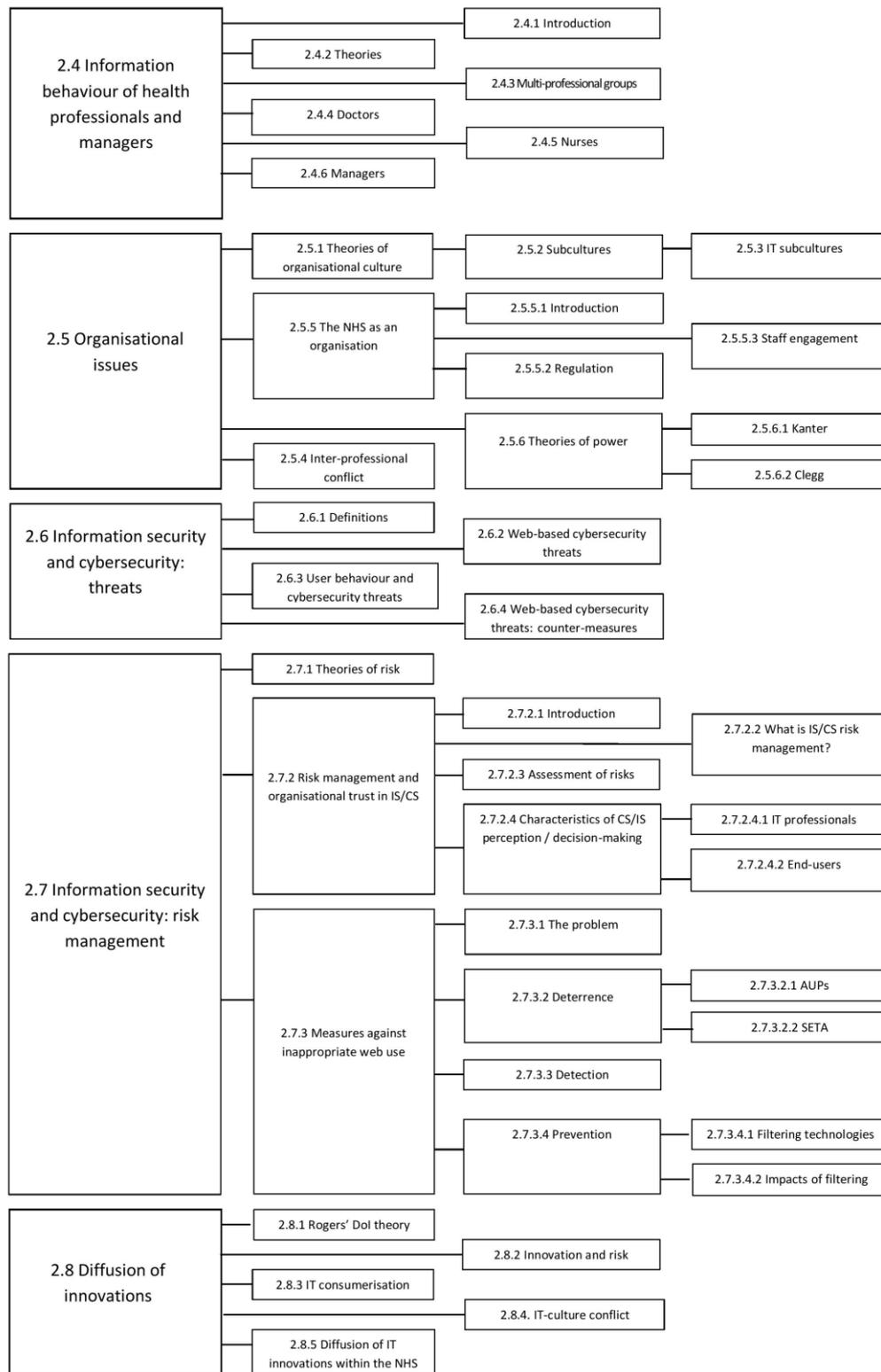


Figure 2.1 Literature review thematic map

3) The technical aspects of information security and cybersecurity management within NHS organisations: to engage in technical discussions, the researcher required a sound basic knowledge of NHS network infrastructure and of the types of security problems (particularly in relation to web applications) requiring to be addressed by NHS information technology specialists, and of the corresponding cybersecurity measures (Section 2.6);

4) Information security / cybersecurity risk in relation to access to e-resources: a more balanced understanding in this area had been called for by medical educators (Prince, Cass, & Klaber, 2010). A similar call had been made by NHS Employers in relation to access to social media applications (NHS Employers, 2013a). The researcher perceived a need to set this in the context of the main social theories of risk, and of approaches to security risk analysis and management. Two issues in particular required to be addressed: those of trust in information security / cybersecurity, and of the management of personal web use (PWU) at work in relation to organisational risks (Section 2.7).

5) Selected theoretical approaches to information technology innovation (including Rogers' theory of the diffusion of innovations, the Technology-Organisation-Environment framework, and the theory of IT-culture conflict): were potentially applicable to user-driven technological innovations such as Bring Your Own Device and individual and corporate use of social media (Section 2.8). Material in all subject areas was drawn upon in the development of the research questions. That in 1), 3) and 4) relates most closely to the "core" issues of the research; the material in areas 2) and 5) informed the development of the interview scripts and conduct of the interviews, and was drawn upon in the coding of the data and in the analysis and discussion of the findings.

The publication of *Information for Health* (NHS Executive, 1998) marked a watershed in NHS IT strategy. The material in 1) therefore covers work on health information behaviour published from this date until the present, with selective inclusion of earlier studies where these were deemed important, and exclusion (on the grounds of lack of currency) of studies published before 2003 that focused solely on use of the Internet by health professionals. It should be noted that, during the period covered by this review, i.e. 1998 to the present, the publication of journals and grey literature substantially moved online (Johnson & Luther, 2007; Mort, 2006), and online publication began to be viewed by users as "normal", hence earlier studies, while possibly providing some useful insights, cannot be relied upon to provide an up-to-date picture of information resource usage. In the later work the World Wide Web features in health professionals' perceptions, certainly as regards professional (as distinct from consumer) health literature, more as a publication platform than as a distinct information resource or entity in itself. The information behaviour of multi-professional groups (2.4.3), doctors (2.4.4), nurses (2.4.5) and health service managers (2.4.6) is considered in

some detail, primarily in respect of preferred sources and barriers. A brief account of the distinctive features of other clinical staff groups' information behaviour is offered in Appendix C.

Within the organisational culture section (2.5), summary coverage is offered of the work of influential authors on organisational subcultures, and a comprehensive treatment of work on information technology staff subcultures; no date limits for inclusion were set. Highly summative accounts are offered of Clegg's circuits of power theory (Clegg, 1989), of actor network theory, of Kanter's theory of structural power, and of organisational trust and staff engagement. The information security and web blocking sections focus on the most recent material on web content categorisation, and on web application security threats and counter-measures, drawing on professional and industry publications where suitable academic sources are not available, and focusing on current practice within the NHS. An eclectic approach was taken to the risk management literature, aiming to provide an overview of those theoretical approaches to risk which were of relevance for information security and governance; again, no date limits were set.

2.4 Information behaviour

2.4.1 Introduction and terminology

Overall, the research was concerned specifically with problems with accessing, using and sharing published information online. The term "published" in this context refers to material that has been communicated or made available publicly ("Publish", 2016). These can be broadly summarised as relating to technical, cultural and policy factors hindering, motivating or discouraging information seeking, time (or lack of it) for information-seeking, awareness of information, and perceptions of access to information, the accessibility, availability and usefulness of information, and convenience in accessing information. The term "online", in current common parlance, generally equates with availability via the Internet, or via an organisation's intranet.

It should be noted that studies of information seeking and learning by groups within professional health services indicated an increasing use overall of web-based resources on a range of mobile devices (PCs, tablets and smartphones) as well as of desktop and laptop computers (e.g. Casebourne, 2012; Davies et al., 2012; Gaglani & Topol, 2014; Mickan, Atherton, Roberts, Heneghan, & Tilson, 2014; Moore & Jayewardene, 2014; Ozdalga, Ozdalga, & Ahuja, 2012). An increasing number of clinically-relevant mobile applications (apps) were available for mobile devices using the main mobile operating systems, including point of care resources, reference sources and textbooks (e.g. Haffey, Brady, & Maxwell, 2014; Havelka, 2011; Payne, Wharrad, & Watts, 2012). A few medical

schools were using tablet computers in medical education; contemporary developments in the use of tablets in medical education were reviewed by Fan, Radford, and Fabian (2016). Within the NHS in England, some Trusts were issuing staff with mobile phones, some of which could be categorised as smartphones, on the basis of operational need. Security and permissions on these devices were managed by IT departments. There was a trend also for staff to use their own mobile devices (tablets and smartphones) for professional purposes. Their use was in some instances officially sanctioned and managed via a Bring Your Own Device (BYOD) policy (Bodhani, 2012; Patel et al., 2015; Wood, 2015). Use of these devices for information-related purposes (e.g. accessing e-books) was often supported by NHS libraries. It was relatively common for board members to be issued with iPads by their trust (e.g. “Expensive iPads go to NHS board members”, 2011; Kelly, 2014). A survey among librarians of how mobile technologies are being used, promoted and delivered within NHS settings was conducted by Chamberlain, Elcock, and Puligari (2015); this identified current trends, and also technical barriers to use (primarily inadequate network infrastructure, with some blocking of websites and applications). No comprehensive discussion was possible within this literature review of all the relevant issues relating to the use of mobile devices in health care, although they are mentioned again briefly in Section 2.8.2 within the discussion of user-driven innovations and “shadow IT”. Encryption requirements for mobile devices are discussed in section 1.4.4, and infection control issues in Appendix H.

The term “Web 2.0”, while difficult to define in precise terms, is commonly given to a second generation of the World Wide Web that is focused on the ability for users to collaborate with each other and to create, upload and share information online; the term refers to a transition from static websites to a more dynamic web environment that is based on serving web applications to users (O’Reilly, 2005). McGee and Begg’s definition (2008) may serve: “A collection of web-based technologies ... where users actively participate in content creation and editing through open collaboration between members of communities of practice”. Applications such as start pages (portals), mashups, folksonomies and podcasting are examples of Web 2.0 applications. Web 2.0 is said to reflect an egalitarian and unstructured approach which is fundamentally different from those of “traditional” IT, being readily accessible, relatively easy to use, and also free of the imposed structures (such as workflow, interdependency and decision right allocations) which are associated with traditional information technologies (Singh & Chandwani, 2014, citing McAfee, 2009). The concept may be broadened to serve as a conceptual frame for describing developments within the World Wide Web as a whole (Allen, 2008).

Social media constitute a subset of Web 2.0 applications. They “[involve] the explicit modeling of connections between people, forming a complex network of relations, which in turn enables and facilitates collaboration and collaborative filtering processes.” They may enable users to see what other connected users are doing; enable the automated selection of “relevant” information; enable reputation and trust management, accountability and quality control; foster the “viral” dissemination of information and applications; and provide “social” incentives to enter, update, and manage personal information (Eysenbach, 2008). Kaplan and Haenlein (2010, p. 61) define social media as follows: “A group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content”. An alternative definition was proposed by van Osch and Coursaris (2013, p. 703): “Social media are technology artefacts, both material and virtual, that support various actors in a multiplicity of communication activities for producing user-generated content, developing and maintaining social relationships, or enabling other computer-mediated interactions and collaborations”. Having considered other possible alternative typologies (Anderson, Hepworth, Kelly, & Metcalfe, 2007; Dalsgaard & Sorensen, 2008; El Ouiridi, El Ouiridi, Segers, & Henderickx, 2014), Kaplan and Haenlein’s influential (2010) categorisation of Web 2.0 and social media types, which is both detailed in respect of the applications it includes and very general in scope, was used in analysing and presenting the results (Section 5.5).

According to Husin and Hanisch (2011), corporate decision makers initially tended to perceive social media and Web 2.0 applications purely as recreational or time-wasting; however McAfee’s advocacy of the use of Web 2.0 applications for organisational knowledge management (McAfee, 2006, 2009), was influential in creating a more positive view.. Social media use within, and the social media policies of, hospitals in the United States and continental Europe (Barnett, Jones, Bennett, Iverson, & Bonney, 2013; Cain, 2011; Eysenbach, 2008; Fast, Sørensen, Brand, & Suggs, 2015; Gagnon & Sabus, 2015; Hamm et al., 2013; Henry & Webb, 2014; Hughes, Joshi, & Wareham, 2008; Koh et al., 2013; Munson, Cavusoglu, Frisch, & Fels, 2013) and within academia generally (Doherty, Anastasakis, & Fulford, 2009; Pomerantz, Hank, & Sugimoto, 2015) have been widely studied, as has the use of social media within health sciences professional education (Gualtieri, Javetski, & Corless, 2012; Hall, Hanna, & Huey, 2013; Hanson et al., 2011; Juricich, 2014; Oakley & Spallek, 2012); cf. Section 2.7.3.2.1. There have been relatively fewer UK-based studies (Anderson & Speed, 2010; Boulos & Wheeler, 2007; Hughes, 2010; Moorley & Chinn, 2014; Scragg, Shaikh, Shires, et al., 2017; Scragg, Shaikh, Robinson, & Mercer, 2017; Thomas, 2013; Ward, Moule, & Lockyer, 2009).

The systematic review of research on the uses of social media in pharmacy education conducted by Benetoli, Chen, and Aslani (2014) found that many studies were descriptive in nature, with no controlled studies being conducted. Another systematic review, by Moorhead *et al.* (2013) identified seven main uses of social media for health communication by professionals: providing health information on a range of conditions; providing answers to clinical questions; facilitating dialogue with other professionals and with patients; collecting data on patient experiences and opinions; use in health education and promotion; reducing stigma; and providing online consultations. The main benefit of social media use was identified in this review as the generation of peer-to-peer discussion. Limitations included issues of privacy, confidentiality and information quality. An earlier literature review of uses of social media applications within medical and health sciences education by Paton, Bamidis, Eysenbach, Hansen, and Cabrer (2011), while recommending their use, was unable to find clear and specific evidence for their effectiveness.

2.4.2 Theories of information behaviour

The terminology used within these studies requires some clarification. Following Wilson (1997, 1999) and widespread subsequent usage (Pettigrew, Fidel, & Bruce, 2001; Li & Belkin, 2010), the researcher employs the term “information behaviour” to mean “those activities a person may engage in when identifying his or her own needs for information, searching for such information in any way, and using or transferring that information”, including within its scope the more specific concepts of “information need”, “information-seeking behaviour”, “information search behaviour” and “information use”. “Information need” in the context of the work environment and of professional activities relates to task, and has two separate aspects, firstly “the awareness of an individual that they are experiencing an uncertainty which requires a ‘stimulus’ or piece of information in order to resolve that uncertainty”, and secondly the need for the individual to be equipped to recognise the existence of their uncertainty (Ford & Korjonen, 2012, p. 261). Work on health professionals’ information behaviour frequently refers to one or more of the established theoretical models. Wilson’s models of information behaviour (Allen & Wilson, 1998; Järvelin & Wilson, 2003; Wilson, 1981, 1997, 2006; Wilson & Walsh, 1996) have been highly influential generally within information behaviour studies. Wilson’s updated model (1997; 1999), shown in Figure 2.2 below, suggested that information seeking behaviour is influenced by contextual factors that he termed intervening variables. These had been referred to as “barriers” in his second 1981 model (Wilson, 1981). Intervening variables may be “supportive of information use as well as preventive” (1999, p. 256) in their effects. According to the model they may be psychological, demographic, role-related or interpersonal, and environmental in nature. The external

environmental variables specifically considered by Wilson include geography, national cultures, and economic constraints (time, the direct costs of information seeking) as well as information source characteristics, which include accessibility (1997, p. 557).

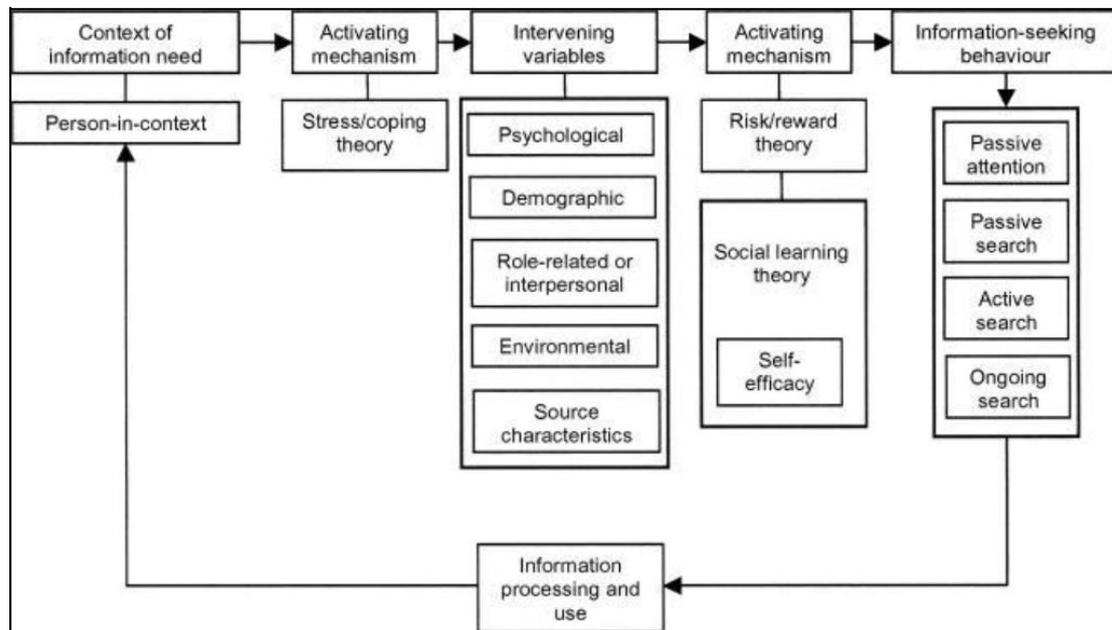


Figure 2.2 Wilson's updated model of information behaviour

Wilson, 1999, p. 257

Reproduced by permission

Wilson (Wilson & Walsh, 1999, p. 253) had expressed criticisms of his own earlier model of 1981: " ... [there is no] indication ... of the factors that result in the perception of barriers, nor of whether the various assumed barriers have similar or different effects upon the motivation of individuals to seek information". His later model (Wilson & Walsh, 1996) introduced a variety of theories to address these deficiencies; however he has nothing to say about non-accessibility of information as a source characteristic and its effects on information seeking other than that "the lack of an easily accessible source may inhibit information-seeking altogether" (Wilson, 1997, p. 561).

The concepts of "bounded rationality" and "satisficing" (Simon, 1956) are relevant to the study. Bounded rationality theory suggests that, faced with circumstances requiring a decision, people's rationality is limited by the nature of the problem faced, their own cognitive limitations, and the time and attention they are able to devote to the issue; thus, they are "rational enough", or "partly rational", rather than being "absolutely rational" (Pomeroy & Adam, 2008). It is common for people faced with shortages of time, with information overload, or with uncertainty, to employ a "least

effort” information processing strategy, using only those resources that they consider sufficient for a “good enough” outcome in the specific context and physical constraints such as of the information need; this constitutes satisficing (Prabha et al., 2007). Agosto (2002, cited by Mansourian & Ford, 2007) suggested the following behavioural categories in relation to information seeking: for bounded rationality, time constraints (external or self-imposed), information overload, required effort, physical or mental fatigue levels; for satisficing, strategies of reduction (confining the search to known sites, using synopses, or categorising searches) and termination (“stop rules”, i.e. when to stop a search). Such “stop rules” can involve acceptance, fatigue, boredom and time constraints. Satisficing behaviour in information seeking by health professionals and students has been described by O’Leary and Ni Mhaolrúnaigh (2012) (Irish nurses), O’Carroll, Westby, Dooley, and Gordon (2015) (Canadian medical students) and Grant (2007, cited by MacDonald, 2011) (Canadian health service managers). It is readily apparent that non-accessibility of information can be a contributory factor to sub-optimal outcomes in “satisficing” behaviour relating to professional information seeking: people will look for alternative less suitable sources, or just do without the material that is unavailable.; compare the discussion in Section 11.3.2).

Fourie and Claasen-Veldsman (2011) suggest that the concept of *information source horizon* is relevant to clinicians’ information behaviour. An imaginary field is posited in which the information seeker selects and positions information sources at different distances according to perceived relevance, accessibility, and quality. A horizon line indicates the outermost boundary of the field of interest; this is the information source horizon (Sonnenwald, 1999). Such horizons are created within the broader context of a perceived information environment, i.e. a set of information sources and channels which the information seeker is aware of and may have used in the past. Judgments as to how resources are positioned may be based on general values, past experiences; the views and attitudes of teachers, supervisors and peers; the situational demands of information-seeking; the content of information need; and perceived accessibility and quality of the resources. It is evident that such information source horizons will govern information seeking strategies, since they suggest which sources should be preferred or avoided (Savolainen & Kari, 2004).

2.4.3 Multi-professional studies

The multi-professional studies based in specialist services examined for the literature review (see Table B.1 below in Appendix B) indicated wide variations in access to and use of the Internet and in preferences for the types of resources consulted. Overall, the findings represented a pattern of moderate online information resource usage. Categories of information need and preferences for

different types of online resource (databases, e-journals, e-books, and professional websites) varied widely by professional group. Doctors were shown to be more inclined to use online resources than nursing or allied health staff. Use of the Google search engine was high among all groups. Obstacles to information-seeking were cited in many of these studies. Shortage of time to carry out searches, and lack of training in methods of effective searching, were the issues that appeared to loom largest; shortages of computer facilities, lack of management support for information seeking, and lack of information resources were also mentioned.

2.4.4 Studies of doctors

Detailed typologies specifically of doctors' information needs are offered by Gorman (1995), Smith (1996), Ebell and Shaughnessy (2003), Florance (1992) and Allen et al. (2003). Information needs within primary care and clinical specialties can be said to fall into two broad categories: keeping up to date with current research, and answering questions arising in the course of clinical contacts with individual patients. Davies (2011a) described the information needs of doctors as relating to 1) diagnosis, 2) treatment options for common diseases, 3) information on rare diseases and syndromes, 4) drug information, 5) information to give to patients; 6) information for study for further qualifications, 7) continuing professional development, 8) research, and 9) teaching.

Doctors' level of access to the Internet can now be presumed to be universal (e.g. Davies, 2011a, 2011b). The 2012 Elsevier survey of European physicians (cited by Walmsley, 2012; n=1093) found that use of mobile devices (smartphones, tablets) for professional purposes was widespread and increasing. Use of mobile devices may serve to alleviate the time issues that have been identified as a barrier to information-seeking (Davies, 2011a).

The ever-increasing size of the biomedical literature, combined with the acute time pressures of clinical practice, inevitably creates information overload and major difficulties for clinicians in managing information, particularly within primary care, and in following the precepts of evidence-based medicine (Gorman, 2001; Slawson & Shaughnessy, 2005; Smith, 2010). The volume of biomedical research doubles every 20 years (Wyatt & Sullivan, 2005). The use of pre-appraised synthesised evidence sources, and an exclusive focus on "patient-orientated evidence that matters", employing a stringent calculus of usefulness, have been advocated as an alternative to the classic evidence-based medicine process of critical appraisal of the primary literature (Ebell & Shaughnessy, 2003). Information needs may, of course, not be recognised. Estimates of the numbers of questions

generated in clinical practice vary considerably; a finding of two questions for every three patients, however, is typical (Booth, 2005).

For the purposes of this study, which focused on barriers to information seeking and use, it was important to consider the following background questions:

- 1) What leads an individual doctor to decide to pursue a question or not?
- 2) What proportion of questions goes unanswered, and what negative impact do unanswered questions have on the quality of clinical care?
- 3) What is the mean time allocated or available to answer each clinical question?
- 4) What effects might barriers to information seeking have on the processes of clinical information seeking and use? Are they a contributory factor in clinical questions going unanswered?

Studies of doctors' source preferences for clinical information seeking are summarised in Table 2.1 below. Booth (2005) suggested that as much as one-third of the total number of clinical information needs may go unrecognised. Del Fiol, Workman and Gorman (2014, p. 712-713) suggested as a conclusion from their systematic review that "Clinicians have many questions in practice—at least 1 for every 2 patients they see, and although they find answers to most (78% to 87%) of the questions they pursue, more than half of their questions are never pursued and thus remain unanswered." The only two significant factors in motivating a doctor to pursue information relating to a clinical question were found to be the belief that a definitive answer existed, and the urgency of the patient's problem (Gorman & Helfand, 1995). Strangely, the generalisability of the answer to other patients was a negative predictor of information-seeking. Other factors, such as the difficulty of finding the answer, potential harm or help to the patient, or self-perceived knowledge of the issue, were not significant.

The direct impact of questions going unanswered upon patient care is difficult to establish. Attempts have been made, however (e.g. by Schilling, Steiner, Lundahl, & Anderson, 2005), to demonstrate the positive impact upon patient care of answered questions, while Westbrook, Coiera and Gosling (2005) discussed studies of the impact of online clinical evidence on clinical practice. Bonis, Pickens, Rind, and Foster (2008) showed improvements in patient safety, reduced complications and shorter length of stay among patients in hospitals in which access was available to the point of care resource, UpToDate®, although it was unclear whether the effect was directly causative. Farnan, Johnson, Meltzer, Humphrey, and Arora (2008) reported substantially negative outcomes of unanswered questions: they analysed the impact of uncertainty in clinical decisions made by medical

residents while on call. Of the reported 18 incidents, 12 involved compromises to patient care: delays in procedure or escalation of care (n=8), procedural complications (n=2) and cardiac arrest (n=2).

The relative merits of Google as a diagnostic aid have been the subject of discussion (Johnson, Chen, Eng, Makary, & Fishman, 2008; Lowes, 2007; Sim, Khong, Jiwa, & Moyez, 2008; Tang & Ng, 2006). The significance for the present research of the use of general search engines for information-seeking is in the heterogeneity of the search results and lack of an overt quality filter. Anecdotal evidence suggested that YouTube was blocked within many NHS Trusts, and that bandwidth on NHS networks could be insufficient to support extensive use of online video. Hughes, Joshi, Lemonde, and Wareham (2009), in their study of online information use by junior doctors in the UK, suggested that 53% of the information they used was Web 2.0 content.

Technical obstacles to information seeking featured only very briefly in these studies, and were usually not described in detail. The main obstacles to information seeking were usually cited as lack of time, information overload, lack of sufficiently specific information, and lack of search skills. Bennett *et al.* (2006) found that the typical barriers participants encountered were difficulty downloading information (24.2%, n=2,385), system too slow (18.2%), too much information to scan (40.8%), and specific information not available (53.4%).

The only specific mention of blocked websites found was that of Hughes *et al.* (2009, p. 651): "Improved access to sites was requested. This concern was not an issue of terminal availability, but the fact that ubiquitous sites such as Google were often blocked based on the policies of the hospital or clinic in question." This was non-specific in detail, but indicated the blocking of online resources that were considered important .

Reported figures for the mean time allocated or available to answer each clinical question vary widely according to context and to the resources available, ranging between less than two minutes (Ely *et al.*, 1999) to 15 minutes (Ramos, Linscheid, & Schafer, 2003).

Authors / Date / Country	Researchers' background	Research subjects	Methods/ coverage	Research focus	Findings: preferred sources
Coumou and Meijman 2006 Netherlands Papers from US (13), UK (4), Netherlands (3), Australia (4), New Zealand (1)	General practitioner, clinical academic	Studies using questionnaires, observation, and interviews (18); qualitative (1) and comparative (2) studies; and reviews (3) (n=21)	Systematic review	Changes in patterns of clinical problem solving by primary care physicians between 1992 and 2005 Search strategies used? Time spent on them? Evaluation of search activities and information sources?	Accessibility rather than quality a major determinant of which sources are chosen Patterns of clinical information seeking not fundamentally altered in character over the period in question
Bennett et al. 2006 USA	University – based researchers, medical educators	US-based doctors across all specialties	Survey (n=2,200) Structured interviews with exercises (411)	(1) How and when physicians pose problems and raise questions that require information as part of reflective practice (2) whether setting influences patterns of Internet information-seeking (3) How barriers to information seeking influence reflection, (4) change in information behaviour since 2001 and 2003	<i>Preferred sources:</i> E-journals (35.5%, n=2,364) Professional association websites (27.3%) Point-of-care databases (25.1%) CME resources (9.2%) Colleagues via email (2.9%) Consultation with colleague often a first preference <i>Facilitators of Internet searching cited:</i> Knowing preferred sites (59.8%) Access within the clinical setting (53.2%) Effort to improve and refine search skills (36.8%) Available technical support (12.5%) Protected time for searching (7.4%)

Authors / Date / Country	Researchers' background	Research subjects	Methods	Research focus	Findings: preferred sources		
Parekh, Mayer and Rojowsky 2009 USA	Market researchers working for Google	General practitioners, endocrinologists, psychiatrists, cardiologists	Online survey incorporating search exercises based on clinical scenarios, interviews (n=411)	Understand how physicians use the Internet in clinical practice: 1) Outline how physicians use search 2) Determine the impact of online searches 3) Evaluate physicians' perceptions of the Internet	Web is major source of health information; 86% had used for professional information; 78% used online CME courses 77% peer-reviewed journals 77% pharmaceutical sales representatives 76% colleagues 56% books 54% health-related organisation 35% magazines 20% videos / DVDs Search engines the top online resource – 81% used (92% Google, 13% Google Scholar)		
Google / Manhattan Research 2012 USA.	Market research company / web search company (anonymous)	Practising doctors	Online survey with supplemental interviews (n=506)	Reassess physicians' digital adoption across devices and media channels, and ascertain their use and resulting impact	Online resources (search engines, professional websites, drug references, mobile applications) used twice as much as print (journals and reference materials) Search engines main online resource Online video widely used for professional updating – mean 3h/wk – main platforms Medscape (67%), YouTube (44%)		
Davies 2011 UK	USA-based LIS academic	Hospital specialists GPs	Online survey (n=636)	Information needs of doctors Clinical question answering Use of computers Preferences in locating evidence Perceived barriers for accessing electronic information to support clinical decision making	<i>Preferred sources</i>		
						<i>Hospital</i>	<i>GP</i>
					Colleagues	2 nd	1 st
					EBM resources	4 th	3 rd
					F/T e-journals	1 st	4 th
					Other health professionals	5 th	5 th
					Hard copy textbooks or journals	3 rd	2 nd

Table 2.1. Doctors' preferred sources for information seeking

The evident lack of time available highlights the importance of filtered evidence sources such as Map of Medicine³², TRIP³³, UpToDate^{®34} and DynaMed³⁵; it also throws into relief the effect of other obstacles, in particular system slowness and blocking of websites. It is clear from these findings that, if an information need cannot be satisfied within the available time “window”, it will very likely remain unmet. This issue is discussed further in Section 11.3.2.

2.4.5 Studies of nurses

Nurses are numerically by far the largest group of health care professionals, but, while the body of nursing research has grown substantially since the 1980s (Carrion, Woods, & Norman, 2004), nurses’ information behaviour has not received the same attention from researchers as that of doctors. Studies have focused more on hospital nurses rather than on nurses working in primary care settings (Randell, Mitchell, Thompson, McCaughan, and Dowding, 2009). Only one substantial literature review was found, that of Spenceley, O’Leary, Chizawsky, Ross, and Estabrooks (2008). All registered nurses had a professional duty to keep their skills and knowledge up to date and to underpin their practice with research evidence (Department of Health, 1999; Nursing and Midwifery Council, 2015, 2011).

Information about nurses’ access to and use of the Internet is relatively sparse. The general assumption in recent information behaviour studies is that Internet access, at least in principle, is universal. Nurses require to access professional information to answer questions that arise in clinical practice and to update and extend their professional knowledge, and consumer health information to provide or to discuss with patients and families, since patient education is an important aspect of nursing work in many contexts (Anderson & Klemm, 2008; Gilmour, Huntington, Broadbent, Strong, & Hawkins, 2011; Gilmour, Scott, & Huntington, 2008; Jones, Schilling, & Pesut, 2011). As in the studies of doctors’ information behaviour, research has focused mostly on the clinical decisions made by nurses as indicators of information need, which may not do justice to the exigencies of nursing work and resulting complexities of clinical uncertainty and information-seeking in nursing (French, 2006), or of implementing evidence-based practice in context (Rycroft-Malone, 2008; Scott, Estabrooks, Allen, & Pollock, 2008; Scott-Findlay & Golden-Biddle, 2005).

³² Map of Medicine: <http://mapofmedicine.com/>

³³ TRIP: Turning Research Into Practice: <https://www.tripdatabase.com>

³⁴ UpToDate[®]: <http://www.uptodate.com/home>

³⁵ DynaMed: <http://www.dynamed.com/home/log-in>

Estabrooks *et al.* (2005) found that nurses categorised information sources in four broad groupings: social interactions, experiential knowledge, documentary sources, and *a priori* knowledge. They discovered that nurses tend to prefer interactive and experiential sources of knowledge over more formal sources such as journal articles and texts. Studies of nurses' information behaviour (e.g. Cogdill, 2003) generally report a preference for human information sources. Thompson *et al.* (Randell *et al.*, 2009; Thompson *et al.*, 2001a, 2001b; Thompson *et al.*, s.d.; Thompson, Cullum, McCaughan, Sheldon, & Raynor, 2004) found in 180 hours of observation involving 1080 clinical decisions that only two forms of text-based information were used: local protocols or guidelines (four times), and the British National Formulary (50 times). Library use among the nurses within the services they investigated was almost exclusively associated with continuing professional development or formal education. Librarians were not perceived as accessible, although the information literacy training they provided was in heavy demand. The nurses tended to use sources they knew and trusted, regardless of the nature of the problem or clinical decision involved. In their survey based in two English hospitals, Marshall, West & Aitken's finding (2011) of a "pervasive oral culture" (p. 232) is typical: a preference for colleagues as information sources as being most useful and accessible, and a rejection of the possibility of using electronic resources owing to lack of time. The perceived usefulness of information appeared to be premised on ease of use and access rather than on accuracy and completeness.

Nurses' lack of access to information may reflect processes of social exclusion and disempowerment within clinical settings, relating in particular to the location of computers on the wards (Adams, Blandford, & Lunt, 2005; Adams & Blandford, 2002b, 2001). These researchers, who investigated digital library implementation within a large London teaching hospital, also found that many senior staff members perceived the Internet as a threat to their status, as providing open access to information sources while offering the potential for misuse (i.e. non-work-related use). "Although digital libraries do not deal with sensitive personal information, apparently innocuous data can also be perceived as a threat to social and political structures" (Adams, Blandford, & Lunt, 2005, p. 179). Senior staff members also expressed information literacy concerns regarding open access to information sources, and tended to think of computers as supporting research, and therefore not necessary on the wards. The influences of workplace cultural factors on information-seeking to promote evidence-based practice, particularly the importance of fostering a positive climate for learning and growth, and the encouragement of staff input into practice change, were emphasised

by Bertulis and Cheeseborough (2008), Bond (2009), Gifford and associates (Gifford, Davies, Edwards, Griffin, & Lybanon, 2007) and Veeramah (2004).

Lack of time to search for information while at work is reported as the most significant barrier to nurses' information-seeking in virtually every study that has been examined (e.g. Dee & Stanley, 2005a; Dee & Stanley, 2005b; Gerrish, 2006; Gilmour, Huntington, Broadbent, Strong, & Hawkins, 2011; Jones, Schilling, & Pesut, 2011). Nurses' work is highly pressurised in nature, particularly in an era of financial stringency and inadequate staffing levels. Respondents in the 2004 Royal College of Nursing information needs survey (Bertulis & Cheeseborough, 2008) reported needing protected time to study. Staff may be unable to leave their clinical area to visit a library or to use computers elsewhere (Gosling, Westbrook, & Spencer, 2004). The perception of lack of time for information-seeking may be associated with negative attitudes to computers: the view that use of information technology does not form part of "proper" nursing, "hands-on" patient care being the priority (Blair, 2006; Bond, 2009; Carney et al., 2004; Farmer, Richardson, & Lawton, 1999; Gerrish et al., 2006; Gilmour et al., 2011; MacIntosh-Murray & Choo, 2005). Staff may experience conflict between using the Internet and providing clinical care (Eley, Fallon, Soar, Buikstra, & Hegney, 2009; Estabrooks, O'Leary, Ricker, & Humphrey, 2003; McKenna & McLelland, 2011). Thompson, O'Leary and Jensen (2008) suggest that nurses who complain of lack of time to utilise research are actually referring to a "culture of busyness" within nursing (p. 544) and to the mental time and energy needed to reflect on, plan and apply research results within complex environments. However, it is thought possible (e.g. Doran et al., 2010; Honeybourne, Sutton, & Ward, 2006) that use of mobile devices could offer an effective way of improving the accessibility and uptake of evidence-based practice information in a time-poor environment.

A number of recent British studies (Callaghan, Doherty, Lea, & Webster, 2008; Raynor, 2009; Shaw & Lloyd, 2013) discuss the information needs and use of nursing and other health care students on placement. Participants in Shaw and Lloyd's (2013) survey reported difficulties in accessing information resources within clinical areas caused by inability of students to obtain Trust network logins or by shortages of computers. They also reported problems with lack of Wi-Fi access in student residences, requiring students to purchase their own mobile Internet solutions (i.e. dongles) using public networks. It was apparent from the findings that students' access to Trust computing facilities depended substantially on local Trust policies, notwithstanding all the efforts made by university and Trust library services to ensure equitable and timely access to information resources. The findings of Moule, Ward, and Lockyer (2010), who investigated the adoption of e-learning in

health sciences education, were similar regarding access to information resources within clinical areas. Health professional participants in the study of information skills training and mediated searching by Brettle, Hulme, and Ormandy (2007) reported “slow networks or lines” and lack of access to computers as barriers to search activity, partly on account of the lack of time available to conduct searches.

Blocking or limitation of access to the web was referred to in a number of studies, although the information given was often insufficiently specific to be useful. Apart from actual blocking of access, slow Internet speeds and restricted access to computing facilities for nursing staff and students were reported. A general picture emerged of limited computer access, “protective” attitudes towards computer facilities on the part of some staff, and negative attitudes towards Internet use in the course of clinical work (Duffy, 2000; Raynor, 2009; Westerman and Hurt, 2007).

2.4.6 Studies of health service managers

Health service managers constitute a heterogeneous group, which includes substantial numbers of clinicians with management responsibilities, sometimes referred to as “hybrid” managers, and both specialist and general management roles. Their work is diverse, covering a wide range of strategic, policy and operational matters (Green, 2011). Their attitudes and behaviour relating to information seeking are of particular interest; they not only involve their own work, but may also, via their influences in the shaping of workplace cultures of information seeking and evidence-based practice, substantially influence other professional groups’ access to published information; *cf.* the discussion in Section 2.4.5 above.

It is assumed for present purposes that this group have access to the Internet at work via desktop or laptop computers. It is suggested that the questions of interest for the purposes of the research are as follows:

- 1) What level of priority do they accord to “evidence-based” management practice and decision-making?
- 2) What are their preferred sources of information?
- 3) What problems or barriers do they encounter in finding and using information?

There have been relatively few studies of the information behaviour of health service managers from a LIS perspective. Other than MacDonald’s work, carried out in Canada (MacDonald, Bath, & Booth, 2008; MacDonald, Bath, & Booth, 2011; MacDonald, 2011) only the work of Niedźwiedzka

(2003) in Poland, of McDiarmid, Kendall, and Binns (2007) again in Canada, and the highly detailed study by Edwards et al. (2013) involving NHS managers in England, appeared directly relevant. According to Walshe and Rundall (2001, p. 441), “the managerial culture is intensely pragmatic, and values the application of ideas in practice more than it does the search for knowledge about those ideas. Managers ... are sometimes actively suspicious of the motives and values of research and researchers”, and thereby neutral or antagonistic towards the ideas of evidence-based practice.

Edwards *et al.*'s (2013) study indicated a wide diversity of habits and patterns of information resource use (internal, external, “academic”) by job role and type of work. (The extent to which each type of source is used is important in considering access to information, since external and academic information are most likely to be found online.) Explicit information need was associated with involvement in strategic planning, as were high-priority tasks, new tasks or high-risk tasks. Online sources of external information, such as search engines and “official” websites (NICE/NHS Evidence, the former DH website, etc.) and also internal sources (policy documents, etc.) were heavily used. Other people (own staff, experts, colleagues, peers in other organisations) were also extensively used and consulted. Generally, relatively low use was made of formal information sources and services such as health care libraries, bibliographic databases, books and journals, although a correlation was demonstrated between use of “academic” sources and level of education, with those with postgraduate degrees being the most likely to use such sources. A considerable amount of information sharing and knowledge brokering took place, thereby facilitating understanding of other groups’ professional cultures (Lomas, 2007). Meetings, conference and workshops provided important information channels. The respondents’ rating of attitude statements indicated a preference for summaries of research, practical demonstrations or “what works” (*cf.* the comment of Walsh and Rundall (2001) quoted above regarding the intensely pragmatic nature of health service management culture), and the perception of a strongly “political” aspect to decision-making. Some differences were identified between NHS Trusts in the degree to which the culture supported information seeking and use. However, there was little evidence to link these with measures of Trust organisational performance.

Significant barriers to information access and use by health service managers have been identified. Respondents in Edwards et al.’s study (2013) referred to lack of time (most important), information overload, lack of a central source of NHS information, delays in cascading information from the DH, “slow computers and out-of-date software” (p. 110), difficulty in searching for information resulting from lack of organisational stability within the NHS (NHS bodies keep disappearing or changing their

names), and the difficulty of understanding and applying academic research (least important). The majority of respondents were generally of the opinion that it was difficult to find information.

2.4.7 Summary and synthesis

This section has provided an outline of selected theories of information behaviour. It has also offered an overview of studies of the information behaviour of selected groups of health professionals: doctors, nurses, and managers. A high level of heterogeneity was apparent in health professionals' information behaviour between professional groups, within professional groups in different job roles, and between comparable groups within different organisations. There were also differences in levels of access to information. Wide differences between professions in attitudes to information-seeking, and cultural attitudes to evidence-based practice, appeared to explain much of this variation. While time factors in information-seeking were frequently discussed indirectly, as in the many references to lack of time, and the comparative accessibility and convenience of online resources, very little direct consideration was given in the reported studies to time frames or degrees of urgency in seeking information; the work of Reddy and Dourish (2002) was an exception. This represents a research gap in an area related to the present study; without a wider range of studies being available that address time frames or degrees of urgency in information seeking, it is difficult to evaluate the impacts of barriers, in which time appears to be a major factor. Technical obstacles, including blocking of websites, slow network and Internet speeds, and (in the case of nurses and nursing students) restricted access to computing facilities were referred to in a number of studies (see 2.7.4 below), although the information given was often lacking in specific detail.

As discussed in Section 2.4.6 above, Edwards et al. (2013) were able to demonstrate correlations between attitudes to information seeking and approaches to information seeking in general, and use of external academic sources of information in particular, among health service managers. Evidence was also found of negative attitudes to information seeking and to the Internet as a root cause of the problems of nurses, allied health professionals and nursing students on placement in securing access to computer facilities (Adams & Blandford, 2001, 2002; Raynor, 2009; Ward & Moule, 2007; Westerman & Hurt, 2007). Anandarajan, Paravastu and Simmers (2006) identified and described what they termed a "cyber-bureaucrat" profile of viewpoints in relation to personal web use at work (PWU), characterised by an emphasis on its possible adverse consequences, and on the need to exert managerial control it via technical methods, policies and monitoring. Such a profile appears to characterise accurately the attitudes described above, and appears generalisable to web use of any sort, not only PWU.

2.5 Organisational cultures and subcultures

2.5.1 Theories of organisational culture

Organisational culture is a complex and contested subject within organisation studies (Martin, Frost, & O'Neill, 2006; Smircich, 1983). There is no agreed definition of culture within the field of social anthropology; it is no surprise, therefore, that organisation theorists have taken up different concepts of culture from anthropology (Smircich, 1983) and that there is little agreement on definitions of organisational culture. The definition of Schein (1996) is the best known, and the most widely cited by information security specialists. His definition focuses on basic tacit assumptions: "how things are done around here" (p. 11). A longer version is as follows: "A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." (Schein, 1992, p. 12, cited by MacIntosh-Murray & Choo, 2005). In this model, organisational culture operates at three levels: of deep tacit assumptions; of espoused values and the norms that derive from them; and of day-to-day behaviour and artifacts. Basic assumptions are taken for granted and therefore invisible; values and norms are more recognisable, particularly when they are challenged, but may remain hidden and unconscious (Kolkowska, 2011); artifacts are visible, but often indecipherable. Organisational culture may be reflected in organisational structure, control systems, and power structures (Johnson and Scholes, 1993, cited by Nord & Nord, 2007).

2.5.2 Occupational cultures and subcultures

It is easier than with the concept of organisational culture to offer a working definition of subculture. A subculture, according to Hatch (2006, p. 176), is "a subset of an organization's members that identify themselves as a distinct group within the organization and routinely take action on the basis of their unique collective understandings". Subcultures may reflect shared professional, gendered, racial, ethnic or occupational identities as well as national or regional cultural influences. The existence of subcultures can create "silos" and barriers to communication and effective teamwork (Van Maanen and Barley, 1984, cited by Hatch, 2006). Occupational communities represent a particular type of subculture; according to Van Maanen and Barley, 1984, cited by MacIntosh-Murray, 2006), they are:

“ ... groups of people who consider themselves to be engaged in the same sort of work; whose identity is drawn from the work; who share with one another a set of values, norms and perspectives that applies to but extends beyond work-related matters; and whose social relationships meld work and leisure” (p. 364).

Occupational cultures relate to distinctive clusters of ideologies, beliefs, cultural forms, and practices; they arise from shared educational, personal and work experiences of individuals who pursue the same profession. Such cultures transcend organisational boundaries (Trice, 1993). Subcultures differ from the organisational culture in which they are embedded; they may intensify aspects of the predominant organisational culture or diverge from it entirely. Differences among occupational subcultures can lead to organisational conflict and dysfunction (Trice, 1993). A number of “signs” indicate the character of an occupational subgroup: ethnocentrism and feelings of superiority related to other groups; the use of esoteric knowledge; being subject to extreme demands; and complaints about members of other subcultures (Trice, 1993).

2.5.3 Information technology staff subcultures and attitudes

Several studies exist of putative information technology staff subcultures. With the intention of identifying the nature of the IT staff occupational subculture, and the extent to which subcultural conflict was contributing to dysfunction within the host organisation, Guzman et al. (2004) undertook semi-structured interviews (n=121) with information technology (IT) staff, end-users and managers across eight small to medium-sized non-profit-making organisations of different types, located in the United States. They found indications that IT staff formed a distinctive occupational subculture: within the responses, consistent with Trice’s claims about occupational cultures (see above, section 2.3.2), were evidence of esoteric knowledge (e.g. maintaining a system single-handedly), extreme demands (heavy workloads and unsocial hours), and complaints about end-users. The researchers also identified characteristic symbols (typical settings, unique vocabulary, and stories) and a marked ethnocentrism: feelings of superiority reinforced by the technical vocabulary of IT, and a tendency to blame end-users for systems failures, with a corresponding distrust of end-users, and desire to restrict end-user functionality in an effort to retain control of the systems. IT staff tended to stereotype end-users as technophobic or distrustful of IT, difficult to communicate with, and ignorant of technical priorities. End-users, in turn, tended to stereotype IT staff as having poor communication skills, being poor at training, given to using impenetrable jargon, and unresponsive to requests for help. The managers expressed their need to rely on the IT staff to maintain systems and safeguard the organisation from external threats. The authors suggested that

communication dysfunctions between IT staff and end-users could potentially exert considerable negative effects on organisational functioning (Guzman et al., 2004).

Doctoral research by Jacks (2012) involved semi-structured interviews (n=25) with IT workers in 32 United States-based companies, on the basis of which survey instruments for IT staff and board members were developed, administered and analysed. His research aim was to explore the values which were collectively important to IT staff. He identified reverence for knowledge, innovation, structure, autonomy, precision and enjoyment as the most important values of the IT occupational culture, with reverence for knowledge central to the scheme as the value on which others depend. The opposites of these values (hacking, disorganisation, technological stagnation) were regarded with particular distaste and were to be avoided at all costs. Jacks suggested that a fundamental cause of the antagonism between IT workers and other groups was an apparent lack of regard for IT workers' core values. Other aspects of the IT occupational culture have been identified: Chase (2008) highlighted the need for constant re-training and learning, and Ramachandran and Rao (2006) the insularity, while Kostera and Postuła (2011) identified a resistance to categorisation and a need for autonomy. The researcher was unable to locate any research in this area relating specifically to the public sector, or to the United Kingdom; this represents a research gap in a field bearing on the current study.

2.5.4 Inter-professional conflicts: professional jurisdiction

Professionalism in the so-called collegial professions can be seen as representing a form of organisation and social control of expert occupational groups. Evetts (2003, p. 4) suggested that there is an inherent link between professionalism and risk: professions can be viewed as structural, occupational and institutional arrangements for "dealing with work associated with the uncertainties of modern lives in risk societies". The concept of the risk society is associated particularly with Beck (1992) and Giddens, who defined it (1999, p. 3), as "a society increasingly preoccupied with the future (and also with safety), which generates the notion of risk". Freidson (1994, cited by Paton, Hodgson, & Muzio, 2013, p. 228) described the arrangement as a "regulative bargain", "whereby the state protects professionals from unfettered competition but trusts them to put public interest before their own". Hafferty (2006, p. 197), in the context specifically of medicine, similarly speaks of "a social contract between medicine and society". A measure of self-regulation, occupational roles affording wide degrees of autonomy and self-governance, (sometimes) chartered status for professional bodies, a monopoly of the relevant areas of work, and high monetary rewards, are afforded to these groups on condition of fulfilment of

requirements by their members, generally involving lengthy, professionally-governed training and adherence to prescribed standards of conduct. Members of these professions are thereby trusted by society to act in their patients' / clients' best interests, and are accorded a corresponding level of authority over their clients (Lambert, Herbert, & Rothwell, 2013). From this viewpoint, professionalism can be seen not only as a normative value system (Evetts, 2013), but as a strategy to gain occupational power (Fincham, 2006). As strategies of professionalisation are pursued, processes of conflict and completion between different professional and occupational groups are likely to occur.

Abbott's theory of professions (Abbott, 1988, 1998) provides a useful way for considering these. His work was based upon an extensive historical review of professions both in the United States and in Europe. He conceived of equilibrium within an interacting system of professions, where the individual professions compete with each other within the workplace and in the broader public arena to establish what he terms *jurisdiction* over intellectual and practical territory. "[A] jurisdiction is an abstract space composed of a set of tasks, often called professional problems." (O'Connor, 2009, p. 285). A profession establishes jurisdiction by identifying a set of tasks that comprise its work and then putting forward a convincing claim that it alone is qualified to perform those tasks (O'Connor, 2009). According to Abbott's theory,

"... the chief characteristic of professional work is education in an abstract, academic knowledge base that provides the context in which to learn procedures ... academic knowledge legitimizes a profession's claims that its expert work effectively addresses the problems it has defined." (Dalrymple, 2002, p. 314).

Note that competitive tactics involve not only the acquisition of new skills or craft-based knowledge, but also a new intellectual framework: a profession will try to "expand [its] cognitive dominion by using abstract knowledge to annex new areas, to define them as [its] own proper work" (Abbott, 1988, p. 102) and confirm the legitimacy of its practice. Membership of a profession thus inevitably creates boundaries in relation to other professions that are cognitive, as well as social; these boundaries may hinder the diffusion of innovations (Dopson & Fitzgerald, 2005).

Within an particular institution, a profession is able, through its ability to create, legitimise and control knowledge and practices, to shape institutional arrangements that privilege its own jurisdictional claims (Currie, Lockett, Finn, Martin, & Waring, 2012). Once having established a jurisdiction, the profession needs then to accredit its members via the mechanisms afforded by

educational qualifications and professional associations, and possibly also campaign to establish a legally-protected monopoly. It is thereby able to protect its jurisdiction from two types of outsiders, the public and other professions, and to entrench its position within the labour market. External and internal developments, such as technological advances, organisational restructuring or changes in regulation, can disturb an existing equilibrium between professions, resulting in jostling for position and readjustments arising from new jurisdictional claims.

According to this account of the mechanisms of professional jurisdiction, disputes over professional territory can be resolved in a number of different ways, with varying levels of stability. These include stratification, sometimes involving the development of hierarchies, within a professional group. This is apparent within accountancy, for example, with its clear differentiation into cost and management accountants, public sector accountants, and auditors (Kotb, Roberts, & Sian, 2012) or perhaps less formally in librarianship, where clear divisions exist between academic, public, and special librarians, health librarians constituting a large group of the latter. While processes of stratification may be observable within the health informatics professions, where, for instance, clear demarcations appear to exist between the main areas of the HICF, evidence will be presented in Chapter 4 of a blurring of boundaries, and consequent “turf wars”, in some areas within the case study organisations. The establishment and maintenance of a jurisdiction via the motivations and processes described by Abbott and others has been described as a “professional project” (e.g. Larson, 1977). Information technology practitioners (Ensmenger, 2001; Iivari, Hirschheim, & Klein, 2008; Zwerman, 1999) and particularly information security practitioners (Burley, Eisenberg, & Goodman, 2014; Reece & Stahl, 2015) have historically been resistant to processes of professionalisation beyond the establishment of professional education and certification schemes. Information technology practitioners as a group within the United Kingdom are said to be marked by “weak professionalisation” (Fincham, 2006, p. 20); this has a bearing on how professional projects in health informatics are pursued.

2.5.5 The NHS as an organisation

2.5.5.1 Introduction

As well as a general overview of the NHS (Section 1.4), it is essential to provide some account of its organisational character. As an organisation, the NHS has frequently been characterised as a “professional bureaucracy” (Hanna, 2008; Harrison & Smith, 2003, citing Mintzberg, 1991; Hyde et al., 2013) operating within an environment of New Public Management. It has a hybrid character, insofar as it is governed by bureaucratic norms in respect of routine administrative and accounting

functions, but governed by professional autonomy, exempt from bureaucratic constraints, in respect of its dealings with patients and with its own staff. The hallmarks of bureaucracy, as proposed originally by Weber (1947), are said to be: a hierarchy of officers, rational-legal authority exercised impersonally through the abstract application of policy or procedural rules to particular cases, authority of officials deriving solely from their official role, a systematic division of labour based upon functional specialisation, impersonality of interpersonal relations, appointment of officials on expertise and merit, and formal record-keeping. Bureaucratic organisational forms are associated also with a high level of centralisation in policy making and allocation of resources (Exworthy, Powell, & Mohan, 1999; Hall, 1963).

New Public Management (NPM), an established trend within the public sector since the 1980s based on neoliberal principles, is said to consist of four main elements: an efficiency drive; cultural change; downsizing, flattening of hierarchies and decentralisation; and a public sector orientation (Currie & Procter, 2005). It is associated also with prominence given to targets established and monitored by external regulators, the fulfilment of which is financially incentivised, with competition introduced via market mechanisms (Dunleavy, 2005), with an emphasis on accountability and transparency, and with the adoption of private-sector modes of organisation and governance (Clatworthy, Mellett, & Peel, 2000). The practical effect of implementation of NPM has often been to strengthen political and senior management control and to increase bureaucratic tendencies; local managerial autonomy may be largely restricted by extensive centrally dictated targets (Hoque, Davis, & Humphreys, 2004). The impact of NPM upon professional groups is said to be highly variable according to the nature of the profession (Farrell & Morris, 2003; Fitzgerald & Ferlie, 2000).

Historically, the medical profession has enjoyed a high level of autonomy within the NHS, considered at all levels: at the micro level (control over diagnosis, treatment and work patterns, evaluation of work, and nature and volume of tasks), the meso level (relations with the state) or the macro level (the status of the “biomedical model”). As well as management reforms following the principles of NPM, recent decades have seen the growth within the NHS of the evidence-based practice (EBP) movement and the introduction of clinical governance, all of which are widely considered to have limited medical autonomy (Allsop, 2006; Davies & Harrison, 2003; Greener, Harrington, Hunter, & Powell, 2011; Harrison & Ahmad, 2000; Harrison & Checkland, 2009; Harrison & Lim, 2003; Harrison & Smith, 2003; Hewitt & Thomas, 2007). Flynn (2002) suggests that, with the advent of clinical governance, the NHS is increasingly moving from a professional bureaucracy to a “machine bureaucracy”, i.e. one in which “encoded knowledge” – that is, collective, explicit knowledge,

codified, subject to organisational control, and stored within policies, guidelines and procedures (Lam, 2000) – has become the dominant knowledge type, rather than the “embrained knowledge” characteristic of professional bureaucracies.

Despite increasing levels of regulation and managerial control, NHS managers’ ability to control service delivery may still be considerably constrained by the need to have regard to the interests of the professionals who form the “professional operating core” of the organisation, i.e. doctors and other clinicians, with whom operational knowledge lies. Doctors in particular may exercise a collective power of veto over decisions that they perceive to be against their professional interests. Managers depend upon clinicians for the achievement of centrally-prescribed targets and objectives; if clinicians do not accept the legitimacy of processes or targets, they can withhold their co-operation, even to the point of sabotage. Hence, managers need clinicians to trust them (Brown, Alaszewski, Pilgrim, & Calnan, 2011).

2.5.5.2 Public distrust, risk and regulation

Health services in Britain and elsewhere have witnessed since the 1990s, in response to a number of high-profile scandals involving poor practice and outcomes, the design and introduction of monitoring and surveillance frameworks that limit the capacity for individual discretion to manage risks. A variety of checking mechanisms (the introduction of the clinical governance system and national service frameworks, changes in professional regulation, the setting up of the National Institute for Clinical Excellence and the Commission for Health Improvement – now the Care Quality Commission) were introduced to ensure the quality of health care provided by clinicians and of the management of NHS organisations in Britain (Alaszewski & Horlick-Jones, 2002). The history of these developments is charted by Ham, Berwick, and Dixon (2016). These initiatives have been defended politically on the basis that they engender confidence and secure public trust in health service institutions. However, the underlying assumptions of this emphasis on regulation and inspection have been challenged by health policy researchers on a number of fronts, as they relate to: the nature of trust and of risk, the increased rationalisation of health service provision, the alterations in professional practice and relations, the erosion of embodied, tacit knowledge, and the contradictory pressures they can create within managers’ roles (Brown, Alaszewski, Pilgrim, & Calnan, 2011; Hillman et al., 2013). As such, although these systems and practices may improve the overall quality and consistency of care, they have the perverse effect of generating public distrust. Clinicians who were formerly trusted to manage their own performance are likely to experience governance systems as expressing mistrust in their professional abilities, and they may, in turn, exhibit mistrust

of those whom they perceive as advocates and implementers of the new system, i.e. middle and senior managers (Brown et al., 2011; Brown, 2008). Moreover, it has been found impossible in practice to eliminate the need for tacit knowledge in clinical decision making. Meanwhile, according to Maddock (2002), risk-averse cultures within the NHS and other public sector organisations create a barrier to positive organisational change; while the government continues its attempts to drive transformation, it does so “via closed-systems thinking and the belief in the risk-free solution” (p. 15).³⁶

In their discussion of medical professionalism, Currie *et al.* (2012) highlighted the concern of policy makers with managing risk, and thus the importance of theorising about risk as a basis for legitimating and maintaining professional power. From this perspective, theorising about risk and its management is particularly effective as a professional strategy, since it is likely to enjoy heightened legitimacy among a wide range of actors. The risk discourses of information governance and IT managers in the NHS – whereby a particular application or activity XXX is identified as an information security or cybersecurity risk requiring to be managed by themselves according to measures that they prescribe – can therefore be seen as a highly “political” in nature. It is suggested on the basis of the foregoing discussion that aversion to risk (Alaszewski & Horlick-Jones, 2002; Maddock, 2002; Matthews, 2009), high levels of regulation, and low levels of organisational trust are characteristic of the NHS as an organisation. Other aspects of risk are discussed below in Sections 2.6 and 2.7.1.

2.5.5.3 Staff engagement, organisational values and organisational trust

Three areas closely related to organisational culture are those of staff engagement, organisational values and organisational trust. The NHS Constitution (Department of Health, 2015) stated that:

“All staff should have rewarding and worthwhile jobs, with the freedom and confidence to act in the interest of patients. To do this, they need to be trusted, actively listened to and provided with meaningful feedback. They must be treated with respect at work, have the tools, training and support to deliver compassionate care, and opportunities to develop and progress.”

Considerable attention to staff engagement has been paid as an organisational priority within the NHS on account of the clear relationships that have been demonstrated between engagement and aspects of organisational performance or effectiveness: staff health and wellbeing, staff turnover, absenteeism, morale, patient satisfaction, and clinical outcomes, including mortality (Harter, Schmidt, Kilham, & Agrawal, 2009; Mailley, 2011; Topakas & Dawson, 2010; West & Dawson, 2012; West, Topakas, & Dawson, 2014).

Sir Robert Francis's *Report of the Mid-Staffordshire Foundation Trust inquiry* highlighted in its recommendations the importance of "of a common culture shared by all in the service of putting the patient first" (Francis, 2013, volume 1, p. 13). To enable staff engagement, it is suggested that a coherent set of organisational values and behaviours needs be developed and adopted, preferably with extensive staff involvement, and thereafter upheld by senior managers and embedded within organisational processes (in particular human resources processes), so that formally stated values are reflected in everyday behaviour (Black, 2012; McLeod & Clarke, 2009, cited by Dromey, 2014). Among the organisational factors cited as leading to greater staff engagement are effective channels of communication, availability of the necessary information for staff to do their jobs well, learning opportunities, concern overall for staff health and wellbeing, and trust by staff in their supervisors and leaders. At the organisational level, it is considered necessary to build and develop cultures of reciprocal trust: staff need to feel both that they are able to trust their leaders, their managers and the system as a whole, and that they are themselves trusted within the organisation to do their jobs (Holmes et al., 2014; Robinson, Perryman, & Hayday, 2004; West & Dawson, 2012; West, Dawson, Admasachew, & Topakas, 2011). The latter is a form of what is sometimes referred to as ascribed trust (Sunderland, 2000) or attributed trust (Box & Pottas, 2014). Trust, according to Mayer and associates (Mayer, Davis, & Schoorman, 1995; Schoorman, Mayer, & Davis, 2007), is based upon the trustor's perceptions of the competence, benevolence and integrity of the trustee. This applies at interpersonal, inter-group, or inter-organisational levels. Managers' trust of staff, according to Powell (2016, p. 8), is "based on the belief that people have a strong intrinsic motivation to perform to the best of their abilities" and is associated with the development of an organisational culture that encourages risk-taking and avoids blame. Bozeman and Kingsley (1998) found that perceived trust in employees by senior managers was a key determinant of risk culture, rather than internal organisational controls in general. They suggested that clarity of goals and organisational trust in general foster positive attitudes to risk; formalisation and "red tape", however, inhibit them; cf. the proposed theoretical model in Section 11.1.

“Engagement” is a somewhat contested concept lacking an agreed definition at an academic level (Purcell, 2014; Truss, Alfes, Delbridge, Shantz, & Soane, 2013). One of the main perspectives on engagement identified by Shuck (2011) describes and defines engagement as the *antithesis of burnout* as defined by Leiter & Maslach (2003, p. 93), a state characterised by “a psychological syndrome of exhaustion, cynicism and inefficacy which is experienced in response to chronic job stressors”. Work engagement, in this perspective, is characterised by energy, enthusiasm and efficacy: the antithesis of burnout. The authors had previously identified (Maslach and Leiter, 1997, 1999, cited by Leiter and Maslach, 2003) six areas of so-called job-person mismatch which are critically implicated in burnout: these are *workload*, *control* (employees’ perceived ability to influence decisions affecting their work), *reward* (the extent to which the rewards of the job – intrinsic, social and monetary – accord with expectations), *community* (the overall quality of social interaction at work), *fairness* (the extent to which decisions at work are perceived as being fair, and people treated with respect), and *values* (alignment of the motivations and ideals that originally attracted a person to the job with the values expressed in its actual practice within the organisation).

Within the Institute for Employment Studies (IES) model of staff engagement, the characteristics of an engaged workforce are summarised as “motivation, satisfaction, commitment, finding meaning at work, and pride in and advocacy for the organisation” (Mailley, 2011, p. 7). Since 2009, the annual NHS Staff Survey (NHS Employers, 2017)³⁷ which is intended to gather views on staff experience at work in key areas, has included questions covering three key areas of staff engagement: staff advocacy, motivation, and involvement. The overall staff engagement score is computed from indicators relating to the characteristics of an engaged workforce given above.

Staff engagement is closely related to the construct of empowerment as discussed in the previous section. Intuitively one might expect that those staff who perceive themselves as empowered within their organisation will also be more highly engaged than those who do not. This supposition is confirmed by much recent human resources management research. For Cattermole, Johnson, and Roberts (2013), empowerment is an important precondition of staff engagement. Greco *et al.* (2006) developed and tested a model that integrated Kanter’s organisational empowerment theory with Maslach and Leiter’s work engagement model as described above (Maslach & Leiter, 1997, cited by Greco *et al.*, 2006), according to which empowerment should result in higher levels of engagement;

³⁷ NHS Staff Survey: <http://www.nhsstaffsurveys.com/Page/1056/Home/NHS-Staff-Survey-2016/>

their findings supported the proposed model (as shown in Figure 2.3 below).

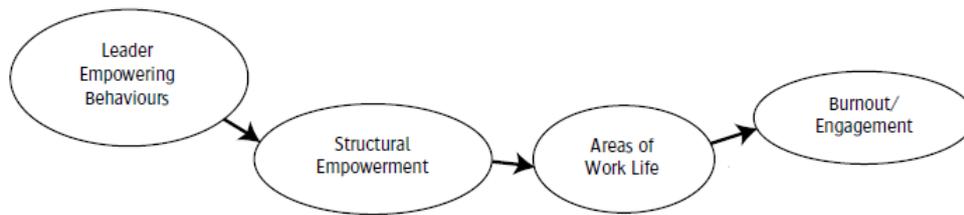


Figure 2.3 Proposed model: the effect of empowering behaviours on work engagement / burnout
Greco et al., 2006, p. 47, Reproduced by permission

The relationships of structural empowerment with areas of work life, as identified by Maslach and Leiter, have been extensively investigated by Laschinger and associates (e.g. Laschinger & Finegan, 2004; Laschinger, Finegan, & Shamian, 2001; Laschinger et al., 2010; Laschinger, 2008; Laschinger, Wilk, Cho, & Greco, 2009) in relation to nursing care outcomes. Within the same conceptualisation of engagement, a more direct relationship can be posited between engagement/burnout and job demands and resources. The job demands–resources model (Demerouti, Bakker, Nachreiner, & Schaufeli, 2001, cited by Crawford, LePine, & Rich, 2010) represents the job attributes and other related working conditions relating to engagement or burnout in terms of two overarching categories: demands and resources. Within the model, “job demands” refer to “those physical, social, or organisational aspects of the job that require sustained physical or mental effort and are therefore associated with certain psychological costs (e.g., exhaustion) and include aspects such as workload, time pressure and difficult physical environments” (Crawford et al., 2010, p. 835). They may be further categorised as presenting either challenges or hindrances. In principle, barriers to information seeking, such as inadequate IT infrastructure or obtrusive security, including the blocking of access to websites and web applications, could be categorised as hindrances; cf. Sasse’s (2015) comments cited in 11.4.2 below on user security fatigue and the need for security to be usable. “Job resources” refer to “those aspects of the job that are functional in achieving objectives, which stimulate personal growth and development, and which reduce job demands and their associated physiological and psychological costs ... [They] include aspects such as control over one’s work, professional development opportunities, participation in decision making, varied tasks, feedback, and social support” (Crawford et al., 2010, p. 835). Challenge demands may elicit positive emotions; hindrance demands, however, tend to trigger negative emotions. According to Crawford et al. (2010),

“... individuals should be less willing to invest themselves to respond to hindrance demands because the negative emotions they experience are likely to make them feel unable adequately to deal with these demands. Since people are likely to believe that using up resources to cope with hindering demands will block them from attaining meaningful outcomes, they are apt to have little motivation to cope with them actively. Resources consumed dealing with negative emotions and the psychological threat associated with hindrances are associated with decreased levels of motivation and engagement”
(May et al., 2004; Porath & Erez, 2009, cited by Crawford et al., 2010, p. 838).

The authors went on to propose a model of the relationships between job resources, hindrance demands, challenge demands, burnout and engagement, which is illustrated in Figure 2.4 below.³⁸

2.5.6 Theories of organisational power

Power is a complex phenomenon that is, in Lukes’s (1974) phrase, “essentially contested”. This review limits itself to two limited and contrasting perspectives on organisational power which are particularly relevant to the study: Kanter’s (1979) theory of structural power and empowerment, and Clegg’s (1989) theory of circuits of power. The first proposes that access to information is one of the necessary structural conditions of empowerment within organisations. The second is relevant on account of frequent references to it within information systems studies, and its particular application within actor network theory, as described below (Sections 2.5.6.2 , 11.3.2).

2.5.6.1 Kanter’s theory of structural power and empowerment

Kanter (1979) defined power within organisations as “the ability to mobilise resources (human and material) to get things done” or as “the ability to get things done, to mobilize resources, to get and use whatever it is that a person needs for the goals he or she is attempting to meet” (Kanter, 1993, p. 166, cited by Manojlovich (2007)). She saw employees’ behaviour and attitudes as arising from their working conditions and from circumstances within their workplace, far more than from personal attributes.

³⁸ Cf. Sasse’s comments on the need for security usability / user fatigue, below (11.2.2)

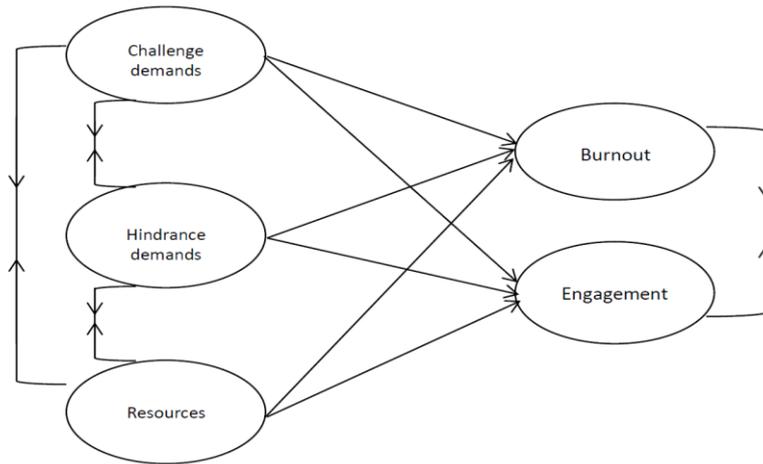


Figure 2.4 Relationships between job resources, job demands, burnout and engagement
 Redrawn from Crawford et al. (2010), p. 841 (simplified)

Power, according to Kanter, may be exercised productively (power to accomplish) or oppressively (power to punish, prevent, sell off, reduce, dismiss – without thought for possible consequences). It may be categorised either as *formal* or as *informal*. Jobs that are perceived as central to the overall purpose of the organisation, that have high visibility, and are constructed in such a way as to afford maximum discretion and flexibility, contain *formal* power. *Informal* power results from positive relationships with superiors (sponsors), peers, subordinates, and external professional contacts. Lines of supply, lines of information (formal and informal), and lines of organisational support all function in this theory as sources of power.

According to Manojlovich (2007), Kanter identified four necessary structural conditions as contributing to organisational empowerment:

“having opportunity for advancement or opportunity to be involved in activities beyond one’s job description; access to information about all facets of the organization; access to support for one’s job responsibilities and decision making; and access to resources as needed”.

Structural empowerment is thus comprised of formal and informal power as well as access to lines of power (Kanter, 1993, cited by Laschinger & Finegan, 2004). “Information” in this context includes technical knowledge related to employees’ job roles (for instance, nursing knowledge and skills), as well as internal information relating to developments within the larger organisation (Laschinger et al., 2010), hence would include published clinical evidence sources. Access to resources “relates to one’s ability to acquire the financial means, materials, time and supplies required to do the work” (Cho, Laschinger, & Wong, 2006, p. 45), hence could include IT infrastructure. Managers play a vital

role in ensuring that their staff have access to these sources of empowerment within the work setting.

2.5.6.2. Clegg's circuits of power theory

The existing studies of concepts of power in information security (Fragos, Karyda, & Kiountouzis, 2007; Jasperson, Butler, Carte, Price, & Saunders, 2002) refer extensively to Clegg's (1989) circuits of power theory. The scenarios discussed by Inglesant and Sasse (2011a) are highly pertinent to the present study, and the researcher has followed these closely in the account that follows.

Within organisations, so-called legitimate power derives from the structures and rules of authority (Silva, 2007, citing Mintzberg, 1983). However, Silva suggested that authority will always be contested, as formal rules are open to interpretation; he identified this (following Clegg, 1989) as the essential source of organisational politics. In order for an organisation to operate, authority and discretion within it needs to be delegated; the right to interpret rules, policies and procedures is thereby granted by senior managers to their subordinates. However, for organisational action to be effective, this delegated discretion needs to be disciplined; that is, those in authority need to ensure that these subordinates interpret the rules exactly as intended, thereby minimising the scope for politics. He suggests therefore that, to ensure their loyalty as delegated agents, formal authorities in organisations attempt to foster members' identification with the aims of the organisation, and employ disciplinary techniques, such as reporting arrangements, policy sanctions or surveillance. Information systems, according to Silva (2007), constitute a key instrument of organisational control, and can radically alter work tasks in a manner which impact on workers' identities.

Clegg's concept of power is illustrated in Figure 2.5 below. It is fundamentally relational; power circulates through the media of social relations and discourses (Silva, 2007). Clegg's theory posits three circuits, a micro-level of *agency* and two macro-level circuits of *social integration* and *system integration*. These circuits correspond to three types of power, termed *causal*, *dispositional* and *facilitative*. The power that is expressed within organisations through information infrastructure controls such as passwords, smartcards, group policies, firewalls etc. is classified as *causal power*, and the corresponding power relations are described as *episodic*. They represent the overt type of power discussed in most organisational theories: that which is defined by Dahl (1957, cited by Silva, 2007) as follows: A exercises power over B when A makes B do something that B would not otherwise do. In other words, A creates for B what is termed as an *obligatory passage point*.

These so-called episodic power relations derive from, and lead into, the two macro-level circuits, those of *social integration* and *system integration*. These together make up a "field of force" within

which “rules, relations and resources” are reproduced or transformed, facilitated or restricted; within which “certain fixtures of meaning are privileged” (Inglesant and Sasse, 2011a, p. 10). Social integration involves “fixing or refixing relations of meaning and of membership” (Clegg, 1989, p. 224). It centres on meaning, rules of practice, and membership categories; in the present instance on the *meaning* associated with the entities, human, social or technological, through which information security controls are exercised. From this meaning derives so-called *dispositional* power, defined as a capacity to wield power, whether or not it is actually exercised. Dispositional power is concerned with the capacities that prefigure the conditions required for the exercise of episodic power (Silva, 2007).

System integration is the converse of social integration: it is concerned with “the empowerment and disempowerment of agencies’ capacities” (Clegg, 1989, p. 224) and in particular with “the technological means of control over the physical and social environment” (Lockwood, 1964, cited by Inglesant and Sasse, 2011a, p. 10). The corresponding type of power, termed *facilitative* power, is understood in terms of its “ability to produce and achieve collective goals” (Silva, 2007, p. 179). This facilitative power, or “power-to”, covers whatever an organisation uses, whether technology, physical constraints, or contractually enforced rules, to enforce its institutional patterns, and as such is subject to changes in technology.

Actor network theory (ANT)(Elder-Vass, 2008; Law & Hassard, 1999; Walsham, 1997), which is widely used to analyse relations within socio-technical networks, is a key constituent of Clegg’s circuits of power theory. The basic premise of ANT is a rejection of any essential distinction between human and non-human actors within a social system; the word “actant” may be used to emphasise this. ANT thus eschews any distinctions *a priori* between what is deemed “technical” and what is considered “social” or “organisational” (Bloomfield & Danieli, 1995).

In ANT, “actants” are perceived as “related not by pre-existing social structures but in networks which emerge through their own actions” (Inglesant and Sasse, 2011a, p.11). Central to these actor networks, and to the circuits of power theory, is the concept of an *obligatory passage point*. An obligatory passage point (OPP) is “an actor that mediates the transactions of other actors in the network, controlling and regulating activity by acting as a ‘gatekeeper’” (Goff, 2014, p.?).

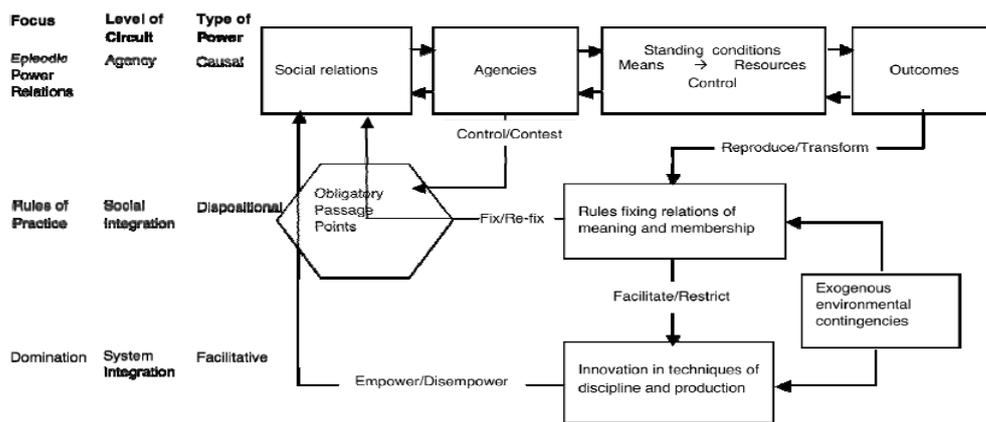


Figure 2.5 Representing the circuits of power

Clegg (1989), p. 214

Reproduced by permission

OPPs are established via a process of what is termed *translation*. There are four so-called moments of translation: *problematization*, *interessement*, *enrolment* and *mobilisation*. Initially a first actor presents an issue in such a way to a second actor that “there is no alternative” to the solution they propose: this is the process of so-called *problematization*, where one actor presents the solution to a problem in terms of that actor’s resources (Silva, 2007). Other actors are then said to be “enrolled” and “drawn into alliances” around this central problem (Inglesant and Sasse, 2011a). Initially the first group of actors must be isolated, i.e. other possible alliances or interference that represent a possible challenge the legitimacy of the OPP must be impeded; this is the process of *interessement*. The subsequent third translation step is termed *enrolment*. During this step, alliances are established and consolidated through negotiations. According to Walsham (1997, p. 469), “successful networks of aligned interests are created through the enrolment of a sufficient body of allies, and the translation of their interests so that they are willing to participate in particular ways of thinking and acting which maintain the network”. The fourth and final process is *mobilisation* of the allies. This step of mobilisation implies that actors will become the spokespersons for the groups they claim to represent; it consists in establishing the legitimacy of the spokesperson. The movement between steps of the translation process is known as *displacement*; when displacement occurs, episodic power is exercised. Information systems, or particular features of them such as enforcement of security measures, can be viewed as OPPs.

It may seem odd at first sight for a professed critical realist (Section 3.2.5, below) to employ ANT, a pragmatist research tradition to which critical realism would appear at first sight to be radically

opposed. ANT appeared, however, to offer a novel, and potentially valuable, method for analysing detailed small-scale information security scenarios, on the grounds that it treats non-humans as important parts of social analysis (Tatnall, 2003; Tatnall & Gilding, 1999). It was also employed by Clegg within his circuits of power theory (1989), as applied to information security by Inglesant and Sasse (Inglesant & Sasse, 2011a, 2011b; see 2.4.9.2, 11.3.2). The researcher chose to pursue it on this basis (Section 11.3.2 below). For general discussions of the possible value and use of ANT concepts within a critical realist framework, see Elder-Vass (2008) and Mutch (2002). Faulkner and Runde's expressly critical realist theory (2011, 2013) of the social position of technological objects, which is based upon Bhaskar's Transformational Model of Social Activity (Section 3.2.5), might have provided an alternative; however this latter did not appear to have been applied so far to issues of power within information systems or information security, and was accordingly much less immediately applicable or usable.

2.5.7 Summary and synthesis

This section has covered a range of organisational issues of relevance to the research, relating to organisational cultures and subcultures in general, professions and professionalism, and power. In particular, it has addressed IT staff subcultures and attitudes, the characteristics of the NHS as an organisation, and issues of staff engagement, trust, risk and regulation within the NHS. There are clear indications of the existence of a distinct IT staff subculture, and of the effects of regulatory processes upon organisational trust and attitude to risk.

Section 2.5.5.2 outlined issues of public distrust, risk and regulation relating to the NHS as an organisation: the introduction of systems of regulation in response to high-profile instances of poor quality of care, their implementation, and their organisational impacts (high levels of local regulation, conflicts between clinicians and managers, low levels of trust of staff by senior managers, cultural aversion to risk), that have been the subject of numerous health management and policy studies. Currie *et al.*'s (2012) study of medical professionalism appears particularly important, on account of its identification of the role of theorising about risk as a basis for legitimating and maintaining professional power.

Section 2.5.3 addressed issues of IT subcultures and professional values. There were clear indications within the studies cited that IT staff can generate distinctive occupational subcultures, of which negative attitudes to end-users (poor ratings of their general IT literacy, web searching skills, and integrity, with consequent distrust and a desire to restrict the IT functionality available to them), are

an identifiable component. End-users, in turn, may develop negative attitudes to IT staff, tending to stereotype them as having poor communication skills, prone to using impenetrable jargon, poor at teaching, and being unresponsive to requests for support. These studies have clear implications for evaluating the perceived quality of IT support and of inter-professional interactions involving IT staff and managers as a factor relating to barriers to information seeking.

Anecdotal evidence had suggested that barriers to accessing and using information could have a negative impact on staff morale and engagement (2.5.5.3). Concepts of staff engagement itself, and of organisational factors promoting staff engagement, have been extensively studied. The job demands–resources model posits a direct relationship between job resources (necessarily including professional development opportunities and access to information), job demands (including so-called hindrance demands, such as poor IT infrastructure or the blocking of access to websites and web applications) and staff engagement, and thus provides a conceptual framework for evaluating the effects of lack of access to published online information.

Sections 2.5.6.1 and 2.5.6.2 addressed issues of power in organisations relating to information and information security. Two relevant constructs were described, the structural empowerment theory of Kanter (1993), developed and extended within nursing by Laschinger and associates, and the circuits of power theory of Clegg (1989). Within Kanter’s theory, access to information is one of the key conditions proposed for staff empowerment. The circuits of power theory was applied by Inglesant and Sasse (2005a, 2005b) to information security scenarios very close to those frequently encountered within the NHS, providing a basis for later discussion and analysis. These were the only relevant studies identified; the numerous other studies of power in information security that were identified by the researcher, including conceptual models, related mainly to overall policy development, system development, or system implementation and enforcement, and were thus of only marginal relevance.

2.6 Information security and cybersecurity: introduction

2.6.1 Definitions

The thesis is concerned with the effects both of information security and of cybersecurity measures upon access to published information. The term “information security” is often used interchangeably and inclusively of the term “cybersecurity”; Olijnyk’s bibliometric analysis (2015) of the profile and evolution of information security literature included aspects of cybersecurity as a sub-category of information security. Until relatively recently, NHS policies (NHS Connecting for Health, 2007)

focused upon “information security” and did not specifically address cybersecurity as such. However, while there is a considerable overlap in scope (see Figure 2.6 below), the two terms are not synonymous: as Refsdal, Solhaug, and Stølen (2015) indicate, cybersecurity is defined in terms of the types of threats to information assets (both information and IT infrastructure) which it addresses, i.e. threats which arise within a cyberspace. Such threats are primarily technical in nature; while cybersecurity may focus primarily on the protection of digital information assets, it is not limited to this, but includes the protection of the related IT environment, i.e. cyber systems.

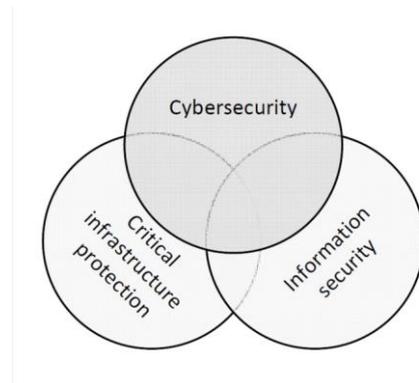


Figure 2.6 Cybersecurity vs. information security and critical infrastructure protection

From Refsdal *et al.* (2015), p. 31

Reproduced by permission

Many critical infrastructures involve cyber systems: critical infrastructure protection focuses on the protection of networked infrastructures of any sort, whether or not they involve a cyberspace. Definitions of the term “cyberspace” itself vary widely in scope and emphasis (Le & Hoang, 2016). These authors suggest that it should be defined as a space that embraces three main elements: *real and virtual entities* (interconnected digital devices of all types, and virtual abstraction of entities, such as data, information, software and services), *interconnecting infrastructure* (networks, applications, information systems and storage that support these entities) and the *interactions* among entities. These interactions include activities and interdependencies among the entities in cyberspace, including human agents. The International Telecommunications Union defines cybersecurity, as follows:

“Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets ... Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization against relevant security risks in the cyber environment”
(ITU 2008, cited by Maurer and Morgus, 2014, p. 31).

This definition, while comprehensive in the scope of activities specified, does not clarify the nature of the “relevant security risks”. These are more clearly spelt out by Amoroso (2006, cited by Craigen, Diakun-Thibault, & Purse, 2014, p. 14): “Cyber security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and so on.” More recently, with a perceived increased risk of cyber-attacks on NHS organisations, cybersecurity has been emphasised more distinctly within the NHS as an aspect of wider national measures, although cybersecurity measures are still considered overall within the framework of the IGT (Carlisle, 2015). The matrix in Appendix P below (Table P.1), which provides examples of common security measures within the different categories, may help to clarify the distinction.

2.6.2 Web-based cybersecurity threats

Generally the impacts of cyber-attacks on the confidentiality, availability and integrity of information can be considered under four headings: of *interruption* (denial of service, preventing access to information), *interception* (network traffic capture of confidential data), *modification* (altering captured network traffic, altering a user name, or source address for network traffic), and *fabrication* (replaying modified network traffic, spoofing identity) (Thomas, 2006). Cyber-attacks, which aim to sabotage an organisation’s IT infrastructure, can be far-reaching in their effects on its operations and services, often involving substantial down time, expense, and damage to safety-critical systems. Attacks on health service providers may affect medical devices (Williams & Woodward, 2015).

The high incidence of web-based attacks means that use of the Internet, while an integral part of people’s business and personal lives, represents in itself a considerable security risk to users and networks (von Solms, 2011). The aspects of cybersecurity within NHS organisations that are relevant to information seeking and use relate primarily to websites and web applications, and derive from: 1) threats to network and system security from compromised websites unwittingly visited by staff using computers and other devices on NHS networks, including malware distributed via drive-by downloads, via so-called pharming, or via so-called phishing attacks, using either social media sites or email; 2) threats to NHS websites; and 3) data loss and theft. Overall, they include the targeting and exploitation of known vulnerabilities in software applications, in particular web browsers; the installation and use of malware of different types (e.g. viruses, browser hijackers, Trojans, worms, bots, rootkits, ransomware, spyware, adware); the exploitation of poorly-managed networks where

security protocols are not used, or are incorrectly applied; and the abuse of trust through social engineering (Harwood, 2011; Lord, 2012; Rouse, 2006).

Ponemon (2015) provided a useful overview of web-based security threats. A user may be lured to a malicious website via so-called pharming or DNS cache poisoning (also known as search engine poisoning) (Imperva, 2013; Rouse, 2007), or via social engineering, typically using email: the so-called phishing or spear-phishing attack (Chickowski, 2013; Howard, 2007). Phishing is defined as the act of sending an email or social media message to a user fraudulently claiming to be an established enterprise or trusted individual, with the aim of enticing the user to provide private information that will be used for criminal purposes (Webopedia, s.d.). Phishing requires user activity, i.e. clicking on a link to a malicious website. Cyber-attacks that obtain personal information (unlike drive-by downloads; see below) require some form of interaction by the user. Drive-by downloads and DNS cache poisoning (Appendix D) are the only forms of web-based security threats that can occur without the site owner's knowledge.

Drive-by downloads are a growing threat.³⁹ A web page is considered malicious if it causes the installation of software without the knowledge or consent of the user (Provos, McNamee, Mavrommatis, Wang, & Modadugu, 2007; Rains, 2011). The mere act of visiting such a compromised or malicious website, without any interaction from the user being necessary, may trigger a malware infection of the user's computer; they are thus arguably the most important category of web-based cyber-threat relating to information seeking. It should be noted that this process is invisible to the end-user (although small iframes may sometimes be visible on a compromised page (Howard, 2007)), and there is no behavioural defence against it, since potentially any website can be compromised (Sjouwerman, 2013). Drive-by downloads are cited as the most serious current web security threat overall; more than 30,000 websites are infected every day, 80% of these being entirely legitimate (Marinos & Sfakianakis, 2012; McCormack, 2016). More technical detail relating to these types of threats is given in Appendix D.

Web 2.0 and social media applications present a range of risks for individuals and organisations. These were reviewed by Baxter and Rudman (2010); Cole (2010); He (2012); ISACA (2010); Khidzir (2016); Kshetri (2012); Palo Alto Networks, (2009); Stritter *et al.*, (2016); and Tennakoon, Ezingear,

³⁹ A variant form of attack has been identified: the drive-by cache (Huang, 2011).

and Benson (2012). Different types of risk to individual users from social media, including security risks, were surveyed by Haynes and Robinson (2015). Such risks include breaches of privacy and confidentiality, exposure to litigation, and other risks to reputation, as well as those relating to cybersecurity. For individuals, inappropriate privacy settings relating to personal information and location may offer opportunities for crime (Cole, 2010). Also, owing to the possibilities they afford for rapid dissemination of compromised content, and via the availability of functionality (e.g. news feeds, rating systems, and comment functions) which incorporates security vulnerabilities, social media applications exacerbate existing cyber threats (Chi, 2011). Applications supporting user-generated content (e.g. forums and blogs) may allow the injection of malicious code such as hyperlinks to images or other external content (Provos, Mavrommatis, Rajab, & Monroe, 2008). Insecure third-party applications may present other risks.

Online advertising presents particular issues for organisations' networks. It is typically syndicated through advertising networks such as Google's DoubleClick,⁴⁰ which act as intermediaries between publishers of websites and advertisers. Advertising content is pulled into web pages from third party servers via HTML content inserted into the publisher's web pages, hence is not under the direct control of the site owner. As well as slowing down the display of the pages and consuming network bandwidth, such systems also have particular vulnerabilities to cyber-attacks, including so-called malvertising, a form of drive-by download. High incidences of malvertising have been found to be associated with sub-syndication processes in which advertising networks auction some of their advertisement slots to other networks (Vratonjic, Manshaei, & Hubaux, 2011; Zarras et al., 2014). Use of consumer online file sharing and collaboration applications such as Dropbox⁴¹, OneDrive⁴² and Google Drive⁴³, which from a corporate perspective represents a form of "shadow IT" (see Section 2.8.3 below) also presents a variety of information security and cybersecurity issues within organisations, arising from the possible lack of security of the application itself (i.e. its possible vulnerability to hacking, non-availability of local encryption), possible unauthorised sharing of information, the difficulty of permissions management, lack of visibility and control to the organisation, lack of strong authentication and access management, and possible abuse of system privileges (Lord, 2017; McClure, 2013; Salazar, 2015). The popular peer-to-peer (P2P)

⁴⁰ DoubleClick: <https://www.doubleclickbygoogle.com/en-gb/>

⁴¹ Dropbox: <http://www.dropbox.com>

⁴² OneDrive: <https://onedrive.live.com/about/en-gb/>

⁴³ Google Drive: <https://www.google.com/drive/>

videoconferencing application Skype,⁴⁴ which uses Voice over IP (VoIP), has been shown to be highly insecure in a number of aspects: it is vulnerable to malware attacks, and stores user data locally in an unencrypted form. It is also possible to determine a user's IP address from their username using a Skype resolver (Gilbert, 2016; Rodrigues & Druschel, 2010; Solutionary, 2014). The researcher has not attempted to address here the complex issues of wireless network security or of the security of mobile devices such as smartphones, which are increasingly made available to NHS Trust staff.

It was noted in Section 1.4.4 that the number of cybersecurity incidents occurring within the NHS increased markedly during the period of the study. This is likely to have related to a increase in the attack surface resulting from greater use of EPR systems, mobile devices and networked medical devices within an environment incorporating many obsolete systems; *cf.* the discussion in Section 2.8.5 below of diffusion of innovations within the NHS. Overviews of the state of cybersecurity within NHS organisations were provided by Millar (2016) and by Sophos (2016b). Cybersecurity threats and trends within health services in general have been reviewed by Kruse, Frederick, Jacobson, and Monticone (2016) and by Luna, Rhine, Myhra, Sullivan, and Kruse (2016).

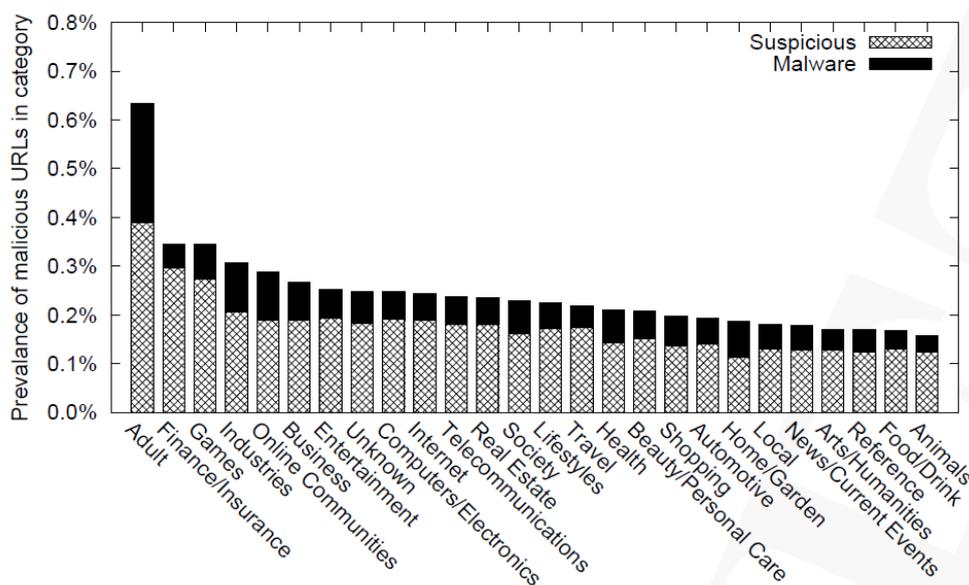


Figure 2.7 Proportion of malicious URLs by subject – random URL sample (7.2 million)

From Provos *et al.* (2008), p. 9 *Reproduced by permission*

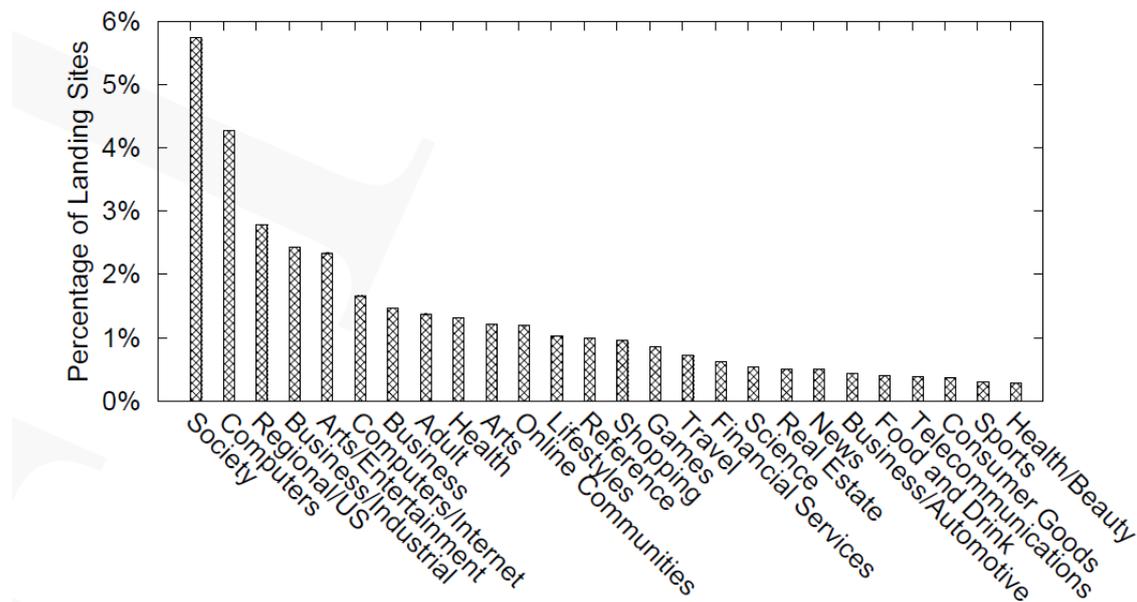


Figure 2.8 Proportion of URLs by subject – all malicious URLs (3.3 million)

From Provos *et al.* (2008), p. 9 *Reproduced by permission*

2.6.3 User behaviour and cybersecurity threats

It was mentioned above that blocking of certain categories of web content was commonly recommended as a defence against web-based cyberattacks. A limited number of studies have attempted to relate malware risks to patterns of user behaviour in relation to Internet use. The findings from these are presented in Table 2.2 below. Based on the findings of these studies, It is difficult to reach definitive conclusions as to what might be said to constitute “high-risk” web activity relating to possible malware infections. This has important implications for cybersecurity guidelines and acceptable use policies, and hence represents a gap in research that bears closely on the present study.

Regarding “adult” websites, Provos *et al.* (2008) found that this category was ranked only 8th out of 26 in percentage of drive-by downloads among the landing pages of malicious or compromised websites, although it was ranked 1st out of 26 in its percentage of malicious sites among the random sample of URLs (Figure 2.7, Figure 2.8), having almost twice the percentage of malicious sites compared with the next ranked category. Lalonde Lévesque *et al.* (2013) found that these sites were associated with lower rates of malware infection than seemingly innocuous categories. They identified eight “risky” categories of web content: P2P applications, social networking, software downloads, gambling, streaming media/MP3, sports, and computers/Internet. The first four of these

are perhaps unsurprising, whereas the latter two at least would normally be considered innocuous. Canali *et al.* (2014) found a weak correlation between numbers of pornographic / “adult” websites visited and malware risk, but a stronger correlation with time spent visiting such sites. Similar to the findings of Carlinet *et al.* (2008), the overall amount of time spent on web-related activity was found by Kent *et al.* (2013) and by Canali *et al.* (2014) to have a positive correlation with risk.

Based on the known propensity of cyber-criminals to compromise popular websites, Keats and Koshy (2009), researchers based at the security vendor McAfee, claimed to have identified the most dangerous subject categories of web search terms. They collected approximately 2,658 popular search terms using a variety of marketing intelligence sources, and used McAfee’s own SiteAdvisor security tool to evaluate the security status and relative risk of 413,368 unique sites retrieved from the Google, Bing, Yahoo!, Live and Ask search engines. “Adult” filters were on. SiteAdvisor tested sites for a range of common security threats, and categorised them as safe (green), requiring caution before using (yellow) or risky (red). Keywords were ranked for risk in two ways, using both 1) the mean risk of all results, and 2) the maximum risk of the riskiest page of results.

They found that the subject categories with the worst mean and maximum risk profiles were music lyrics sites and “free” sites (e.g. free music downloads); health-related searches were among the least risky. The research was published in a brief report published by McAfee itself, but not in any peer-reviewed journals or conference papers. The researchers acknowledged limitations of their methods in respect of how search terms were identified and categorised. The findings were widely discussed in the popular computing press at the time of publication, but the work has not been cited in any subsequent academic study to the researcher’s knowledge. Larsen (2015), a researcher for the security vendor Symantec, investigated subject categories of sites implicated in search engine poisoning attacks, and the search terms which had led users to them. The results were published informally on the company blog. He noted a trend for searches for specific sites (Instagram in particular), and for non-English-language searches to lead to these sites. “Adult” and health-related search terms did not feature strongly (Larsen, 2015).

Authors / Date / Country / Background	Research setting and subjects / datasets	Methods	Research focus	Findings
Provos, Mavrommatis, Rajab, and Monrose, (2008); Provos, McNamee, Mavrommatis, Wang, and Modadugu (2007); Provos, Rajab, and Mavromattis, (2009) United States private sector – search provider	Sites crawled by Google search engine; sites randomly sampled from Google index; sites reported to Google by users	Presence of malware verified via honeypot using AV programs and execution-based heuristics Sites assigned DMOZ subject classifications	Subject distribution of malicious websites compromised by drive-by downloads	No strong association between web content category (thus browsing risk) and risk of exposure to drive-by downloads – though “adult” content appeared to present twice the level of risk within the random sample: see Figures 2.7 and 2.8 for details
Carlinet, Mé, Debar, & Gourhant (2008) France private sector – telco / ISP	Activity data from ADSL customers of telco / ISP	Case control study of online behaviour of users in relation to types of traffic and malware risk Included non-web applications such as FTP	Aspects of user behaviour in relation to risk of malware infection in general / personal computer use	Use of Windows operating systems, streaming applications, high levels of web searching shown to be risk factors for malware infection Results for P2P and web chat applications were inconclusive Did not investigate type of URL visited or aspects of end-user computing environment other than operating system
Lalonde Lévesque, Nsiempba, Fernandez, Chiasson, and Somayaji, (2013) Canada University	Activity data from University staff and students (n=50); survey responses	Epidemiological study of online behaviour using experimental laptops issued to research subjects; used logistic and general regression analyses	Behavioural risk factors for malware infection in general / personal computer use	Computer expertise and age were possible risk factors for increased risk of malware infection Eight ‘risky’ categories of web content identified via regression analysis: streaming media / MP3, P2P, software downloads; Internet infrastructure, social networking, computers/Internet, gambling, sports Three further risky categories of web content identified via the general regression analysis: pornography, illegal/questionable, translator / cached

Authors / Date / Country / Background	Research setting and subjects / datasets	Methods	Research focus	Findings
Kent, Liebrock, and Neil, (2013) United States university	Activity data from end-users within national laboratory	Security compromise indicated by AV, intrusion response, phishing or proximity	Relationship between 'early adopter' behaviour within corporate setting and risk of security compromise	Early adoption, i.e. visiting unique websites or visiting websites before others in the population, was associated with increased risk of security compromise, as was total unique location visit count.
Yen, Heorhiadi, Oprea, Reiter, and Juels (2014) United States university / private sector	McAfee AV security logs, network access logs, web proxy logs, employee database in relation to malware vectors, VPN logs, user demographics, browsing behaviour and place of use (on-site vs. off-site) (hosts n = 85,000)	Epidemiological study: logistic regression using demographics, web activity (categories of sites visited, web usage, blocked and low-reputation domains), VPN activity	Relationship between user demographics and behaviour and risk of malware infection	Risk of malware infection associated with technical expertise, junior position in organisation, use of computers outside organisational network, use of external drives Recommendations made: user education, more refined content categorisation of websites by proxies
Canali, Bilge, and Balzarotti (2014) France university / private sector	Symantec dataset (n=160,229 users) of web pages visited by users of Symantec security products	Correlation analysis, logistic regression analysis	Relationship between web use and malware infection risk	Level of malware infection risk is associated with nocturnal use, and is directly proportional to amount of time spent in web searching. 'Adult' content and use of URL shortening services are associated with increased risk. An individual's level of malware infection risk may be derived from his/her browsing profile, as derived from 74 unique variables relating to web browsing behaviour.

Table 2.2 Studies of malware risk in relation to web browsing behaviour

2.6.4 Web-based security threats: counter-measures

Cybersecurity and information security vulnerabilities may be categorised overall as arising from three possible sources: malicious activity, facilitating behaviour by end-users, and inadequate technical protection measures (Leitold, 2016; see Figure 2.9, below). The different types of defences and counter-measures may thus be classified as either technical or social. Either category may be further divided to include approaches of prevention, detection, reaction or deterrence (Fléchais, Riegelsberger, & Sasse, 2006): see Table 2.3 below. Cybersecurity is rapidly evolving: web security risks change over time as new vulnerabilities are discovered, and new defences and new versions of application frameworks, web servers, operating systems, browsers, plugins and extensions are developed (Sullivan & Liu, 2012). Vulnerabilities in browsers or browser extensions are widespread, particularly in older browsers (Cova, Kruegel, & Vigna, 2010; Grossman, 2012; McCormack, 2016). Acrobat Reader, and which render different languages, such as Flash, have proved to be a major security concern (Hoffman, 2012; Skoudis, 2005). While browser security has generally improved, plugins (software that interfaces with the browser) which play media files, including QuickTime and Acrobat Reader, and render different languages, such as Flash, have proved to be a major security concern (Hoffman, 2012; Skoudis, 2005). The ActiveX framework within Microsoft Internet Explorer has long been recognised as a security threat, although recent versions have been “sandboxed” to a much greater extent than previously (Lambert, 2013). (A sandbox may be described as “an isolated computing environment in which a program or file can be executed without affecting the application in which it runs” (“Sandbox”, 2005)). Recently Java has been targeted extensively by hackers, leading some security researchers to recommend that the Java Runtime Environment (JRE) should be disabled on end-users’ computers unless required for business reasons (F-Secure, 2012).

Internet Explorer version 6 (IE6) was notoriously insecure, and its use was deprecated by Microsoft (Reisinger, 2011) and by the Department of Health Informatics Directorate, which, in 2010, recommended upgrading to IE7 (DH Informatics Directorate, 2010). However, its use was continuing in parts of the NHS, no doubt because of compatibility issues with a range of critical “legacy” applications (Arthur, 2010; NHS Networks, 2013).

Recommended security measures to reduce the risk of drive-by downloads and other web-based attacks include standardisation of browsers, applications and plugins, auto-updating of browsers and critical applications; disabling of Java except where specifically needed; blocking of inappropriate categories of web content; reputation-based URL filtering to screen out compromised or malicious websites, use of strong passwords, and control of applications at the endpoint (Sophos, 2016a).

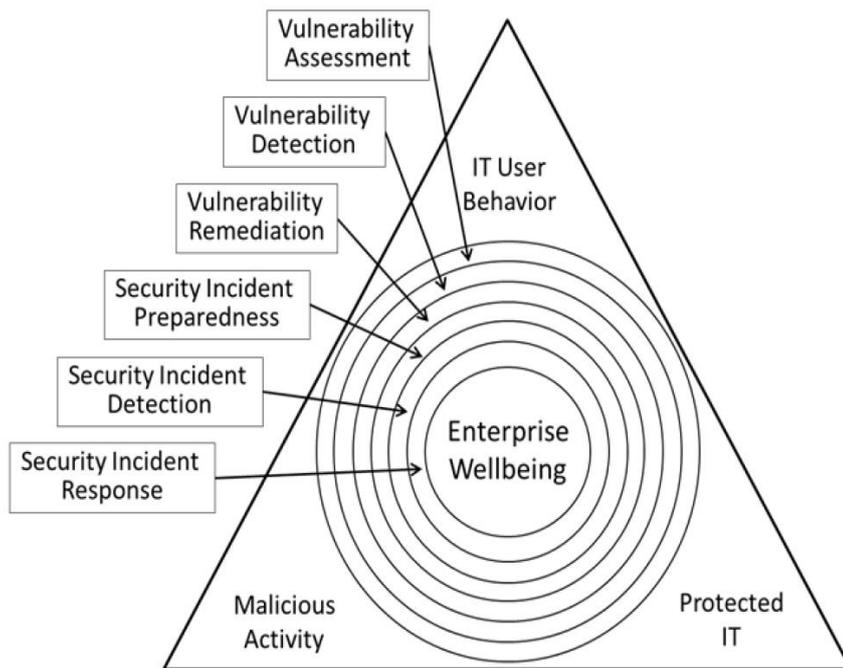


Figure 2.9 Triunal model of cybersecurity vulnerability

From Leitold (2016), p. 4, Reproduced by permission

Further defences include browser-based warning services (Firefox, Chrome, Safari, IE8, IE9); and web-hosted link checking services (Bradbury, 2010). Technical and social information security counter-measures are illustrated in Table 2.3 above, and are discussed further in Section 2.7.3 below. Technical defences against malware and unauthorised network access are of various types.

Spam filters, as the name implies, filter out spam (unwanted and unsolicited email) and suspected phishing messages, and prevent them from reaching users' inboxes. *Anti-malware (anti-virus) systems* afford varying degrees of protection against known threats. They are commonly required to be installed on all desktop machines connected to the network or with access to the Internet, on servers and on mobile devices.

	Category	Description	Examples
Technical countermeasures	Prevention	Stop attacks from happening	Firewalls, secure web gateways, intrusion prevention system Appropriate system permissions Encryption and / or password protection of portable media and devices
	Detection	Notice and identify an attack	Intrusion detection systems User monitoring
	Reaction	Stop or mitigate an attack in progress	Automated response mechanisms linked to intrusion detection systems
	Deterrence	Discourage misuse	Awareness / visibility of technical countermeasures, e.g. individual user monitoring, website blocking
Social countermeasures	Prevention	Stop attacks from happening	End-user information security good practice: prohibition of password sharing, use of encrypted and / or password-protected portable media and devices Acceptable use policies User education: detection of social engineering, basic security measures
	Detection	Notice and identify an attack	System administrators Alert users Audit
	Reaction	Stop or mitigate an attack in progress	System administrators or emergency response teams
	Deterrence	Discourage misuse	SWG warnings to users when websites are blocked Internal disciplinary sanctions Possibility of criminal prosecution for illegal activity

Table 2.3 Technical and social information security counter-measures

Based on / updated from Fléchais, Riegelsberger, & Sasse (2006), p. 1

Intrusion detection systems (IDS) work rather like burglar alarms; they monitor network traffic and log or notify of any possible malicious activity. Host-based and network-based *intrusion prevention systems* (IPS) are able to exercise access control to protect computers or networks from exploitation, and also have the ability to take immediate action, based on a set of rules established by the network administrator.

The *firewall* is a key component of any network security infrastructure: it is a device (hardware or software) which functions in a networked environment to prevent communications forbidden by the security policy. It has the basic task of controlling traffic between different zones of trust, e.g., between the Internet (low trust) and an organisation's internal network (high trust). There are four main classes of firewall: packet filter firewalls, stateful inspection firewalls; application proxy firewalls, and deep packet inspection firewalls, also known as next-generation firewalls (Honan, s.d.). All types of firewall have common characteristics in that they distinguish good from bad network traffic according to a set of criteria (Gattine, 2014). Network perimeter firewalls are unable to

prevent cyber-attacks on web applications. Next-generation firewalls, however, vary in the features they provide; they can be configured to provide control of access to websites and web applications at a detailed level, as well as bandwidth management (Ferrar, Wood, Penny, & Date, 2009; Sullivan & Liu, 2012). *Data loss prevention* (DLP) solutions relate to information security specifically, they may be implemented to protect against data loss via email or social media.

An important type of security device commonly used within the NHS is the secure web gateway (SWG), a type of web proxy. The popularity of these as security devices has increased in response to the increased incidence of web-borne threats, as described above (Roiter, 2007). All web traffic has to pass through the SWG, which has two roles: 1) it performs security-related tasks such as authorisation and authentication relating to web content requests sent from a user's browser, rejecting requests which do not meet the configured criteria; 2) it examines the requested content for malware and other threats before sending it to the user. SWGs are able to categorise URLs and to analyse and manipulate scripts on web pages (Blue Coat Systems, 2015).

The Google, Yahoo and Bing search engines incorporate screening for compromised websites; safe sites are indicated as such in search results (Ranadive, Demir, Rizvi, & Daswani, 2010). All the browsers in common use offer extensively customisable security configuration options which can reduce the attack surface. Within an institutional network, such configuration options may be restricted by group policies. However, higher security settings may result in considerable loss of browser functionality and inability to access content or applications, thereby potentially conflicting with business need.

It should be recognised that there is no such thing as an impenetrable digital defence (Austin & Darby, 2003): the overall aim should be to maximise network resilience (Scully, 2011). It is commonly recommended that a layered or integrated approach to network security is implemented within organisations, involving a combination of devices and strategies, to reduce the probability of cyber-attacks, mitigate their impact when they inevitably occur, and to assist recovery from them. As well as implementing security devices as described above, it is advocated, in addition, that steps be taken to reduce attack surfaces, such as standardising user applications, implementing system policy restrictions limiting downloads to approved sources, "hardening" network operating systems through restricting system permissions, and segregating applications within the network (e.g. Ferrar et al., 2009; Oltsik, 2013). Security functions may be unified within a single unified threat management (UTM) system, or reports of security events from different systems may be integrated

via use of a security information and event management (SIEM) system. These latter are, however, expensive and complex to implement (Lawton, 2015).

Sections 2.6 and 2.7, being closely related, are summarised and synthesised together in 2.7.4.

2.7 Risk in information security and cybersecurity

2.7.1 Theories of risk; factors influencing risk assessment

Risk is a complex and ambiguous concept with an interesting cross-disciplinary history, as outlined by Althaus (2005) and Hay-Gibson (2008). The Royal Society report of 1992 defined risk as “the chance, in quantitative terms, of a defined hazard occurring.” (Power, 2004, p. 53). In the context of IT, the National Institute of Standards and Technology (NIST) handbook (2001, cited by Gerber & von Solms, 2005) defined risk as “the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence” (p. 21). Zinn (2005, p. 1) characterises this type of technical / scientific understanding of risk as “an objective concept relating to the management of future uncertainties through rational action based on calculations of probability”. For Douglas, (1994, p. 30), by contrast, the essence of the concept of risk is that of “danger from future damage”. This definition, unlike the previous one, does not make a conceptual connection between risk and measurable probability (Power, 2004, p. 53; Joffe, 1999).

It should be noted that sociological approaches to risk may be classified as either “weak constructionist” or “strong constructionist” in their epistemology (Lupton, 2009). The “risk society” (Section 2.5.4) and “cultural symbolic” approaches may be classified as “weak constructionist”: risk is understood as socially constructed, but there is posited to be a world “out there”, although it is not directly knowable; risks are both socially constructed and objective (Zinn, 2006). This accords with a critical realist epistemology (see below, Section 3.2.5), and is broadly the approach followed by the researcher in this thesis. Within this perspective, undesirable events are always to some extent socially defined or socially constructed, and “real” consequences are always mediated through social interpretation and linked with group values and interests (Renn, 2008a).

“Strong constructionist” approaches, by contrast, reject the notion that something can constitute a risk “in itself”; from these viewpoints a risk is never knowable outside particular belief systems and moral positions. Lupton (1999, pp. 49-50) offers a useful typology of epistemological approaches to risk in the social sciences: see Table 2.4 below. Realist approaches to risk and risk management are discussed in relation to information security / cybersecurity in Section 2.7.2.

<i>Epistemological position</i>	<i>Associated perspectives and theories</i>	<i>Key questions</i>
<p><i>Naïve realism:</i> Risk is an objective hazard, threat or danger that exists and can be measured independently of social and cultural processes. Risk perceptions may be distorted or biased through social and cultural frameworks of interpretation</p>	Technico-scientific perspective	<p>What risks exist? How should we measure and manage them? How should information about risks be effectively communicated to the public? How to reduce 'bias' in the public's responses?</p>
	Cognitive psychology	How do people respond cognitively to risks? What world views shape their responses?
<p><i>'Weak constructionist/critical realism'</i> Risk is an objective hazard or danger that is inevitably mediated through social and cultural processes and can never be known in isolation from those processes</p>	<p>'Risk society' perspective 'Cultural symbolic' perspective</p>	<p>What is the relationship of risk to the structures and processes of late modernity? How is risk understood in different sociocultural contexts? Why are some dangers understood as 'risks' and others not? How does risk operate as a symbolic boundary measure? What are the situated contexts of risk?</p>
<p><i>'Strong' constructionist:</i> Nothing is a risk in itself – what we understand to be a risk (or hazard, threat or danger) is the product of historically, socially and culturally contingent 'ways of seeing'</p>	<p>Governmentality perspective Post-structuralism Biophilosophy</p>	How do the discourses and practices around risk operate in the construction of subjectivity, embodiment and social relations? How does risk operate as part of governmental strategies and rationalities? How are risk assemblages configured?

Table 2.4 Epistemological approaches to risk in the social sciences

Lupton (1999), p. 49-50

Reproduced by permission

An extensive body of research exists on how individuals perceive and act in the face of risk, which has been reviewed by Maule (2004), by Nurse, Creese, Goldsmith, & Lamberts (2011) and by Parsons, McCormac, Butavicius, and Ferguson (2010). One strain of this research suggests that

people's cognitive capacities in relation to risk are limited and, as a result, they often use "heuristic" forms of thinking based on simple rules. Slovic (1982, cited by Quigley, Burns, & Stallard, 2015) suggested that heuristics in relation to risk may be classified in relation to two primary dimensions: unknown risk and dread risk. People may be more concerned with risks that are not observable or well understood (unknown), or with uncontrollable, hence potentially catastrophic, risks (dread). Their risk assessments may be based on how people feel about a situation (the affect heuristic) or on availability (the ease with which an episode can be recalled (the availability heuristic). This suggests that the perceived risks associated with events that are available (readily visualised, that are of recent occurrence, or are of high personal significance, and hence can readily be brought to mind) tend to be set too high; conversely, those that are associated with events that are hard to visualise or recall are often set too low. Representativeness is another heuristic, whereby decisions are made by identifying and classifying the problem as that of a known type based on previous experience (West, Mayhorn, Hardee, & Mendell, 2008). Use of such heuristics is likely to lead to biased judgements in relation to risk.

Other forms of bias in risk perception and decision-making relating to risk have also been identified. These include the optimism bias (adverse events are far more likely to occur to others than to the subject), the omission bias (omissions are perceived as less risky than acts) and the influence of familiarity (familiar risks are perceived as less severe than unfamiliar ones). Pressures of time, and lack of knowledge and understanding of a risk, leading possibly to bounded rationality or "satisficing" behaviour (Section 2.4.2), may be a factor. Also, individual users and organisations may unconsciously maintain an "acceptable" level of risk, increasing their levels of risk-taking within environments in which security measures are increased, a process known as risk homeostasis (Kearney, 2016; Stewart, 2004; Wilde, 1998).

The following section outlines three social theories relating to bounded rationality in the understanding of risk which are relevant to the research: the cultural hypothesis, the social amplification of risk, and the social representations theory.

Douglas and Wildavsky's cultural theory of risk, also called the cultural hypothesis, refers to the tendency of persons to form perceptions of risk that reflect their involvement with a particular "cultural way of life" (Kahan, 2008). Risk perception is considered specifically in relation to the two cross-cutting dimensions identified by Douglas and Wildavsky of *grid* and *group*. *Group* here refers to the strength of the group ethos, whereas *grid* is concerned with the extent of social constraints

on behaviour within the group. In relation to these two dimensions of social organisation, the authors identified four characteristic individual and group approaches to risk: *hierarchists*, *egalitarians*, *individualists*, and *fatalists*. *Hierarchists* (high group and high grid) are inclined to respect authority, to have confidence in institutions, to conform closely to group expectations and norms relating to risk, and to have a propensity to trust routine procedures for risk management; *egalitarians* (high group and low grid), are distrustful of externally imposed norms and have a participatory attitude to risk; *individualists* (low group and low grid) tend to take a positive view of risk-taking as bringing benefits, support self-regulation of risk, and are inclined to trust individuals rather than organisations; *fatalists* (low group and high grid) lack group cohesion but are otherwise constrained in their behaviour, tending to trust to luck or fate in relation to risk (Douglas & Wildavsky, 1982b; Lupton, 2009). Renn's (2008a, citing Thompson, 1980) development of the cultural theory of risk identifies similar categories: *bureaucrats*, *egalitarians*, *entrepreneurs*, *atomized individuals*, with the addition of a fifth category, *hermits*. Renn's approach describes these typical combinations of values, world views, and convictions as what he terms "cultural prototypes"; these have characteristic specific viewpoints on risk topics, as well as corresponding attitudes and coping strategies; see Figure 2.10, below.

The cultural theory of risk makes two characteristic claims. The first is that attitudes to risks tend to vary according to "cultural way of life". The second is that individuals base their beliefs about the risks and benefits of a putatively dangerous activity on their cultural appraisals of these activities, based on the way of life to which they are committed (Kahan, 2008; Kahan, Braman, Slovic, Gastil, & Cohen, 2009, citing Douglas & Wildavsky, 1982). It is suggested, moreover, that the different "cultural ways of life" each generate a characteristic set of general attitudes and values, variously referred to as a cosmology or cultural bias, which act as filters in evaluating information relating to risk; the notion of *cultural cognition of risk* (Rippl, 2002).

The framework of social amplification of risk (Kasperson et al., 1988; Renn, 2008; Renn, Burns, Kasperson, Kasperson, & Slovic, 1992) was designed to integrate psychological, social, and cultural factors of risk perception and risk responses. It denotes "the phenomenon by which information processes, institutional structures, social-group behavior, and individual responses shape the social experience of risk, thereby contributing to risk consequences" (Kasperson et al., 1988, p. 181).

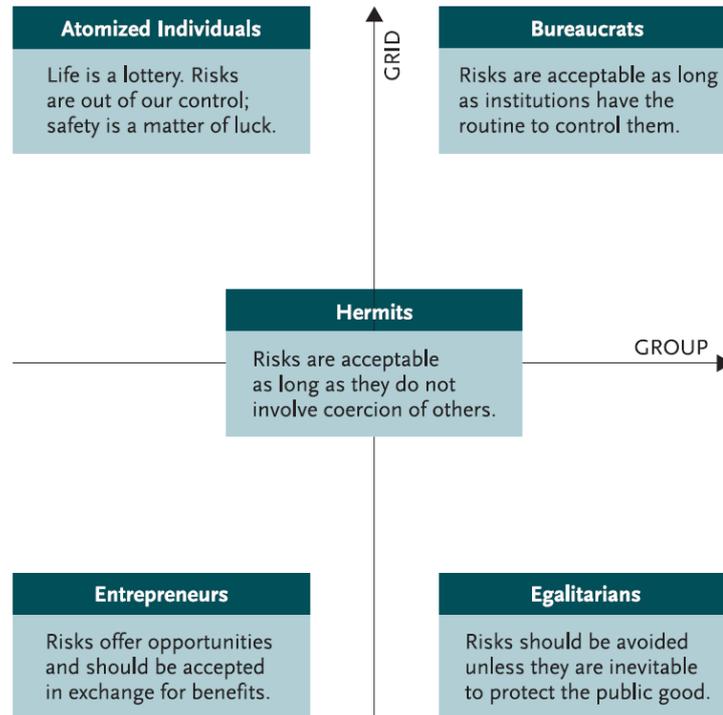


Figure 2.10 Cultural prototypes and their perspectives on risk

Grid = extent of acceptance of formal systems of hierarchy and procedural rules

Group = extent to identification with a social group

Renn (2008a, p. 62)

Reproduced by permission

Processes of “amplification” in this framework include those which both intensify and attenuate indications of risk. These begin either with an adverse event (such as a data breach) or with the recognition of an adverse effect (such as the discovery of a cybersecurity flaw). In both cases, individuals or groups act as “amplification stations”: they select specific characteristics of the events or aspects of the relevant reports and interpret them according to their perceptions and mental models; these interpretations are subsequently communicated to other individuals and groups. Amplification stations can include the conductors of technical risk assessments, risk management organisations, professional and popular news media, individual opinion leaders, personal networks, and public agencies. Messages from the stations may contain meanings which are factual (relating to the message content), inferential (the conclusions that may be drawn from it), value-related (in relation to existing standards) and symbolic (evoking specific images and cultural associations).

Social interactions can heighten or attenuate perceptions of risk; by shaping perceptions of risk, they also influence behaviour relating to the risk. Behavioural patterns, in turn, may generate secondary consequences, such as litigation, regulatory responses, loss of trust and public concern. Such secondary effects can trigger demands for additional institutional responses and protective actions, or, in the case of risk attenuation, impede the installation of protective actions. The processes are illustrated in Figure 2.11 below.

The *social representations theory* (Moscovici, 1988) concerns social cognition: it is relevant both to the theory of innovations (Section 2.8 below) and to risk. A social representation is “a system of values, ideas and practices with a twofold action: first, to establish an order which will enable individuals to orient themselves in their material and social world ... and secondly to enable communication to take place among the members of a community by providing them with a code for social exchange and a code for ... classifying ... the various aspects of their world and of their individual and group history” (Moscovici, 1998, p. 12).

It addresses the complexity of the meanings made by individuals positioned within specific social contexts, referring both to the process through which representations are elaborated and to the structures of thought that emerge from those processes (Duveen, 2000, cited by Joffe, 2003). It is interpretivist in its basis; it claims that representation is fundamentally a social process, and that particular social representations, once developed and elaborated, constitute our reality.

Within the theory, social representations are viewed as socio-cognitive in nature, meaning that they are not merely imposed on the individual agent by the community, but are generated by agents’ own reflective process and experiences (Vaast, 2007). Two specific processes are used when people build representations of events: *anchoring* and *objectification*. Anchoring refers to the way in which new knowledge is understood and integrated through a process of relating it to familiar categories and concepts, so that new risks are understood in relation to existing ones; objectification is the process whereby an abstract theory is made concrete, or new meaning is given to objects: available information is classified, selected, simplified and de-contextualised (Abric, 1993; Vaast, 2007).

Social representations are closely linked to social identity (Elejabarrieta, 1994) and to organisational culture (Kummerow & Innes, 1994). The theory maintains that common sense, or lay understandings, are all too often denigrated and seen as inferior to other forms of knowledge, such as scientific or expert knowledge (Flick & Foster, 2008). In a social representations perspective, expert knowledge is not privileged; different communities are not either “ignorant” or

“knowledgeable” about, for instance, a risk issue (such as information security), but know different things about it. Thus, in Vaast’s (2007) study of social representations of information security within health services, clinicians associated it with the security of patient information, respect of patients’ privacy, and regulatory compliance, whereas IT professionals saw it mostly as a technological issue and defined it in terms of systems security (hardware, software, network security and data integrity). The theory finds a particular application in relation to social media adoption (Kaganer & Vaast, 2010), as discussed in Section 2.8.4 below. The overall relevance of these social theories of risk to information security risk assessment and management will be readily apparent; compare also the discussion of the “political” aspect of risk identification in Section 2.5.5.2 above.

2.7.2 Risk management and organisational trust in cybersecurity and information security

2.7.2.1 Introduction

Information security as well as cybersecurity risk management policies and practices can affect information seeking in a variety of ways, as will be evident from the discussions above of requirements for encrypted mobile storage (1.4.4), restrictions on forms of “shadow IT” (2.8.3), access and authentication requirements (1.4.5, 2.6.1), etc.

A substantial element of information security / cybersecurity risk is considered to arise from user behaviour (e.g. Leitold, 2016; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005). *Internal threats may* be categorised as passive / non-volitional (e.g. arising from lack of security common sense or forgetting to apply security procedures); volitional but not malicious (users taking inappropriate risks due to ignorance); and intentional / malicious or harmful (deliberately malicious or negligent acts) (Box & Pottas, 2014). Many questions therefore inevitably arise in relation to the risk management of web use within organisations, which the review endeavours to address:

1. How can the inevitable risks arising from web-based security vulnerabilities and threats (as discussed in 2.7.1 above) be assessed appropriately? (2.7.2.3)
2. How do end-users perceive information security / cybersecurity risk in relation to web use? (2.7.2.4.2)
3. What factors underlie web-related computer misuse by employees, whether intentional or unintentional? (2.7.3.1)
4. Do information security policies or acceptable use policies influence end-users’ behaviour? How far can users be trusted to comply with acceptable use policies? (2.7.3.2.1)

5. How effective are training and awareness interventions aimed at reducing user-related incidents involving web use? (2.7.3.2.2)
6. How do organisations respond to information security incidents? (2.7.2.4.1)
7. How do security managers perceive information security / cybersecurity risks in relation to web use, and how do they make decisions relating to them? (2.7.2.4.1)

2.7.2.2 What constitutes risk management in cybersecurity / information security?

Risk management in the context of information security / cybersecurity may be defined as “the process that allows business managers to balance operational and economic costs of protective measures and achieve gains in mission capability by protecting business processes that support the business objectives or mission of the enterprise” (Oost, 2010, p. 216, citing Peltier, 2004). The core aspects of risk management involve a Plan-Do-Check-Act cycle, as described by Jones (2007), consisting of the following processes: Identify risks [Act], Assess risks [Plan], Treat risks [Do] and Monitor and report risks [Check], the details of which are given in Appendix K. Such a process is prescribed for the NHS in the document *Information security management: NHS code of practice* (NHS Connecting for Health, 2007); see above, Section 1.4.4. Within [Act], risk evaluation criteria, impact criteria and risk acceptance criteria need to be established. Assets (data, hardware, software and network) in relation to the consequences of loss need to be identified, as do threats and vulnerabilities (Millar, 2016). Treating, monitoring and reporting risks ([Do] and [Check]) represents the work of risk management proper, described as “planning, monitoring and controlling activities which are based on information produced by risk analysis activity” (Gerber & von Solms, 2005, citing Scarff et al., 1993).

Risks may be treated in four ways: *risk modification*, *risk retention* (accepting risks according to the criteria established in [Act]), *risk avoidance* and *risk sharing*. Treating risks usually involves removing or reducing threat sources, addressing vulnerabilities, and lessening, as far as possible, the impact of negative events (Fischer, 2016 – add citation). Controls, the selection of which is generally based on a cost/benefit ratio unless the risk is particularly severe, are intended to treat risks by reducing them to an acceptable level (Millar, 2016). Controls “promote a preferred behaviour of the system being controlled” (Aken, 1978, cited by Dhillon, 1999). An information security policy should determine the nature and overall framework of the controls applied (Dhillon, 1999).

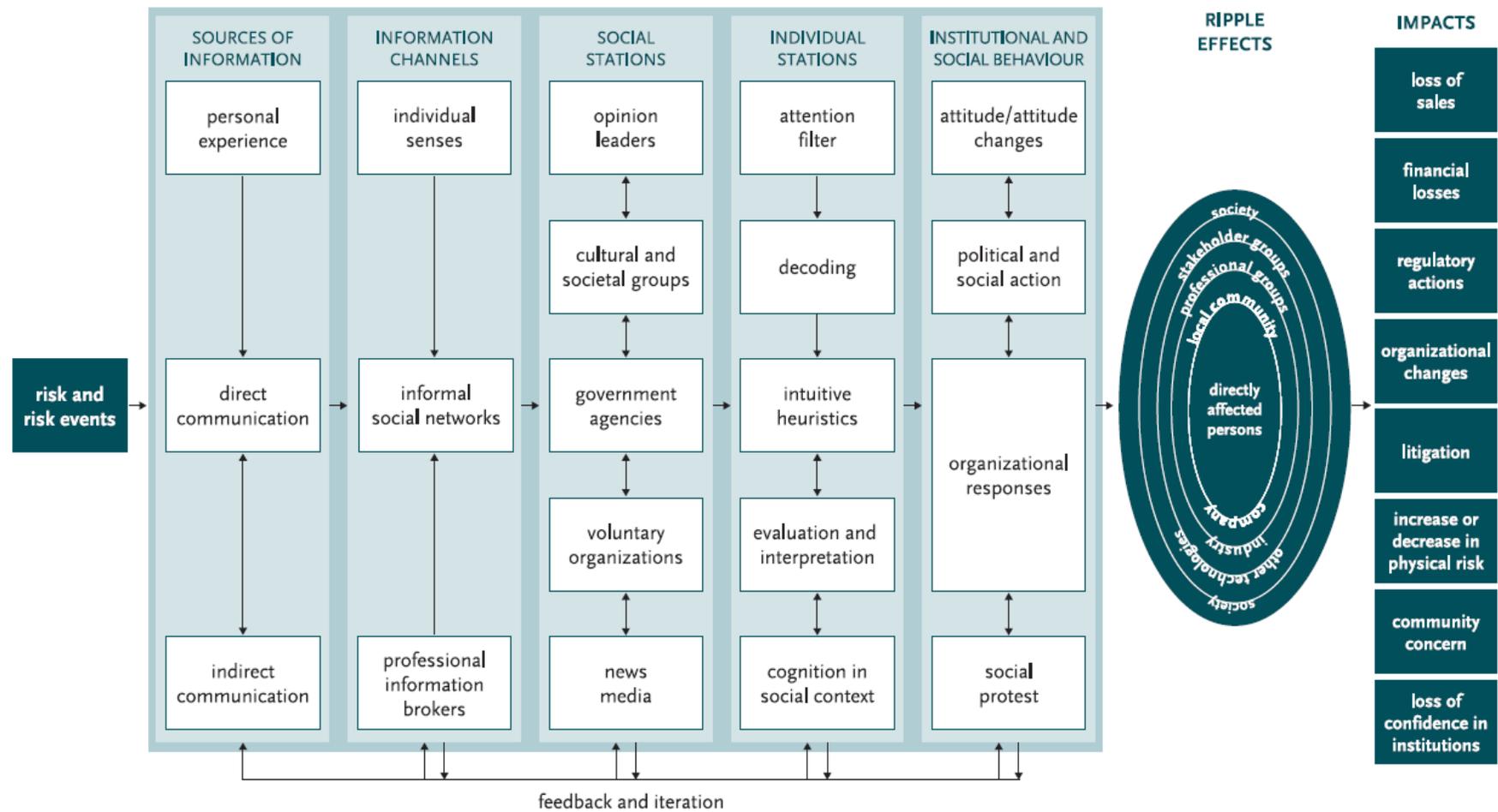


Figure 2.11 The social amplification of risk

Renn (2008b), p. 197

Reproduced by permission

2.7.2.3 Assessment and analysis of cybersecurity / information security risks

While cybersecurity risks relating to specific forms of online behaviour, as described in Section 2.6.3, are not well understood, technical cybersecurity vulnerabilities in general are relatively well documented. Extensive research efforts have been devoted to developing taxonomies of them in an effort to provide frameworks for systematic security assessments; these are reviewed by Ijure and Williams (2008) and by Joshi, Singh, and Tarey (2015). Taxonomies in common use include Common Vulnerabilities and Exposures (CVE) (MITRE Corporation)⁴⁵ and the Open Web Application Security Project (OWASP) Periodic Table of Vulnerabilities.⁴⁶ It should be evident however that, given the complex and rapidly evolving threat landscape, which can present hitherto unknown risks, and the uncertain judgments involved in the identification of risks and in both quantitative and qualitative risk analysis methods, information security / cybersecurity risk management is an inherently chance-ridden and subjective process, and can never be 100% certain of success (Gerber & von Solms, 2005, Ijure & Williams, 2008). In any computer application there is almost always a trade-off between security and functionality (Besnard & Arief, 2004; Post & Kagan, 2007), and the relationships between risks, vulnerabilities, threats and security measures can be very complex: for example, one threat can attack several different vulnerabilities, one measure can protect against multiple threats, or one asset will require protection via several different security measures (Bojanc, Jerman-Blažič, & Tekavčič, 2012). Oppliger (2015) suggested that quantitative risk analysis approaches are impossible to apply outside laboratory settings, since insufficient information is available to estimate either the probability of occurrence or the extent of the expected damage in a meaningful way. Similarly Utin, Utin, and Utin (2008, p. 168) suggested that “information security risk management quantitative analysis is more an art than a science and cannot be relied upon to produce consistent and trustworthy data”. Stewart (2004) was strongly critical of much current professional thinking in information security risk assessment, contending that it is both precautionary in character and also commercially driven. He disparaged the current attitudes and predispositions of information security / cybersecurity professionals as they related to the commercial security industry as a manifestation of groupthink (Pidgeon, 1998; Rose, 2011; Turner & Pratkanis, 1998). Quigley *et al.* (2015) concluded from their examination of cybersecurity discourse, based partly on the body of research on the psychology of risk perception discussed above in Section 2.7.1, that cybersecurity risks are often over-simplified and over-dramatised within popular literature, and that the probability of some

⁴⁵ Common Vulnerabilities and Exposures (CVE): <https://cve.mitre.org/>

⁴⁶ OWASP Periodic Table of Vulnerabilities: <http://www.owasp.org>

cybersecurity risks to critical infrastructures (such as health services) are over-estimated. Baskerville (1991) preferred to understand information security risk analysis methods as a means of recording and manipulating sociological, rather than natural, events, and as a valid means of generating contextually-situated professional knowledge using intuitive judgements. There appeared to be a wider issue of the applicability of different models of information security, i.e., technical or social, and hence of different approaches to social theory, and of the application of different paradigms (Burrell & Morgan, 1979) to security (Jones 2002, Drake & Clarke 2001); cf. the discussion of information security service culture in Section 2.7.2.4.1 below. Drake and Clarke went so far as to suggest that information security had hitherto been approached as a “pseudo-scientific domain” (2001, p. 2). They proposed a “critically normative approach” as an alternative.

2.7.2.4. Characteristics of information security / cybersecurity risk perception and decision-making

2.7.2.4.1 IT professionals

It is important to establish how decisions are made in respect of user-related cybersecurity /information security risks, particularly regarding the implementation of technical controls. The processes of information security managers’ decision-making were investigated by Pettigrew and Ryan (2012) via a series of 23 interviews with experts and leaders in the information security community. They found that a range of different criteria were used in self-evaluation: these included compliance; a combination of compliance, intrusion prevention, content filtering, and patch management; securing adequate investment for IT security; and degree of success in building a social environment. Njenga and Brown (2012), identified via hermeneutical analysis and interpretation of interview data a considerable element of improvisation in information security managers’ decision-making rather than a total dependence on rational choice techniques. Werlinger and associates (Botta, Muldner, Hawkey, & Beznosov, 2010; Werlinger, Hawkey, & Beznosov, 2009; Werlinger, Hawkey, Botta, & Beznosov, 2009) conducted a wide-ranging investigation of the human, organisational and technical factors in information security from the perspective of practitioners. They found that much decision-making in information security management was tacit in nature. Significantly, “open environments and academic freedom” were perceived as an organisational challenge for information security management: “You’re constantly trading access versus risk” (Werlinger, Hawkey, & Beznosov, 2009, p. 11). So also were the distribution of IT responsibilities across organisational units, and use of mobile devices.

Within the topic of IT staff subcultures (2.5.3) there is the particular issue of what Rastogi and von Solms (2012) describe as *information security service culture*: the pattern of shared values and beliefs among the staff responsible for information security. While many IT professionals and information security researchers would concur with the view that end-users are an important cause of security breaches, what Schneier (2000) described as the “weakest link”, their perceptions of end-users and their role in information security may vary widely. It was noted above (2.5.3) that a tendency to blame end-users for systems failures, with a corresponding distrust of end-users, and desire to restrict end-user functionality, were identified as characteristic of IT subcultures. McFadzean, Ezingard, and Birchall (2006) and Rastogi and von Solms (2012) related this difference in perspective to different paradigms operating within information security research and practice. Information security service culture, according to Rastogi and von Solms, depends critically on the assumptions made about end-users and about the organisation by information security managers and system developers. Such assumptions may be described in terms of the concept of technological frames (Orlikowski & Gash, 1994). Technological frames, which the authors define as “core sets of assumptions, expectations and knowledge of technology collectively held by a group or community” (p. 199), may powerfully influence overall design and use of technologies within the organisation.

The authors also drew upon Burrell and Morgan’s (1979) account of paradigms in organisational analysis, as adapted by Hirschheim and Klein (1989), to characterise the mind-set of developers. According to this analysis, system developers, adhering to a functionalist paradigm, and assuming a stable organisational reality, tend to assume the validity of the organisational objectives with which they are presented, failing to appreciate that they may be the subject of considerable disagreement. (Functionalism is defined by Burrell and Morgan (1979, p. 26) as an overall approach which “seeks to provide essentially rational explanations of social affairs”.) Information security managers, for their part, adhering strictly to the same functionalist paradigm, see security primarily as a technical/administrative matter which can be implemented simply via hardware and software controls. They typically approach their task in a “command and control” fashion, remaining isolated from actual end-users, being unwilling to understand their perspective or to negotiate with them, and continuing to rely on their own preconceptions (Ashenden, 2008; cf. Hedström, Kolkowska, Karlsson, & Allen, 2011). The contrasting perspective sees cybersecurity / information security as essentially a socio-technical endeavour (Hedström, Karlsson, & Kolkowska, 2013). The latter perspective, assuming as it does the “mutual constitution of people and technologies” (Sawyer & Jarrahi, 2014, p. 5-1), emphasises the need for security to be as usable as possible, and also the necessity of organisational commitment, that is of aligning security policy and practices with organisational strategy and culture

via the involvement of business areas other than IT in policy development and implementation (Fléchaïs & Sasse, 2009; Kayworth & Whitten, 2010; Koskosas & Siomos, 2011; Koskosas, 2013; Maynard, Ruighaver, & Ahmad, 2011; Siponen & Oinas-Kukkonen, 2007; Spears & Barki, 2010; Woodhouse, 2007).

Albrechtsen and Hovden (2010) suggested that relationships between end-users and information security managers are typically characterised by incorrect perceptions, distrust and antagonism; this, they claimed, leads to a bureaucratic, “policing” approach to information security policy and controls, and to a reliance on technological tools as a means of controlling and monitoring end-user behaviour. This, in turn, tends to lead to end-user resistance and non-compliance. Kolkowska (2011) investigated, via a qualitative case study, using both semi-structured interviews and documents, the respective attitudes and values of IT professionals and end-users (lecturers, research staff and PhD students) within two academic departments of a Swedish university regarding information security matters. Twelve end-users were interviewed in department one and seven in department two, with four IT professionals interviewed in each department. Schein’s three-tier model of organisational culture (artifacts, espoused values and basic assumptions) (Schein, 1996; see Section 2.5.1 above) was used to provide a conceptual foundation. Kolkowska’s study uncovered further complexities of information security service culture, in that she identified conflicts both between the basic assumptions held by IT professionals and users, and, within information service cultures, between IT professionals’ espoused values and their basic assumptions. Basic assumptions were identified from behaviour and from visible structures and processes (artifacts). Conflicting assumptions between IT professionals and end-users in department one concerned: security responsibilities; the scope and limits of end-users’ freedoms in relation to computer use; and protection of information and IT resources. Conflicting espoused values and basic assumptions in department one were observed in relation to protection of information: IT professionals stressed the responsibilities of end-users for protection of person-identifiable or confidential information, but the author found no visible structures or processes supporting this. In department two, information security was managed by the IT professionals in a top-down, “professionals know best”, fashion, in contradiction of their espoused values of respect, dialogue, communication and cooperation. Other conflicts arose in relation to standardisation and control (IT) versus creativity and flexibility (end-users); control (IT) versus freedom (end-users); planning (IT) versus flexibility in relation to support requirements; implementation of technical controls (IT) versus need for trust and respect (end-users); and appropriate level of involvement of end-users in information security strategy and decision-making.

It should be noted that the purpose of risk management is not solely about the avoidance of risk to minimise losses, but also about the need to take risks to reap rewards (Hirsch & Ezingard, 2008, 2009); the terms “risk appetite” and “risk tolerance” are used to refer to and define the quantity and nature of risk that organisations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility (Whitman & Mattord, 2010).

A phenomenon of interest relating to the formulation of access controls in relation to information security or cybersecurity is that of the *empathy gap*, as identified by Smith and associates (Smith, 2012; Wang, Smith, & Gettinger, 2012), rooted in forms of cognitive bias. Their work related to the specification of access controls within EPR systems, where they found that the wording of experimental scenarios (abstract / role-based, as compared with placing the participant in a live clinical setting), affected the extent to which access was constrained with the policies that were devised by the research participants. It seems possible that such empathy gaps could be a factor also in the setting of web access controls to published information or web applications, in addition to those relating to the differing professional backgrounds of IT and information governance professionals and clinician end-users; cf. Section 2.7.1.

It was mentioned in Section 1.4.4 that information governance, including information security, tended to become a higher strategic priority in NHS organisations that had experienced data breaches. This informal observation accords with a number of research findings in other types of organisations. Goodhue and Straub (1991; cited by Farahmand, Atallah, & Konsynski, 2008), based on their questionnaire surveys of IT professionals and end-users, argued that managerial concern about an organisation’s security is a function of 1) the risk inherent in the industry 2) the extent of the effort already made to control these risks, and 3) individual factors such as awareness of previous security breaches, background in security work, etc. Ezingard, Bowen-Schrire, and Birchall (2007), conducted interviews (n=26) among information security managers of companies in Sweden and the United Kingdom to test a number of hypotheses: that an organisation’s information security management practices are influenced by the board’s and senior management’s perception of risk; that there is a link between the perceived strategic importance of information security in the organisation and actual practice; and that adverse information security events, internal or external, are a significant influence on information security practice when deemed to be significant by decision-makers within an organisation. Positive correlations were observed between the frequency of information security reviews and the level of awareness of information security issues among the board (rated as high/medium/low), and between adverse events (n=16) and changes in information security practice, generally initiated by senior management. Volpentesta, Ammirato, and Palmieri,

(2011), who conducted a survey of information security managers of Italian companies (n=106), also found that adverse events heightened their perception of risk. In accordance with the known phenomenon of risk homeostasis, however, it would be expected that such heightened emphasis on security issues would revert over time to its previous level (see above, Section 2.7.1).

2.7.2.4.2 End-users

The importance of understanding end-users' risk perceptions and security decision making as they relate to effective risk communication and user education in respect of cybersecurity and information security has been highlighted by Nurse (2013). Studies of end-users' mental models of cybersecurity / information security have been reviewed by Volkamer and Renaud (2013). End-users' perceptions of risk within the information security / cybersecurity domain have been investigated by Friedman, Nissenbaum, Hurley, Howe, and Felten, (2002), Huang and associates (Huang, Rau, Salvendy, Gao, & Zhou, 2011; Huang, Rau, & Salvendy, 2007, 2010), Harbach, Fahl, & Smith (2014) and Byrne *et al.* (2016); earlier studies were reviewed by Howe *et al.* (2012). These studies have generally been wide in scope, and focused on transactional online activities. The only work found which referred to end-users' perception of risk in relation specifically to information behaviour was that of LeBlanc and Biddle (2012), which investigated users' risk ratings of 20 different online activities in terms of possible benefits: likelihood; immediacy; temporal extent of impact, and severity of negative impact; and frequency. They found that users perceived online searching as a very low-risk activity in relation to possible loss of personal information. Vaast's (2007) study of social representations of information security among different groups of health professionals, which did not focus on risk as such but on threat perception, has been referred to above (Section 2.7.1).

In relation to end-users' risk perception and decision-making, many of the same heuristics and biases known in relation to risk perception in general (Section 2.7.1 above) have been identified within the information security / cybersecurity domain (Smith, 2012; Nurse, 2013). In relation to their online behaviour and security decision making, other important phenomena have been identified which are specific to the domain: *security fatigue* and the (related) *compliance budget*. These are relevant to any security-related behaviour involving decision-making and choice. Furnell and Thompson defined security fatigue in terms of a "threshold at which it simply gets too hard or burdensome for users to maintain security" (2009, p. 7). For Stanton, Theofanos, Prettyman, and Furman (2016), security fatigue is "a type of weariness, a reluctance to see or experience any more of something" as it relates specifically to security. The authors suggested that security fatigue "often manifests as resignation or a loss of control in people's responses to online security" (p. 27).

Beautement and colleagues (Beautement & Sasse, 2009; Beautement, Sasse, & Wonham, 2008; Sasse, 2015; Steves et al., 2014) proposed the important concept of the *compliance budget*, defined as the level of effort that an individual is prepared to expend to comply with information security policies for no personal gain. It is suggested that where information security measures are not enforced technically, users will tend to comply with a security policy only as far as it does not require extra effort, or does not impede their work.

While the relationship of cybersecurity / information security events to specific forms of actual online behaviour is imperfectly understood, end-users' proneness to a variety of non-malicious insecure behaviours online has been conclusively demonstrated in a wide range of studies (e.g. Flinn & Lumsden, 2005; Howe et al., 2012; Stanton, Stam, Mastrangelo, & Jolton, 2005). A literature review by Derbentseva, Fraser, Gibbon, and Hawton (2016) identified ten categories of non-malicious insecure behaviour, as related to: web use (visiting unsafe web pages, downloading files from unverified sources); e-mail practices (opening emails from unknown sources, falling victim to phishing attacks through opening links or attachments); password practices and account protection; removable media; use of network resources outside the organisational perimeter; Web 2.0 and social media; BYOD; system maintenance (failing to update operating systems or anti-malware signatures, not backing up data, ignoring security warnings); and AUP non-compliance. Such problems are highly complex in nature; they are thought to relate to security mechanisms' usability and acceptability to end-users, and their relationship to attitude and motivation, and to decision-making strategies, as well as to perceptions of risk (Derbentseva et al., 2016; Fagan & Khan, 2016; West et al., 2008). In consequence it is common within information security research for end-users to be cited as the "weakest link" in security (Schneier, 2000). Such an assessment may, however, relate primarily to social engineering attacks and users' vulnerability to deception. In consequence, it is frequently thought appropriate to treat risks by applying security controls within organisational networks in a manner that removes users from security decisions as far as possible (Nurse, 2013). It is intuitively apparent that restrictive technical controls are likely to constitute a more prominent element of cybersecurity measures within a corporate environment in which there are limited resources for risk communication and user education in relation to web-related risks. As has been shown (Section 2.6.2 above, Appendix D), there are, in any case, no behavioural defences against some of the commonest threats that arise in the course of online searching, hence supposed deficiencies in risk perception and security decision-making are of limited relevance in relation to these.

Trust necessarily involves the acceptance of risk (Inglesant & Sasse, 2011b), which itself constitutes a risk management approach (Section 2.7.2.1). Consideration of information security risk management naturally leads on to discussion of the role of trust within information security, since trust is commonly defined as “an attitude of positive expectation that one’s vulnerabilities will not be exploited” (Trist & Balmforth, 1951, cited by Inglesant & Sasse, 2011b, p. 2). It is common, following Luhmann (1979, cited by Cofta, 2007), to cite the importance of trust as a social enabler that reduces complexity and transaction costs within organisations, leading to a reduction in management controls, and hence greater efficiency; compare this with the discussion of organisational trust in 2.5.5.3 above. The work of Kirlappos and Sasse (2014, 2015) emphasised the role of organisation-employee trust in information security, and of practices that foster it. However, it is not within the scope of this thesis to pursue this subject in detail here.

The enforcement of acceptable use policies (Section 2.7.3.2, 2.7.3.4.1) by technological means (secure web gateways, group policies etc.) is rarely total (Dubois & Mouratidis, 2010); the organisation has to trust its employees not to circumvent or otherwise negate policies, even if there is strong technological enforcement in place. In the case of policy requirements to uphold copyright legislation, in particular, it is difficult to envisage appropriate means of technological enforcement. The trust placed in employees is nearly always only one part of a web or social and technological power through which security is maintained; power is inscribed and normalised through micro- and macro-level circuits of integration (Clegg, 1989; Inglesant & Sasse, 2011; see above, Section 2.5.6.2). This leads on to the discussion of measures against inappropriate web use in the following section.

2.7.3 Measures against inappropriate web use

2.7.3.1 The problem

As discussed in section 2.7.1, use of the web presents a variety of security risks in itself. All organisations need to address the issue of facilitating legitimate use of the web for work-related purposes by their staff while limiting inappropriate use, in a manner that is not intrusive or demotivating.

Generally, the issue of PWU is treated by researchers without reference to the wider field of behavioural information security; conversely, personal use of the web at work (PWU), as a potential source of risk to an organisation, is only very occasionally addressed within behavioural information security research itself. Inappropriate PWU is varyingly conceptualised (Kim & Byrne, 2011; Schalow et al., 2013). The nature of its effects is strongly disputed; some research shows strongly positive

effects associated with PWU, such as increased productivity and job satisfaction, improved morale, relief of stress and improved work-life balance (Anandarajan et al., 2006; Jiang & Tsohou, 2014; Lim & Chen, 2012; Oravec, 2002). It is self-evident, however, that some forms of personal use of the web at work (sometimes termed “Internet misuse”, “cyberloafing” or “cyberslacking”) can present productivity, security and legal risks to organisations (Bandey, 2011a; Stratton, 2010). Different categories of seriousness may be identified (Blanchard & Henle, 2008; Griffiths, 2010; Weatherbee, 2010). In the United Kingdom and elsewhere personal use of the web at work is relatively common (Whitfield, 2005), and can have serious organisational consequences in terms of an employer’s legal liability for users’ acts. Illegal activities perpetrated by users via their workplace computers for which UK employers may be vicariously liable include possession and distribution of illegal (i.e. paedophile) pornography and other obscene material or racially inflammatory material, racial or sexual harassment, discrimination, hacking, the defamation of management, customers or competitors, software piracy, copyright infringement, fraud, and breaches of the Data Protection Act (Bandey, 2011; Holt, 2004; Willson & Oulton, 1999). Network performance may be degraded as a result of bandwidth being clogged by excessive use of non-work-related sites, and productivity adversely affected. Access to non-work-related websites or web applications is also thought to present increased security risks to corporate networks.

2.7.3.2 Measures against inappropriate web use: deterrence

2.7.3.2.1 *Acceptable use policies*

It is generally considered important, as a deterrent first step in minimising inappropriate web use, that an acceptable use policy (AUP) be in place and be clearly understood by staff (Siau, Fui-Hoon Nah, & Teng, 2002) as part of a wider framework of information security and governance policies. While an evidence base is lacking for the formulation of AUPs that are effective in preventing inappropriate web use (Henle, Kohut, & Booth, 2009), they are frequently cited as an essential component of information security management systems and processes (e.g. Guttman & Bagwill, 2012). Acceptable use policies aim, through the establishment of clear limits on PWU by staff members and contactors, to improve productivity, to minimise or prevent excessive bandwidth consumption, and to mitigate legal liability risks arising from misuse of Internet resources. Among other things, they set out organisational policy on employees’ use of the web, specifying categories of material and activities that are proscribed and establishing the scope of allowable PWU. Individual staff members’ rights and responsibilities regarding Internet technologies are clearly set out, as well as disciplinary sanctions to be applied for infringements of the policy. The scope of PWU that is

proscribed may extend beyond that which presents security risks, or is illegal or potentially illegal, to include a wide range of non-work-related activities and subject matter.

The HSCIC had set out a model AUP designed for adoption by NHS organisations which permitted users to access research material and other information relevant to their work, and to access websites and webmail accounts for personal use so long as this did not interfere with work: details are given in Appendix G. The emphasis here was clearly on the nature and purpose of the activity being pursued, rather than on what was being accessed as such; there was a clear recognition that some material that would otherwise be considered inappropriate could in principle be legitimately accessed by health professionals for work-related purposes.

Social media use in organisations may be addressed as part of wider AUPs or within separate social media policies or guidelines. Policies may address general corporate use, individual use, or both: frequently, no distinction is made between on-duty and off-duty conduct in respect of individual use. The main content components of on-duty social media policies are generally confidentiality and data protection, authority (who is entitled to speak for the organisation on social media, with a corresponding requirement to state identity and issue disclaimers), and arrangements for establishing and managing departmental social media sites, including provisions for appropriate moderation. Regarding individual use, they relate to the mitigation of risks to organisational and professional reputation through the establishment of clear standards of online conduct (“e-professionalism”). It should be noted that social media may be used by organisations either for externally facing functions (e.g. marketing and public relations, staff recruitment) for internal functions (e.g. internal communications, knowledge management), or both (Segers, El Ouiridi, El Ouiridi, & Hendrickx, 2014).

Of the very few research studies have been published of social media policies within health service organisations (Cain, 2011; Fast, Sørensen, Brand, & Suggs, 2015; Henry & Webb, 2014; Scragg, Shaikh, Robinson, & Mercer, 2017), only the last of these was British and related to the NHS. This mixed group of radiography practitioners and academics undertook a grounded theory study of the tone and content of the social media policies of nine NHS Trusts in the north west of England. Tone was categorised as either discouraging, encouraging or enabling. In respect of tone, the policies were mainly discouraging through being prohibitive. In respect of the content, five main themes could be identified: training and education; productivity; security; conduct and behaviour; and

reputation. However, not all were addressed equally: training and education were relatively under-emphasised in comparison with security, which was heavily emphasised.

Acceptable use policies are not generally considered to be effective on their own in preventing inappropriate web use (Anandarajan, 2002; Galletta & Polak, 2003; Mirchandani & Motwani, 2003); they are commonly used in combination with education and training in web searching and/or cybersecurity, preventive measures (web filtering), detection measures (monitoring) and remedial measures (the threat of disciplinary sanctions) as enforcement measures. However, it is suggested that periodic reminders to staff of the content of AUPs can be effective to a considerable extent in reducing inappropriate web use (Shepherd & Klein, 2011; Shepherd, Mejias, & Klein, 2014). There are differences of opinion among IT professionals as to how far non-work-related sites that are still considered acceptable within the terms of the organisation's AUP should be blocked ('IT Slave', 2011). It should be noted that content filtering is not implemented centrally within N3 other than for gambling sites (Read, 2010).

2.7.3.2.2 Security education, training and awareness

While there is an extensive literature (e.g. Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Pfleeger & Caputo, 2012; Puhakainen & Siponen, 2010) on critical success factors for effective user security education, training and awareness (SETA) interventions, and in particular on the basis of users' motivations to adhere to good security practices, such interventions are frequently reported as being ineffective in changing user behaviour (Bada & Sasse, 2014). There is little direct evidence, also, of the effectiveness of SETA in reducing unintentional user-related incidents. Proctor's (2016) literature review of reports of effectiveness of SETA interventions failed to identify any clear statistically-based studies. McElroy and Weakland's (2013) report for Educause discussed a survey concerning SETA of 95 higher education institutions in the USA, and subsequent case studies conducted within individual institutions. The main security issues were found to be phishing, compliance with national standards for information security and copyright, BYOD, and data loss. Tools or methods used to measure the effectiveness of SETA with the institutions covered included metrics on the numbers and types of security incidents, employee feedback, behavioural change, and user surveys. The case studies focused on phishing, compliance with standards, BYOD and data loss, as these were perceived by survey respondents to present the most serious problems: web-based attacks, cloud security, social networking or wireless network security, which are the issues most relevant for information behaviour, were not covered. University A claimed a 40.9% decrease in phishing incidents as a result of three rounds of awareness campaigns on phishing. University B

cited a 71% decrease in breaches of copyright following an awareness campaign for new students. University C achieved a 99% adoption rate of a secure email system on user-owned smartphones through a SETA campaign. University D reduced the number of outgoing messages containing confidential information by 80% by implementing a data loss prevention (DLP) solution which sent “educational” messages to staff members who attempted to send such messages.

2.7.3.3 Measures against inappropriate web use: detection

Monitoring of website access can be used with allowable legal limits to detect inappropriate web use (see below) as an alternative or addition to web filtering, e.g. activity logs can be analysed to identify access to questionable sites, and spot checking processes can be instituted requiring staff to account in precise detail for their business reason for accessing particular sites. While such an approach does not of itself restrict access to information, and is therefore from the information behaviour point of view a far preferable approach to enforcing AUPs, monitoring can raise serious issues of data protection, privacy, and organisational values (Clarke, 2005). Use of monitoring, while effective in reducing PWU, has been found to lower the overall job satisfaction of the employees being monitored (Urbaczewski & Jessup, 2002). It can also affect workers’ performance (Whitty, 2004), and may even trigger deliberate computer misuse (Posey, Bennett, & Roberts, 2011). “Employees may feel they are no longer trusted, become stressed, and begin wondering if they cannot be trusted with the net why should they be trusted with anything else” (Canaan Messarra, Karkoulian, & McCarthy, 2011, p. 255). This may be compared with the following from a publication by NHS Employers: “We trust our staff with patients’ lives, so why don’t we trust them with social media?” (NHS Employers, 2013a, p. 9).

All monitoring of Internet access within the workplace in the United Kingdom required to be carried out in accordance with the provisions of the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000, following the Information Commissioner’s Office guidance, which had the force of law (Holt, 2004; Information Commissioner’s Office, 2005). The Act, while not precluding systematic or intermittent monitoring of Internet access, required in particular that employees be notified of the detailed arrangements of monitoring and of the business rationale for it, and that any adverse impacts on individuals resulting from monitoring be justified with reference to the anticipated benefits to the employer and others. Issues that required to be considered here include possible impact upon the relationship of mutual trust and confidence that it is desirable should exist between staff and their employer, and whether the monitoring itself could be considered oppressive or demeaning. Glassman, Prosch, and Shao, (2015) found that use of “quota”

and “confirmation” functions within a web filtering system substantially reduced PWU and promoted compliance with the acceptable use policy.

2.7.3.4 Measures against inappropriate web use: prevention

2.7.3.4.1 *Web filtering: technologies*

Web filtering in various forms (prevention) can be used to block access to websites and web applications that are deemed inappropriate to access in a work environment (see Section 2.6 above). Overviews of the various tools and technologies used by governments, internet service providers and organisations to block websites are provided by Banday and Shah, (2010); Bertino, Ferrari, and Perego (2006); Gomez Hidalgo, Sanz, Garcia, and Rodriguez (2009); Houghton-Jan (2010); Lovaas (2015); Murdoch and Anderson (2008); and Nicoletti (2009), on whose accounts I have depended in what follows.

Some web filtering systems screen according to content rating via metadata systems such as the Protocol for Web Description Resources (POWDER, maintained by the World Wide Web Consortium; successor to the Platform for Internet Content Selection, PICS), and that of the former Internet Content Rating Association, ICRA (discontinued in 2010). These rely on good practice implemented by content providers, and involve a) a self-labelling system used to describe the content in terms of predefined categories (its sexually explicit nature, suitability for children etc.) b) a client-side filter that recognises content labels and matches them with the user’s access policy, delivering or blocking the content as indicated. Most popular browsers provide content filtering options using such schemes. However, the use by publishers of content labelling is purely voluntary; it is estimated that only a small percentage of web pages include these labels (Bertino et al., 2006).

Commonly, content is filtered otherwise based on a combination of domain, URL and file type, with selective screening for “prohibited” words or phrases. Blocking of URLs and their associated IP addresses is most commonly carried out using blacklisting (listing of objectionable sites to be blocked; more common) or whitelisting (listing of permissible sites); blacklisting is the primary mechanism used by commercial web filtering products, combined with supplementary whitelisting to ensure that certain important sites are never blocked. Blacklists may be maintained and supplied to web filtering product vendors by third-party services. They may not necessarily be maintained in-house; they are often purchased by web filtering system vendors as a third-party product. The requested web page’s URL and equivalent IP address is compared with a stored list of URLs. From the technical point of view this is a rapid and efficient approach; however, it requires that the lists be

constantly updated to be effective. This process can be partly automated using web spidering techniques and web analytics, focusing on websites that appear as the most popular. Content analysis and classification techniques are generally employed by web filtering systems to carry out this updating automatically and assign previously unknown sites to the pre-determined categories.

URL blocking and content analysis are the primary filtering technologies used in commercial and open-source web filters. The most primitive form of content analysis is keyword matching, which blocks access to websites on the basis of the occurrence of “objectionable” words and phrases regardless of semantic context, comparing words in a retrieved page against those in a keyword dictionary of prohibited expressions. Such an approach is sometimes used by web filters in the preliminary screening of sites, “suspect” pages then being referred to a more sophisticated content analysis process. The two most prominent “intelligent” content analysis approaches used by commercial web filters are text classification and image processing using skin detection, the latter being particularly relevant to the detection of pornography. Of the available techniques for text-based web content filtering, automated text classification using a machine learning approach is the most widely used. Details of these processes, or of the types of sites blocked and how they are categorised, are never made public by the system vendors, who are hence not accountable for their effects (Willard, 2010). Blocking by file type is possible with some filters, e.g. .jpg (still images), .avi (video), or .mp3 (sound). However, owing to the multiplicity of file extensions available for some file types, the ability to embed images in other file types, and the lack of metadata associated with images, blocking by file type cannot be applied selectively to “objectionable” content (Houghton-Jan, 2008). Some filters provide for quota restrictions to be applied to particular types of content, or for a “warning / confirm” message to be displayed on the screen when an attempt is made to access questioned content, either requiring a simple click-through or entry of a password (*cf.* Figure 2.11 above).

Web filters are generally evaluated either in terms of percentages of false positives (blocking of legitimate websites) and false negatives (sites which should have been blocked according to the configured policy, but were not), or of precision (P) (proportion of items classified as positive that were really positive) and recall (R) (proportion of items classified as positive from the whole set of positive items). (In clinical contexts, the terms “specificity” and “sensitivity” are used as the equivalent of “precision” and “recall”.) An “ideal” filter that is totally error-free does not exist; moreover there is a trade-off between percentage of true positives and percentage of false positives (Resnick, Hansen, & Richardson, 2004; Resnick, Richardson, & Hansen, 2002). The trade-off can be

represented graphically using a Receiver Operating Characteristic (ROC) curve. More details are given in Appendix L. Resnick *et al.* (2004) described two measures of over-blocking, one negative, one positive: the *blocked-sites overblocking rate*, i.e. the fraction of all blocked sites that are legitimate, and the *legitimate-sites overblocking rate*, i.e. the fraction of legitimate sites that are blocked.

Experimental evaluations of web filtering systems rarely translate into real-world conditions (Gomez Hidalgo *et al.*, 2009). Resnick *et al.* (2004) presented a framework for designing and interpreting such evaluations. They stressed the need to use large test sets, to create the test sets in an unfiltered environment, for the collection process to be objective and repeatable, and for a range of filter configurations to be tested. They had earlier carried out an influential test of the effectiveness of commercial web filters, which can be taken as representing best practice in evaluating filtering effectiveness (Richardson, Resnick, Hansen, Derry, & Rideout, 2002; Rideout, Richardson, & Resnick, 2002). They examined the effectiveness of commercial web filters in screening out pornography without hindering access to legitimate health information. They used a simulation approach, testing with results from searches approximating the results of adolescents' web searching for health information and pornography. At the least restrictive setting, configured to block only pornography, the products tested blocked a mean 1.4% of health information sites; however, 10% of health sites found using search terms related to sexuality were blocked. The mean pornography blocking rate was 87%. At the most restrictive settings, the mean blocking rate was 24% for health information sites and 91% for pornography sites. Houghton-Jan (2008) also evaluated the accuracy of four widely-used commercial filters (Barracuda, CyberPatrol, FilterGate and Websense). Library workstations were set up, one without filtering, the others with each of the filters to be tested. Their accuracy in filtering "content of an adult sexual nature", sexuality-related content "not of an adult sexual nature" (e.g. rape victim support sites, LGBT support sites) and also web proxy / avoidance sites, using the applicable categories on each filter, was tested using 135 test questions and scenarios. These included general keyword searches using three different web search engines, direct URL access to a variety of types of site and content, image searches, library catalogue searches, and bibliographic database searches. RSS feed content access was also tested. No attempts were made to find illegal material.

Type of Content Tested	Accuracy Percentage
Content of an Adult Sexual Nature – direct URL access	87%
Content of an Adult Sexual Nature – keyword searches	81%
Content not of an Adult Sexual Nature – direct URL access	86%
Content not of an Adult Sexual Nature – keyword searches	69%
Image Searches	44%
Email Attachments	25%
RSS Feeds	48%
Library Catalog Searches	75%
Library Database Searches	88%

Table 2.5 Web filtering accuracy

Houghton-Jan (2008), p. 7

Reproduced by permission

Houghton-Jan's findings are summarised in Table 2.5 above. She found that the filters were far more accurate for direct URL access, keyword searches using search engines and bibliographic database searches than they were for image searches or RSS feeds. Results for library catalogue searches were less accurate than for bibliographic databases. She described her results as being similar to the findings of earlier studies, which she summarised, in indicating high levels of over-blocking of legitimate content.

2.7.3.4.2 Web filtering technologies: impacts upon information seeking

As stated above, the purpose of implementing website blocking and filtering technologies is to enforce the organisation's acceptable use policy. NHS AUPs were not intended to constrain information seeking for work-related purposes. Anecdotal evidence, as collated by Blenkinsopp (Blenkinsopp, 2008a, 2008b) suggested that it was relatively common, however, for material even of a professional nature relating to subjects such as violence, sexual behaviour or drugs of abuse to be blocked entirely by NHS web filters which had detected particular terms out of context. This could have far-reaching consequences, such as the blocking of entire library catalogues and collections of purchased e-book or e-journal content; even government websites could become inaccessible. Web applications that were deemed to be in some way a security risk (e.g. peer-to-peer file sharing, webmail and Google tools, popular social networking platforms, web conferencing, instant messaging, and Skype), and resource sharing sites with a social component, such as SlideShare, Delicious and YouTube, were also frequently blocked. Interactive functionality within blogs could be disabled, and individual services, such as libraries, could be prohibited from running their own blogs. While processes for getting content unblocked generally existed, they were frequently reported to

be slow and bureaucratic (TDAG, 2009b); permission could, for instance, require to be given by a so-called Information Asset Administrator within the service where a person was working before IT staff were able to act. There were *prima facie* indications, therefore, that actual website blocking and filtering practices with NHS organisations did not correspond with the intentions of the NHS model AUP. Within the NHS, guidance from the HSCIC on content filtering had at the time of writing apparently been “in preparation” for several years. It should be noted that content filtering was not implemented centrally within N3, other than for gambling sites (Read, 2010).

Web filtering is “of its nature intrusive and disruptive” (Gomez Hidalgo et al., 2009, p. 270); it represents a denial of autonomy in information-seeking, and inevitably involves a form of censorship. It is controversial within organisational settings mainly on account of its questionable accuracy, particularly in respect of over-blocking, as described above. However, the underlying socio-cultural and moral values of web filtering vendors have also been questioned. Willard (2002) documented the existence of close links between conservative Christian lobby groups and eight of the vendors supplying web filtering systems to American high schools. Numerous instances of apparently values-based categorisation or blocking of websites by mainstream vendors were documented by Ayre (2004a) and Houghton-Jan (2010). Blenkinsopp (2008a, p. 10) reported that, within the NHS, “... sites on HIV/AIDS have been blocked as ‘having gay or lesbian content’”. It was clear that health information presented a particular problem as regards over-blocking, particularly within areas such as sexual health and behaviour, maternity services, child protection, dermatology, substance misuse, and forensic psychiatry, where access to professional information is frequently found to be blocked. (Lehmann, Cohen, and Kim (2005) described the problems of maintaining legitimate access to an online dermatology atlas while controlling pornography seeking.) Within mental health services there was a particular issue in respect of content accessed by patients (for example, sites promoting illicit substances, encouraging eating disorders or self-harm, providing information about methods of suicide, supporting violent political extremism etc.) which clinicians could need to investigate for purposes of diagnosis, case formulation and therapy.

The concerns of NHS librarians, as outlined by Blenkinsopp (2008a, 2008b), regarding the blocking of websites in particular led to the former Strategic Health Authority Library Leads’ (SHALL) Technical Design and Authority Group (TDAG) undertaking a survey of NHS librarians (n=151) in December 2008 (TDAG, 2009a, 2009b). A summary of the survey findings was circulated to NHS librarians via the customary channels; otherwise this important work was not published. The survey found that access to a variety of e-resources was blocked within NHS Trust networks, including e-books and e-

journals purchased locally or nationally, as shown in Figure 2.10 below. It identified (as well as the blocking of websites) the following: lack of required software on PCs to access audio-visual media; lack of administration rights by library staff to install it; blocking of browser functionality required to run applications; restrictions on size of email attachments; storage problems, including limited access to encrypted memory sticks, coupled with restrictions on USB connections and the disabling of CD/DVD writers and floppy disc drives; and slow networks. Follow-up measures subsequently agreed by TDAG in consequence of the findings are described in Section 1.4.5.

The consultant paediatricians Prince, Cass, and Klaber (2010) undertook a survey within 37 NHS Trusts in England of accessibility of web-based resources to postgraduate medical trainees, the results of which were published in a relatively brief article within a peer-reviewed journal. It was not stated how these Trusts were selected, nor to which clinical specialties the respondents belonged. In each Trust, a doctor working on a computer within a clinical area tested access to a sample of 22 different online resources. The websites were selected to cover common online file format types, including text and audio files, images, video and dynamically driven e-learning sites.

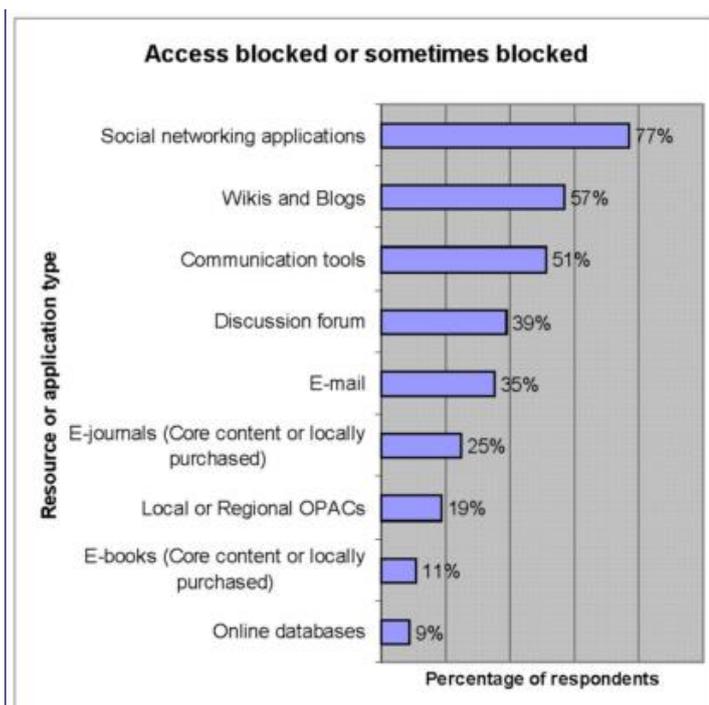


Figure 2.12 Blocking of access to e-resources in NHS libraries

TDAG, 2008, Reproduced by permission

It was found that, while established resources such as the National Library for Health were accessible in over 95% of Trusts, important clinical resources were blocked, and it was sometimes difficult to download PDF or PowerPoint files. Their findings are summarised in Figure 2.12 above.

Online video and audio (podcast) content was often difficult to view, and sound was usually absent. YouTube was blocked in most Trusts, and iTunes University was not accessible, as it required iTunes to be installed. The DH's "E-learning for Healthcare" programme modules were fully functional for only 32% of respondents. YouTube and webmail applications were sometimes blocked. The authors drew some far-reaching conclusions: that IT managers' approach to risk management in relation to web content was flawed: "Shouldn't we be managing the risks more effectively in order to allow learners the freedom to use IT resources to better effect?" (p. 437), and that the technical logistical obstacles they had identified presented a potential obstacle to the future development of medical e-learning which required to be addressed at a national policy level.

Childs *et al.* (2005) conducted a qualitative multi-method study aiming to identify barriers to and solutions/critical success factors for e-learning in health sciences. It included a systematic review, semi-structured telephone interviews and a questionnaire survey. A total of 57 articles and reports relating to conditions in the United Kingdom, the United States and elsewhere were identified as suitable for review, based on their subject content. Thirteen telephone interviews were conducted with managers and training staff. The survey aimed to elicit the views of users and non-users of e-learning; 149 questionnaires were returned. Details of the samples, and of the percentage response rate for the survey, were not stated. As well as organisational problems, the study identified a variety of technical barriers to e-learning, which included network bandwidth problems, and deficiencies in hardware, peripherals, software and technical support for e-learning. The authors also found evidence of computer skills deficits and a variety of pedagogical issues acting as barriers to effective e-learning.

The more recent overview by Lafferty (2015), provided a detailed account of technological barriers of various kinds to technology-enhanced learning (TEL).⁴⁷ This was a technical report prepared for Health Education England, and was based primarily on her own experiences with delivering e-learning within NHS settings, with contributions from other e-learning practitioners; other work was not referenced. Issues she highlighted included lack of support for users' mobile devices, lack of access to adequate Wi-Fi connectivity including non-availability of eduroam on many NHS sites, blocking of e-learning support resources, including social media, by Trust web filters, lack of appropriate hardware and software (sound cards, video cards, or appropriate browsers or media

⁴⁷ The researcher is identified as one of four contributors of content to the final version (2.1) of this document. An updated version (2.8) was recently published by Health Education England (Lafferty, 2017).

players) and inability to transfer large files owing to restrictions on portable media and access to external network resources. Many aspects of her account were borne out by the comments of participants in a Tweet chat conducted by #WeNurses (2015) on the theme “Are barriers to the use of technology in learning a real issue for healthcare professionals?”

Studies have been carried out of the negative impacts on information seeking of web content filtering in other contexts: Australian (Broucek, Turner, & Zimmerli, 2010) and South African (Rensleigh, 2002) universities, in American schools (Simmons, 2005; Sutton, 2005a, 2005b, 2006) and colleges (Stanley & Stovall, 2008), also in American (reviewed by Cooke, 2006, and Shearer, 2010) and British (Brown & McMenemy, 2013; Cooke, 2006; McMenemy, 2008; Payne et al., 2016; Shearer, 2010; Spacey & Cooke, 2014; Spacey, Cooke, Creaser, & Muir, 2013; Spacey, Cooke, Muir, & Creaser, 2013) public libraries, and on consumer health information seeking in particular (Richardson et al., 2002; Rideout et al., 2002). In particular the effects of web filtering on secondary education in the United States have been extensively investigated, although most of this work exists in the form of dissertations and theses. Sutton (2005), for example, found that web filters frequently blocked legitimate web content that the students needed for their assignments, giving rise to considerable wasted time, frustration, annoyance and alienation on their part. She concluded that information literacy training in use of the Internet was a far more effective way than using web filtering of keeping students safe from potentially harmful content; *cf.* Ofsted (2010; Willard (2010). Web filtering in public libraries raises issues of democratic accountability and transparency, particularly in instances where web filtering policy is outside the control of library staff. Studies of the impact of web filtering or monitoring within organisations (e.g. Whitty, 2004) have tended to focus on employee attitudes in general rather than on information seeking specifically. The only work found specifically relating to information behaviour was that of Deisz (2005), who undertook a questionnaire survey for his MSc thesis of workers in 24 Norwegian companies, both filtered and un-filtered, found that more than 33% of respondents (n=48) felt that filtering in their company blocked too many sites and hindered their work.

2.7.4 Summary and synthesis

Sections 2.6 and 2.7 have provided an overview of relevant issues relating to information security / cybersecurity risk management, including social theories of risk, cognitive biases in decision-making under conditions of uncertainty, and the relationship between security management approaches and adverse events. It has also discussed in detail the measures adopted by organisations

(acceptable use policies, training, monitoring and filtering) to address risks related to use of the web, their effectiveness or otherwise, and their impacts on individual workers' information behaviour.

Web-borne malware presents a well-attested and growing threat to corporate networks. However, it is apparent that the relationship between malware infection risk and web users' browsing behaviour is not well understood; in particular, the correlation between subject content and frequency of compromise has been found to be relatively weak (2.6). While there may be valid legal and governance reasons for subject-based filtering of web content, the practice of restricting access on security grounds based on website subject categories, therefore, cannot therefore be said to be strongly supported by the available research evidence.

All organisations and societies emphasise certain risks and ignore or downplay others (Douglas & Wildavsky, 1982b). Sociological theories of risk and risk perception (2.7.1) would seem to indicate that risk management in general is subject to a range of organisational and cultural influences. End-users' decision making in relation to online risks has been shown to be subject to a variety of cognitive biases, as well as to the security fatigue phenomenon. The relationships between end-users' perceptions of online risks and actual security behaviour have been demonstrated to be complex, with very little evidence for any direct effect of training interventions on levels of security incidents. Two contrasting approaches to information security management were identified and described, the functionalist and the sociotechnical (2.7.2.4.1). Risk management in information security / cybersecurity has been shown to be a matter of professional judgement rather than a precise science. Decision-making by security professionals has been shown to be largely tacit in nature (2.7.2.4.1). Studies were identified specifically of decision making in information security management within the private sector and in academia, but not within health services (2.7.2). Kolkowska (2006, 2011) characterised what she described as different information security cultures within an academic context, and described their impacts upon end-user computing activity (2.7.2.4.1). A relationship was identified between information security management approaches and adverse events (2.7.2 .4.1).

The organisational rationale for web filtering derives from the productivity, security and legal risks that some forms of PWU at work can present. However the nature of the phenomenon and its effects are contested (2.7.3). PWU itself, and the effectiveness and organisational appropriateness of measures to prevent or minimise it (via deterrence, detection, and prevention) has been extensively studied, although not in health service contexts. The technical deficiencies of web content filtering solutions, and their adverse impacts on information seeking, were discussed. The evaluation

methodologies of Resnick and associates and of Houghton-Jan (2008) were outlined. A range of studies were identified that discussed the negative impacts of web filtering in non-health settings, mainly education services or public libraries. The only studies found which related specifically to health-related information seeking were those of Resnick and associates (2.7.3.4.2). These studies demonstrated negative impacts arising from the lack of accuracy of filtering technologies and lack of accountability in their implementation. The only two studies found relating to web filtering and other security-related technical barriers to information seeking in general within the NHS were the unpublished TDAG survey (2009) and that of Prince *et al.* (2010). Technical obstacles to information seeking, i.e. related to deficiencies in computer systems, were mentioned in some studies, and occasionally blocking of websites (Beke-Harrigan *et al.*, 2008; Gilmour *et al.*, 2011; Hughes *et al.*, 2009; Jones *et al.*, 2011), but generally in insufficient detail to be informative. Childs *et al.* (2005) identified a variety of barriers within NHS settings to e-learning, which included deficiencies in hardware, software and technical support for e-learning. Chamberlain *et al.* (2015) identified technical barriers (inadequate infrastructure, blocked websites and web applications, lack of BYOD implementation), to the use of mobile technologies by health professionals in NHS settings. Lafferty (2015) documented in detail a range of technical and related policy obstacles to e-learning encountered within NHS environments, relating particularly to social media policy, and briefly indicated their impacts, but did not discuss organisational issues in any depth.

2.8 Diffusion of innovations

2.8.1 Rogers' theory of diffusion of innovations

Theories of the diffusion of innovations are relevant to the literature review as a whole in that they address the responses of individuals, organisations and societies to new technologies. They are treated here mainly with reference to Web 2.0 and social media. Innovation is discontinuous and transformational in character (Brown & Osborne, 2013). It may be defined as “new ideas that work”, or, more precisely, “the intentional introduction and application within a role, group or organization, of ideas, processes, products or procedures, new to the relevant unit of adoption, designed to significantly benefit the individual, the group or organization or wider society” (West & Farr, 1990, cited by Brown & Osborne, 2013, p. 188).

Within the theory of diffusion of innovation popularised by Rogers (1967/2003), diffusion is defined both as “the process by which an innovation is communicated through certain channels over time among the members of a social system”, and the process by which an innovation is adopted and gains acceptance among members of that system (Koçak, Kaya, & Erol, 2013, citing Rogers, 1983).

The theory is applicable both to individuals and to organisations. Rogers suggested that in most cases an initial few people (*innovators*) are open to the innovation and adopt it. *Early adopters* also invest early on in new technologies as a means to address their specific problems. As these innovators and early adopters (who may be influential opinion formers) spread the word within their communities, the innovation is adopted by more and more people, leading to the formation of a *critical mass*. Once this critical mass is achieved, diffusion of the innovation becomes self-sustaining. Over time the innovation becomes diffused among the population until a saturation point is achieved. The process can be represented by an S-shaped curve.

With interactive innovations such as Web 2.0 / social media, the innovation becomes involved in its own diffusion, and later adopters influence earlier adopters as well as *vice versa*; this process is termed *reciprocal interdependence* (Markus, 1987). It is shown in Figure 2.13 below:

Regarding organisational use of Web 2.0 and social media, a distinction needs to be made between internal and external use; it is perfectly possible for an organisation to use social media applications for public and supplier engagement, while blocking or strictly limiting their use by individual staff members within the network perimeter (Saldanha & Krishnan, 2012).

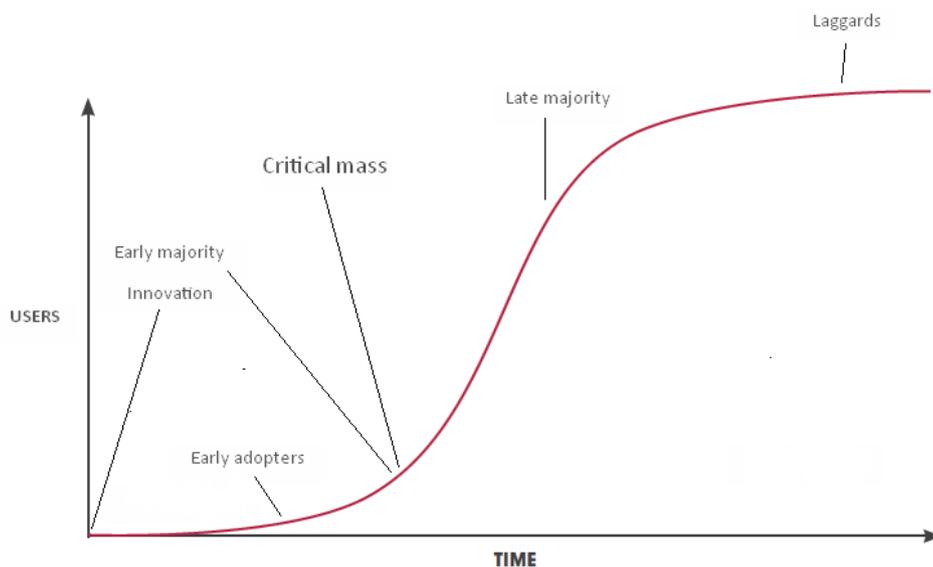


Figure 2.13 Diffusion curve for an interactive innovation

After Rogers (1966/2003) *Diffusion of innovations*, 5th ed., p. 344 (amended)

One aspect of the theory concerns the manner in which characteristics of innovations influence the rate of their adoption. Five key characteristics are proposed:

- 1) Relative advantage: to what degree is an innovation perceived as an improvement on what it replaces? (Rogers, 2003, p. 229)

- 2) Compatibility: to what degree is an innovation perceived as consistent with the existing values, past experiences and current needs of prospective adopters (Rogers, 2003, p. 240)?
- 3) Complexity: to what degree is an innovation perceived as being difficult to understand and use (Rogers, 2003, p. 257)? Perceived complexity correlates negatively with the likelihood of adoption.
- 4) Trialability: to what extent can an innovation be experimented with on a time-limited or trial basis (Rogers, 2003, p. 258)?
- 5) Observability: to what extent are the results of an innovation observable by others (Rogers, 2003, p. 258)? Observability correlates positively with the likelihood of adoption.

Another aspect describes the process of decision making regarding innovations. Five basic stages can be identified: *knowledge*, *persuasion*, *decision*, *implementation* and *confirmation* (see Figure 2.14, below). The process may be further described in terms of phases of *agenda setting*, *matching*, *restructuring*, *clarifying* and *routinising*, as shown in Figure 2.15, below. This sequential process can be observed both in individual and in group or corporate decision-making (Rogers, 2003, p. 170ff.); however, many studies of social media adoption and use within organisations have focused on the individual user rather than on groups (van Osch & Coursaris, 2013, 2015).

Organisational readiness for innovation may be defined as “the availability of the needed organisational resources for adoption” (Iacovou, Benbasat & Dexter, 1995, cited by Geenhuisen & Faber, 2015, p. 4). The structural characteristics of organisations identified by Rogers (2003) as related to innovativeness within organisations, or organisational readiness for innovation, include 1) characteristics of individual leaders 2) internal characteristics of the organisation, and 3) external characteristics. The internal characteristics include *degree of centralisation* (the extent to which power and control are held by relatively few individuals); *complexity* (members’ level of training and range of professional and occupational specialities); 4) *degree of formalisation* (relative importance of procedures and rules); 5) *level of interconnectedness* (degree to which units within the organisation are linked by interpersonal networks); 6) *degree of organisational slack* (availability of uncommitted resources) and 7) *size*, although he suggests that size is probably a proxy measure for other characteristics, such as total resources, slack resources, employees’ technical expertise, and organisational structure.

These variables may have different effects at different stages of the innovation process, e.g. low formalisation or high complexity serve to facilitate initiation of the adoption process, but inhibit implementation. A more general concept relating to organisational readiness for innovation is

absorptive capacity, defined as “dynamic capability pertaining to knowledge creation and utilisation that enhances an organisation’s ability to gain and sustain a competitive advantage” (Zahra and George, 2002, cited by Geenhuizen & Faber, 2015, p. 6).

Prior contextual conditions which influence the decision-making processes of individuals and groups may also be categorised under the headings of *Technology-Organisation-Environment (TOE)* (Oliveira & Martins, 2011). *Technology* includes IT governance, existing IT infrastructure and IT support, IT security, and satisfaction with existing systems (Geenhuizen & Faber, 2015). *Organisation* includes communication processes, size, social norms, professional heterogeneity (Ferlie, Fitzgerald, Wood, & Hawkins, 2005) and levels of technology literacy and readiness. Processes of diffusion may be “messy, dynamic and fluid” rather than linear (Ferlie et al., 2005, p. 118, citing Van de Ven et al., 1999).

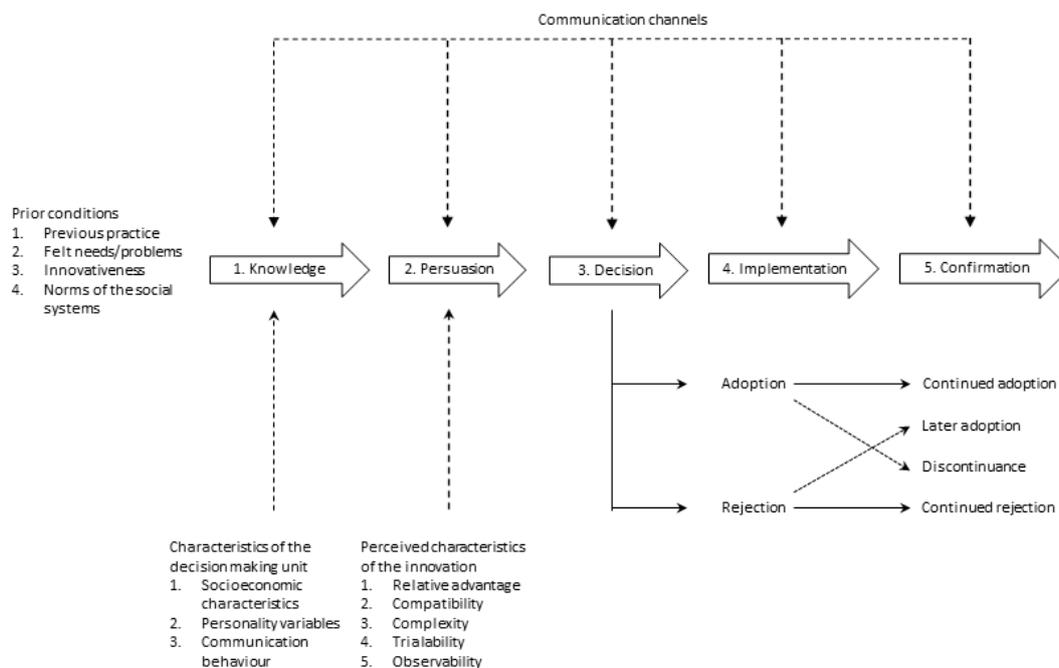


Figure 2.14 Decision-making processes in innovation

Redrawn from Rogers (2003), p.170

Internal organisational politics may be a factor, in that groups and individuals are more inclined to adopt an IT innovation if they perceive that the innovation will support their position of power within the organisation; conversely, if they perceive a potential threat presented by the innovation to their power base or professional autonomy, they will resist (Markus, 1983).

Environment includes external regulation and legal issues, competitive pressures, and political pressures. In relation to the organisational component of this framework, the theory of IT-culture conflict is applicable (2.8.3). Characteristics of the decision-making unit itself, namely socioeconomic position, personality variables and habits of communication, bear upon the “knowledge” phase. Characteristics of the innovation itself, as enumerated above, influence the “persuasion” phase. Some writers refer to “culture of innovation” as a factor influencing uptake of innovations. Apekey, McSorley, Tilling, & Siriwardena, (2011) identify five dimensions of culture of innovation: risk, resources, information, targets, tools, rewards, and relationships. The issue of risk is discussed further below (Section 2.8.2).

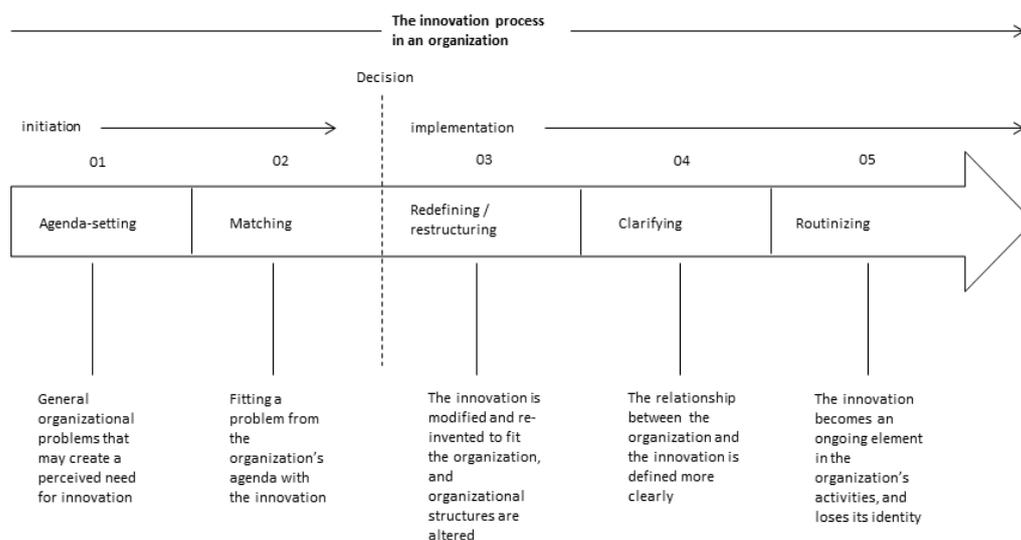


Figure 2.15 The innovation process in an organisation

Re-drawn from Rogers (2003), p. 421

In relation to information and communications technology innovations within health services, attitudes of health professionals to information technologies (an aspect of “organisation” within the TOE framework) have a particular bearing on organisational readiness. According to Svensson, Snis, Svanberg, and Svensson (2009), attitudes of practitioners are a significant factor in the level of acceptance and consequent efficiency of the use of IT in practice. The main evidence published in English for attitudes of health professionals to information technology in general was set out in a comprehensive literature review conducted by Ward, Stevens, Brentnall, and Briddon (2008). The authors found that the issues predominantly affecting health professionals’ use of information technology in their everyday practice were hardware availability, design of content and provision of user training programmes. The majority of workers felt that there were pervasive issues relating to usability and fitness for purpose. Needs were expressed for more education and training prior to the implementation of new IT systems, and more use of e-learning in continuing professional education.

Experienced IT users were found to have more positive attitudes towards the introduction and use of IT in their work settings; this was the only consistent indicator found of likely attitudes to IT. In some contexts gender differences in access to computer systems were identified.

2.8.2. Innovation and risk

Innovation and risk-taking are inextricably linked: innovation is “uncertain both in process and outcome” (Hartley, 2013, p.53). Flemig, Osborne, and Kinder (2016) distinguish between *risks* (that can in principle be evaluated and planned for) and *uncertainties* (considered to be unquantifiable, and which cannot be planned for). They also distinguish between “hard” (top-down) and “soft” (people-driven) risk management approaches: “hard” approaches are well suited to managing evolutionary innovation, but stifle innovation when applied to uncertainty.

A key concept here is that of organisational *attitude to risk* (also referred to as *appetite for risk* or *risk culture*): it may be defined as “the organisation’s propensity to take risks as perceived by the organisation’s managers” (Bozeman and Kingsley, 1998, p. 111) (compare the discussion in 11.1 below). Attitude to risk is considered to be a component part of an organisation’s overall culture of innovation (Mulgan & Albury, 2003); compare the discussion in 2.8.1 above. It may vary across different parts of an organisation (Power, 2004), and is subject to change. Welbourn (2013, p. 1) recommended that, to establish the right conditions for the adoption and diffusion of innovations, “leaders should establish an appetite for risk that is nurtured by a culture of trust and openness capable of treating failure of new ideas as the occasional price for learning” The need for a “risk-taking climate” is mentioned also by Greenhalgh, Stramer *et al.* (2008) as a necessary antecedent of innovation, this being one in which “one in which experimentation is encouraged; failed projects lead to reflection and efforts to improve features of the system” (p. 5); compare Powell’s (2016) observations concerning organisational trust cited in Section 2.5.5.3 above.

Flemig *et al.* (2016) suggested that risk aversion may not be an inherent characteristic of public sector organisations, but a result of exogenous factors, such as organisational size or media scrutiny: normal organisational processes of innovation, which involve learning and evolving from mistakes or failed innovations, cannot occur, because risk and failure are both perceived as normatively “bad”, and structural incentives, in particular, statutory regulation, are set to minimise or avoid blame, both corporate and individual (*cf.* the discussion in 2.5.5.2 above).

2.8.3 IT consumerisation

From the perspective of diffusion of innovations, use of personal cloud storage, Web 2.0 and social media applications can be classified with other aspects of IT consumerisation (which is described by Leclercq-Vandelannoitte (2015, p. 2) as “the adoption and adaptation of consumer applications, tools and devices in the workplace as a means to carry out work tasks”) under the category of *user-driven technologies*. As a means of enhancing productivity, it seems appropriate, from the users’ point of view, to wish to use in a work context the technologies with which they have become comfortable in their personal lives, rather than to draw a line between the personal and the corporate (Baxter & Rudman, 2010). From an IT services management perspective, however user-driven or user-led technologies are often categorised negatively as *shadow IT*, defined as “the use of unauthorised applications within a corporate environment, and the processing or storage of business information on unapproved devices” (Johnson, 2013, p. 5). Such a characterisation reflects the perceived risks presented by the holding of organisational data (*shadow data*) within such applications or devices. The existence of shadow IT can be taken as indicating problems of communication, deficiencies within formal structures or other misalignment between business and IT functions, as presenting risks to the operational performance or security of IT systems, or as creating problems for IT governance (Betts, 2016; Györy, Uebernickel, Cleven, & Brenner, 2013; Johnson, 2013; Kettinger & Lee, 2002; Rentrop & Zimmermann, 2012; Sullivan, 2015). It is evident that its existence and use represents a loss of centralised decision-making power and control for the IT department (*cf.* Andriole, 2015). It has, however, been shown to provide considerable benefits to the organisation in terms of innovation (Silic, 2015). The issue of shadow IT is not addressed within best practice frameworks such as ITIL and COBIT. Strategies adopted to address IT consumerisation (Harris, Ives, & Junglas, 2011) include *authority* (banning or tightly limiting the use of consumer devices and applications: common in highly-regulated sectors such as financial and health services), *anarchy* (allowing new devices and applications to enter the workplace without restriction: common in start-ups, venture partnerships and universities) and a number of different approaches to carefully managed *adoption*, of which Bring Your Own Device (BYOD) implementation is one (French, Guo, & Shim, 2014; Leclercq-Vandelannoitte, 2015; Tokuyoshi, 2013). Measures adopted to regulate or restrict shadow IT can include the blocking of unauthorised web applications on corporate networks. Schalow *et al.* (2013) highlight the blurring of boundaries between work and private life that mobile devices and applications have facilitated, which is important from an information security perspective.

Despite the sometimes high overheads for IT departments (Wood, 2015), a number of NHS organisations have begun to allow BYOD (Amedume, 2012; Azzurri Communications, s.d.; Phillips, 2013; Thorne, 2012). It has been reported that many NHS doctors and nurses are unofficially using their own smartphones for work purposes (Stephenson, 2015). The relation of BYOD to social media adoption was discussed briefly by Lafferty (2013, 2015).

2.8.4 IT and organisational culture: IT-culture conflict

The theory of IT-culture conflict presents another perspective on information technology innovations and organisational factors that serve to facilitate or inhibit them. According to Scholz (1990, cited by Thompson & Kaarst-Brown, 2005) the values of system developers and champions are embedded in both the explicit and the tacit design features of new systems, including security systems and network controls. Information systems are not culturally neutral; they may come to symbolise a host of different values driven by underlying assumptions and their meaning, use and consequences (Koch, Leidner, & Gonzalez, 2013; Robey & Markus, 1984). The theory of IT-culture conflict (Leidner & Kayworth, 2006) posits that the values embedded within a work practice that is supported by a particular information technology (such as, for instance, smartphones enabling any time / anywhere work) can be said to be *embedded* within that technology. System conflict, which is one type of IT-culture conflict, is said to occur when the values of group members are unsupported by, or are contrary to, the values embedded within a specific information technology which is being implemented within the group members' workplace.

Koch *et al.* (2013) set out, in tabular form, how workplace values may contradict the values inherent in social media applications (Table 2.6 below). Disagreements about social media policy and restrictions on access to social media applications within the workplace may thus reflect an IT-culture conflict. The authors suggested that the perceived inherent conflict with organisational or professional values may serve to inhibit staff from exploring how and when different forms of social media / Web 2.0 functionality (e.g., discussion forums, blogs and wikis) may be used within the workplace. The theory is applicable in principle also to SWGs and their implementation within specific organisational contexts (Section 2.6.4 below).

Category	Group values: workplace	Values embedded in IT: SMS
Information	communication (e.g., broadcast and formal), hierarchical decision-making, hierarchical information flow, and security	collaboration, communication (e.g., informal and open), crowd sourcing, information sharing, and transparency
Employee relationships	chain of command (i.e., authority, power), hierarchical structure and work–social life separation	community, democratization, socialization and work–social life integration
Work	bureaucracy (e.g., plans, policies and procedures), control, risk management, work and productivity (i.e., value and financial gain metrics)	ceding of control, change, experimentation, fun and risk taking

Table 2.6 The theory of IT-culture conflict as related to social media applications

Koch et al. (2013), p. 206

Reproduced by permission

2.8.5 Diffusion of information technology innovations within the NHS

The overall relatively low level of expenditure on IT within health services in the United Kingdom compared to other sectors of the economy is shown in Figure 2.16. There is a considerable body of work which attempt to address issues of adoption and implementation of information technology within the NHS; however much of this is either very broad in scope (Greenhalgh, Robert, Bate, Macfarlane, & Kyriakidou, 2008; Liddell, Adshead, & Burgess, 2008; Welbourn, 2013) or is focused specifically on electronic patient record systems (Dickinson & Scott, 2012; Fernando, Choudrie, Lycett, & de Cesare, 2012; Greenhalgh & Stones, 2010; Greenhalgh, Stramer, et al., 2008; Wainwright & Waring, 2007; Walley & Davies, 2002), so there is little of direct relevance to social media adoption. Liddell, Adshead and Burgess (2008) list, among the critical factors hindering technological and other innovation, the following: lack of strategic leadership, narrow decision-making processes; lack of availability of resources to deal with changes; complexity of procurement processes; lack of incentives for clinicians to adopt technologies that are not directly clinical; and lack of awareness of the benefits of technologies among decision makers.

A number of other factors are cited by researchers as presenting barriers to innovation within the NHS and as possible contributory factors to low levels of commitment to and expenditure on IT infrastructure and innovation at Trust level. These include poor levels of computer literacy (Robertson et al., 2010; Sheikh et al., 2011; Warm, Thomas, Heard, Jones, & Hawkins-Brown, 2008); aversion to computer use and deficiencies in health informatics knowledge among clinical staff (Kirshbaum, 2004; Devitt & Murphy, 2004; Ward, Stevens, Brentnall, & Briddon, 2008); deficiencies of existing infrastructure (Sheikh et al., 2011), and low levels of usage of everyday technologies such as email and online booking systems (Liddell et al., 2008). The hitherto problematic and politically contentious nature of information technology implementations within the NHS, as well as

perceptions of inadequate infrastructure, have engendered a perception exemplified by one nurse commentator, “The NHS is terrible at practitioner sensitive, patient-centred, joined-up technology” (Rickards, commenting on Merrifield, 2015), and a consequent unwillingness on the part of many clinicians to engage with innovative information technologies (Kirshbaum, 2004; Royal College of Nursing, 2006).

Attitude is a necessary constituent of technology acceptance (Ward, 2013), which in turn is an essential aspect of information technology innovation; however, studies focusing specifically on the professional attitudes, values and norms health service staff in the UK relating to use of IT, including in relation to technology acceptance, are relatively few in number. They have focused on particular types of applications, such as EPR (Kirshbaum, 2004; Poulter & Bath, 2012), other systems and platforms such as simulation, social media / Web 2.0, and mobile devices (Brailsford et al., 2013; Moore & Jayewardene, 2014), on the attitudes of a particular profession or group (e.g. Bond, 2009; Hall, Hanna, & Huey, 2013; Scragg et al., 2017) or on specific contexts (e.g. Ayatollahi et al., 2013).

As reported below in Section 4.8.5, T1’s IT department had self-rated using the Informatics Capability Maturity Model (ICMM) (Health and Social Care Information Centre, s.d.) and National Infrastructure Maturity Model (NIMM). Use of ITIL within NHS IT departments as best practice guidance for IT service management was referred to in Section 1.4.4, while the Digital Maturity Assessment (DMA) was referred to in Section 1.4.3. Results of the latter were published only after data collection was complete (NHS England, 2016). While there has been some critical discussion of published health informatics digital maturity assessment instruments in general (Carvalho, Rocha, & Abreu, 2017, 2016; Carvalho, Rocha, & Vasconcelos, 2016), the actual results of ICMM and NIMM assessments were generally not made available for comment. Results of the DMA were discussed briefly in the Wachter review (2016) and in the computing trade press (e.g., Clark, 2016; Evenstad, 2016). Tools such as IT ServQual (Pitt, Watson, & Kavan, 1995) and the ten-point IT service climate evaluation instrument of Jia and Reich (2011, 2013) have not been applied to health services IT to the researcher’s knowledge.

While much theoretical work has been carried out in the area of information technology innovation in health services to elaborate Rogers’ diffusion of innovations theory (Cranfield et al., 2015), relatively little theoretical literature exists on adoption of Web 2.0 and social media. That which does exist is mostly concerned with social-psychological aspects of individual adoption; there is little socio-technical material (Osch & Coursaris, 2015).

There are some studies extant of factors underlying adoption of Web 2.0 and social media technologies at the individual employee level in settings other than health services (e.g. Saldanha & Krishnan, 2012, p. 322). Jacobs and Nakata (2012) used organisational semiotics methods to assess readiness within organisations for internal uses of social media. The work of Kaganer and Vaast (Kaganer & Vaast, 2010; Vaast & Kaganer, 2013) presents another instance of the application of a socio-technical perspective within studies of organisational social media adoption and use.

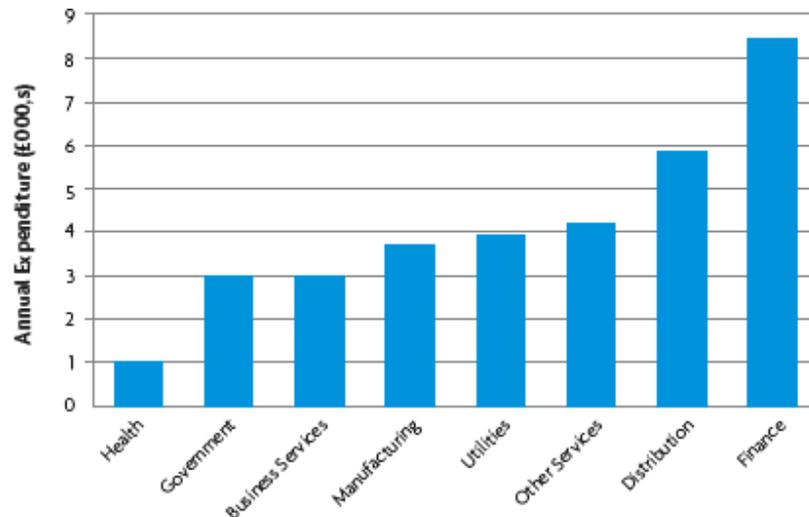


Figure 2.16 Annual expenditure per employee on ICT in the UK in different economic sectors, 2000. *Quam and Smith (2005), p. 532, reproduced by permission*

These authors applied social representations theory to the analysis of social media use and policy formulation in organisations, within a theory of diffusion of innovations framework. As a means of eliciting social representations of social media within corporate governance mechanisms, they undertook a thematic analysis of the social media policies of 25 organisations. The focus of their research was on emerging social representations of social media use in the enterprise held by organisational decision makers. They found that the policies applied governance practices to the use of social media which were rooted in other organisational domains, notably communications and human resources; they evinced a limited comprehension of the possible organisational uses of social media applications, and a strong focus on mitigation of the possible risks and threats they might present. In social representations theory terms, these policy responses were rooted in processes of “anchoring” and showed little movement towards “objectification” (*cf.* above, Section 2.7.1). In the traditional pattern of technological innovations, decision makers first develop a *shared understanding* of the new technology; this builds upon and sustains an *organising vision* for the local innovation, resulting in a *local social representation*. Decision makers then decide: whether or not to implement the technology; if yes, how to facilitate end-users’ adoption and learning processes. They maintain that the adoption of Web 2.0 technologies, which is primarily end-user-driven, conflicts

with established business application infrastructures and traditional IT decision-making processes, and also requires revision of views on the diffusion and assimilation of new technologies (*cf.* 2.8.1 above). The comprehension or shared understanding element has thereby shifted into the time frame of implementation and assimilation. With an end-user-driven technology, decision makers must 1) develop an understanding of the innovation, and 2) decide how to respond to it on behalf of the organisation as a whole. They therefore have to 3) develop ways to guide and direct end-users, which involves deciding a) what end-users may and may not do with the technology, and b) whether (and, if so, how) the technology is to be officially adopted and used within the organisation. Their comprehension helps them react to it and to communicate about it. Their conception 1) is made explicit as the basis of policy. Decision makers are thus faced with a pressing need to devise policies just as they are starting to make sense of the innovation themselves. This perspective offers a ready explanation of the type of policy response to social media observed at T1: a complete block on use of social media until a Trust policy had been developed (9.2.3).

Chretien and Kind (2014) offer a possible explanation for this form of shift of perception and attitude within medicine and health care in terms of an analogy with Maslow's hierarchy of needs. According to Maslow's theory, basic levels of needs have to be met before higher, aspirational levels can be attained. The three levels in the social media in medicine hierarchy of needs posited by the authors are *security*, *reflection*, and *discovery*. In this model (Figure 2.17, below) the essential need for security must be respected in order to move towards the reflection and discovery phases.

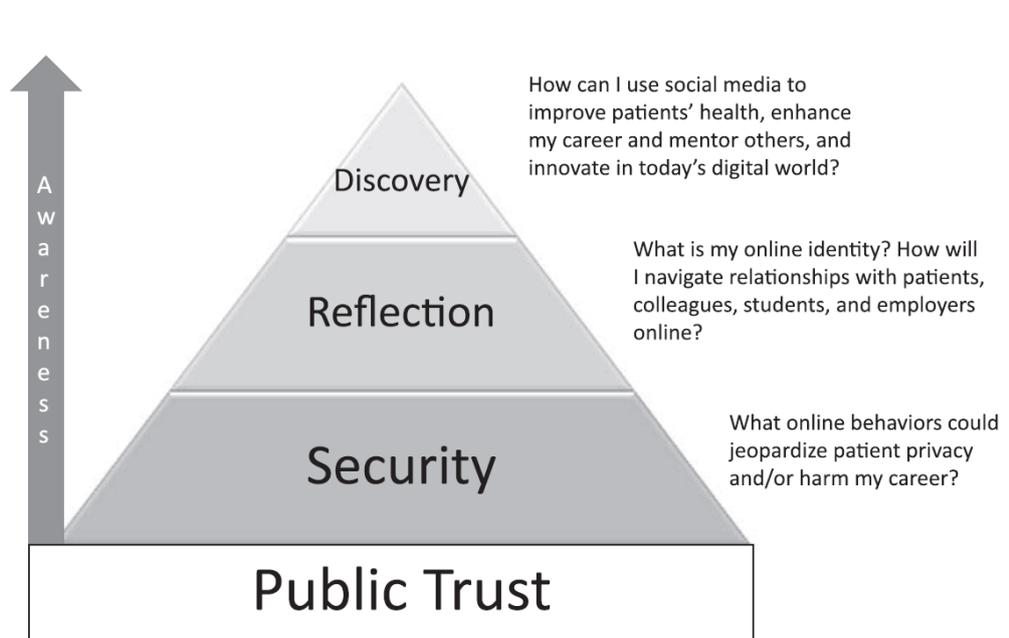


Figure 2.17 Social media in medicine hierarchy of needs pyramid

Chretien and Kind (2014), p. 1139

Reproduced by permission

2.8.6 Summary and synthesis

This section has provided an account of three key theoretical frameworks relating to innovation: Rogers' theory of diffusion of innovations, the Technology-Organisation-Environment framework, and the theory of IT-culture conflict. It has also discussed IT consumerisation in terms of user-driven innovation, and offered a critical overview of studies on information technology innovation within the NHS and hindrances to it. Kaganer and Vaast's social representations model of social media adoption and use within organisations, and Chretien and Kind's model of attitudes to social media adoption within health services based on Maslow's hierarchy of needs, were proposed as being of possible relevance to social media adoption and use within the NHS.

Theoretical frameworks for studying diffusion of innovations and organisational readiness for innovations, in particular Rogers' theory (2.8.1) and Vaast and Kaganer's work on decision processes in organisations' social media adoption (2.8.4), can be applied to processes of social media adoption and IT consumerisation occurring within the NHS. The theory of IT-culture conflict presents another useful perspective, both on social media adoption and on secure web gateway (SWG) implementations (2.8.4). Few studies appeared to have been carried out of NHS staff attitudes to information technology, and none of NHS IT service quality (2.8.5). Many of the studies identified of information technology innovation in the NHS were either very broad in scope, or focused specifically on electronic patient records, with little of relevance to social media adoption; however, a number were found that identified organisational and other factors hindering NHS innovation in general and NHS IT innovation in particular (2.8.5).

2.9 Overall summary

In Section 2.5.3, there were clear indications of the importance of IT staff subcultures in the development of reciprocal stereotyping and mutual antagonism between IT staff and end-users, the role of which in determining access to published information appeared to be worth investigating. The syntheses of research on the technical aspects of information security / cybersecurity and on cybersecurity and risk perception in Sections 2.6 and 2.7 presented interesting problems and findings in a number of areas which illustrated the overall complexity of the issues facing NHS organisations in managing information security / cybersecurity risk in relation to use of the Internet. Specific areas included the phenomenon of personal web use at work (PWU) (2.7.3.1); the relationship between malware infection risk and web users' browsing behaviour (2.6); the technical shortcomings of web filtering devices in relation to categorisation of online content; end-users' risk perceptions of online activities (2.7.2.4.2); the character of professional judgements in information

security (2.7.2.4.1); and antagonism between IT professionals and end-users in relation to security (2.7.2.4.1). The work of Kolkowska (2006, 2011) influenced the present research in respect both of its findings and its research methods. It used semi-structured interviews and observations of behaviour and practice to study different security cultures within two academic departments of a single university, and their impacts upon end-user computing activity. It demonstrated the existence of a disjunction between the information security values and actual practices of IT staff, which it was thought could possibly be paralleled within the study settings (2.7.2.4.1).

Section 2.4 outlined current overall trends in clinical information behaviour and gave an account of those of its features and characteristics which are of relevance to assessing the effects upon it of technical and organisational barriers, which are the focus of RQ2 (1.6). The importance of time constraints upon information seeking was emphasised. As described in Section 2.4.7, several information behaviour studies referred to the importance of cultural attitudes to information seeking in determining access to computer facilities for accessing the Internet, contributing to the focus on these in RQ3. The “cyber-bureaucrat” view of personal web use (PWU) identified by Anandarajan, Paravastu and Simmers (2006) was identified as a possible accurate definition and description of negative management attitudes to use of the web in general for information seeking, again highlighting the importance of cultural attitudes and presuppositions in determining levels of access to published information.

Generally, the specific frameworks and theories which were discussed informed the analysis and discussion rather more than the actual research design. While the examination of information behaviour theories in Section 2.4.2 (Wilson’s second model, the satisficing and information horizon concepts) yielded some useful conceptual frameworks for considering the effects of non-availability of information (see below, Section 11.3), these did not strongly inform the research questions, aims and objectives.

Risk management is a fundamental problem for NHS organisations. The discussions of issues of public trust, risk and regulation as they bear upon the cultural and organisational characteristics of the NHS, and of conflicts between powerful professional interests (as presented, for example, by Brown et al. (2011) in Section 2.5.5.2), strongly informed RQ3. They were also central to the analysis. The work of Currie *et al.* (2012) in relation to risk identification and professional power (2.5.5.2) can be highlighted in particular. The job demands-resources model (2.5.5.3; Figure 2.4) provided a conceptual framework for evaluating the effects on staff engagement of lack of access to published online information. Kanter’s theory of structural empowerment, as developed by Laschinger and

associates (2.5.6.1), highlighted the importance of access to information in staff empowerment and engagement, while Clegg's (1999) circuits of power theory using ANT, as applied to information security by Inglesant and Sasse (2005a, 2005b)(2.5.6.2), addressed an information security scenario commonly experienced within the NHS. Both theories provided important bases for later discussion and theory building. Consideration of the nature and influences of occupational subcultures was informed by Schein's (1996) organisational culture framework (2.5.1).

The importance of organisational approaches to the management of risk was highlighted in the previous paragraph. The sociological theories of risk and risk perception outlined in Section 2.7.1 clarified the organisational and cultural influences to which risk perception and risk management could be subject. The typology of approaches to information security risk management which were identified and described in Section 2.7.2.4.1, and the range of innovation frameworks discussed in 2.8.6, were important in characterising the risk culture of the NHS in relation to user-driven IT innovations and to web filtering. Prince et al.'s (2010) framing of information access issues in terms of approaches to risk management in IT services strongly influenced the research design and data collection in this study.

As stated above (2.7.4), references to technical barriers to accessing information made within studies of information behaviour or e-learning implementation were brief and generally uninformative. Also no studies appear to have been conducted of IT service quality or IT service climate within NHS settings, hence of the quality of infrastructure and technical support (2.8.5), and no British studies of IT subcultures were identified. Recent LIS-oriented British studies of web filtering and its impacts have focused solely on public library services, and not addressed the issue elsewhere within the public sector (2.7.3.4.2). The studies of Resnick *et al.* (2004) were important in establishing an evaluation methodology for web filters; however, they were conducted ten years before the present study was undertaken. Since Resnick *et al.*'s work concerned consumer health information, and was based in the United States, it had limited applicability to the NHS context (2.7.3.4.2). Only four studies in all (2.7.3.4.2) were identified that directly addressed technical and organisational obstacles to information seeking and e-learning within health contexts in any detail. One of these (Childs et al., 2005) related to e-learning, another (Chamberlain et al., 2015), to the use of mobile devices, the latter published only during the analysis and writing-up phase of the research. The only two detailed studies relating to web filtering and other security-related technical barriers to information seeking, use and sharing in general within the NHS have been the unpublished TDAG survey (2009) and that of Prince *et al.* (2010). Personal web use, and the effectiveness and organisational appropriateness of measures to prevent or minimise it (via deterrence, detection, and

prevention) has not been studied in health service contexts. No studies were identified of professional Web 2.0 / social media use within the NHS, or of IT acceptable use policies relating to the NHS, and social media policies in particular; the work of Scragg, Shaikh, Shires *et al.* (2017) and Scragg, Shaikh, Robinson, and Mercer (2017) was published only at a very late stage of the research process. Lafferty's (2013, 2015) detailed report on obstacles to social media use for e-learning within the NHS and their impacts did not discuss organisational issues in any depth. No studies were found of decision making in information security management within health services; all the published work identified related to the private sector or to academia (2.7.2).

Reference was made earlier (2.5.3) to the value-laden nature of IT in general. Within a secure web gateway (Section 2.6.4) the vendor's cultural values and priorities could be envisaged as implicit within the available categorisations of website content and the recommended or default security settings (2.8.4 above); *cf.* the comments of Willard (2002), Ayre (2004) and Houghton-Jan (2008) regarding value-laded categorisations of web content by vendors (Section 2.7.3.4.2). The possibility thus arises that the value systems of the commercial developers of web security gateways, embedded within the technology, are being imported into the NHS without adequate reflection or consultation, and may represent a poor "cultural fit" with aspects of the culture of the NHS.

The literature across the relevant subject areas has thus been reviewed and synthesised, and gaps identified, from which the research questions have been developed. An opportunity has been clearly identified 1) to characterise the nature of technical and policy-related restrictions on access to published professional information within the NHS (RQ1); 2) to assess their effects upon information behaviour and working practices (RQ2); and 3) to investigate the underlying organisational issues (RQ3). Owing to the wide range of issues involved and the lack of previous work in the area, the study needed be wide in scope and of an exploratory character (Yin, 2009).

Chapter 3. Methodology and methods

3.1 Introduction

The aims and specific objectives of the research, and the research questions, were set out in Section 1.5. The overall aim was to investigate barriers to online professional information seeking, use and sharing within the English NHS and their possible effects. Its specific aims were threefold: to establish in detail the nature of these barriers; to determine their effects within the contexts of clinical and management practice, education and research, and their possible consequences; and to investigate cultural factors among the different stakeholder groups which could bear on information seeking, use and sharing, and the influences they might be exerting,

An important clarification requires to be made regarding the usage of the terms “methodology” and “method”. “Methodology” may be used 1) simply to refer the study of methods; 2) to refer to the actual methods used in a particular piece of research, so that each study is considered to have its own methodology; 3) to refer to particular combinations of methods that occur many times in practice or are designed *a priori*, or to structured sets of guidelines or activities; Checkland’s soft systems methodology or grounded theory would be examples; 4) to characterise the process of research. It may also be used in a much more fundamental sense 5) as equating to “philosophy of methods” (Sapsford, 2006), “ways of acquiring knowledge” (Stahl, 2007), or “overall logic of enquiry” (Cecez-Kecmanovic & Kennan, 2013), including a set of philosophical assumptions or a particular paradigm as a foundation for the selection of particular research methods, and an overall strategy of conducting research, including the construction and justification of knowledge claims (Cecez-Kecmanovic, 2011). “Method” generally refers to well-defined sequences of operations (e.g. focus groups, surveys, interviews, ethnography, documentary analysis, walk-throughs) that, if carried out proficiently, yield useful results (Mingers, 2001, citing Checkland, 1981, and Livari, 1998).

3.2 Methodology / philosophy of social science

3.2.1 Introduction

Methods of social research are not neutral tools; they are closely connected with different visions of how social reality should be studied (Bryman, 2008) and hence to different theoretical perspectives (Crotty, 1998) and philosophical assumptions concerning the nature of social reality (Creswell, 2007). The areas of philosophy concerned may be identified as follows: ontology (the nature of reality), epistemology (how knowledge claims are established), axiology (the purposes served by the research, and the values it embodies) and logic (the nature of scientific explanation) (Cecez-

Kecmanovic, 2011). These are inter-related, insofar as epistemology depends upon ontology (explanations of how knowledge of the world is attained depend upon what that world is believed to be) and particular ontological, epistemological and axiological assumptions may lead to the choice of certain methodologies rather than others (Dobson, 2001, citing Rowland, 1995) and to particular viewpoints regarding the nature of scientific explanation. It is therefore important that researchers should be clear and explicit about their ontological and epistemological assumptions before starting any research project (Guba & Lincoln, 1994 cited by Andrade, 2009). Scholars differ in the role they assign to philosophical background in actually determining methodology: some (Cecez-Kecmanovic & Kennan, 2013; Dobson & Love, 2004, citing Garcia & Quek, 1977) suggest indeed that philosophical and theoretical assumptions should provide the the starting point for a choice of methodology and initial guidance for the research process, while others more open to multi-paradigm or mixed-method approaches (e.g. Crotty, 1998; Patton, 2002), take a more pragmatic – or possibly pragmatist - view, regarding the research question as the primary determinant of the research approach.

Social science research is shaped, explicitly or otherwise, by what are often referred to as paradigms. There is no agreed definition of what is meant by the term “paradigm”. As originally employed by Kuhn (1970, cited by Mingers, 2004a) the term referred to a broad underlying theoretical and conceptual framework (e.g. Newtonian physics) that is not questioned within “normal” scientific activity. This framework is considered to inform all actual experimentation. A paradigm is said to develop from a high degree of professional consensus established within particular communities of scientific researchers regarding aspects of theories, standards for research and established findings; it involves aspects of fundamental philosophical beliefs. Within the classical Kuhnian account, one paradigm is normally dominant, to the exclusion of others: only at times of “revolutionary science”, when many problems in explaining research findings within the prevailing paradigm become manifest, do rival paradigms compete. The newer, theoretically more satisfactory paradigm that emerges within a scientific field must then totally supplant its predecessor. However, within social science, Burrell and Morgan (1979), whose own typology of paradigms has been highly influential within organisation studies, put forward the idea that competing paradigms (defined more broadly than in Kuhn’s usage to refer an explicit combination of assumptions about the world and of knowledge) can co-exist within a discipline. They maintained moreover that social research methods are bound to particular paradigms, and that paradigms themselves are incommensurable, i.e. that their ontological and epistemological presuppositions are so pervasive that it is literally impossible to compare them (Mingers, 2001). A substantial body of scholarly opinion (including Bryman, 2011; Lincoln, Lynham, & Guba, 2011; Mingers, 2001, 2003, 2004b; Orlikowski & Baroudi, 1991; Venkatesh, Brown, & Bala, 2013) now disputes this position, however, arguing in favour of methodological

pluralism in various forms. The issue of paradigm relationships in the information systems field is discussed extensively by Fitzgerald and Howcroft (1998), Goles and Hirschheim (2000), and Mingers (2004b).

Chalmers (1982, cited by Willis, 2007) identified five components of a paradigm: stated laws and theoretical assumptions; standard approaches to applying these in particular contexts; characteristic experimental methods and techniques, guiding metaphysical principles, and general methodological prescriptions. A paradigm is thus not solely a philosophy of science; it includes relevant theoretical perspectives and their associated research frameworks, and the manner of their application to practice (Willis, 2007). Overall, research paradigms have been variously classified; the categorisation of research paradigms that has been most influential within information systems research is that of Chua (1986): into positivist, interpretivist, and critical (Mingers, 2004c; Myers & Klein, 2011). A comprehensive and very useful overview of paradigms within organisational and management research is provided by Cunliffe (2010).

An overview of the main social science research paradigms is offered below in Sections 3.2.2 to 3.2.5.

3.2.2 Positivism

The positivist paradigm⁴⁸ is based on an objectivist ontology and epistemology: it is claimed that there is a world of objective reality that exists independently of human beings and that has a determinate nature or essence that is knowable (Chua, 1986). Moreover, subject and object are held to be distinct, hence the researcher is considered to be independent of the object of the research, and observations and generalisations are free from temporal and situational constraints. Positivism embraces also a correspondence theory of truth, i.e. the notion that research is concerned with producing accounts which correspond to an independent reality of objects and structures, knowledge being achieved when a subject correctly discovers and “mirrors” this (Dobson & Love, 2004; Hirschheim, 1985). Positivist research is characterised by formal propositions; the use of quantitative techniques which emphasise the quantification of constructs (although qualitative research can also be carried out within the positivist paradigm (Myers, 1997); the assignment of numerical values to perceived qualities of things; the use of variables; the drawing of inferences

⁴⁸ The researcher does not discuss here different forms of positivism, or historical controversies between positivists and anti-positivists; a useful summary treatment is offered by Hirschheim (1985).

concerning a phenomenon from the study sample to the specified population; and experimental or statistical control for sources of error. It tends to assume that human activity is intentional and rational, or at least boundedly rational, and that conflict within organisations or societies is dysfunctional. It claims that real, uni-directional cause-effect relationships exist that are capable of being identified and tested via hypothetico-deductive logic and analysis, in an attempt to improve predictive understanding of phenomena (Orlikowski & Baroudi, 1991). Qualitative research can also be carried out within the positivist paradigm (Myers, 1997).

Positivism is claimed to be *nomothetic* (Greek νόμος "law" + τίθημι "to put, place, lay down"): it is said to be concerned with establishment of causal laws, i.e. formal expressions of causal relations, and hence also with prediction and control (Hirschheim, 1985; Myers, 1997). The nomothetic/idiographic distinction is ascribed to Windelband (1894, cited by (Hirschheim, 1985). Positivism is thus concerned with generalisability of a theory or theoretical statements. From the positivist viewpoint, theory can be tested against irreducible statement of observation, "the facts". Positivists hold the "naturalist" viewpoint that the method of the natural sciences is the only rational source of knowledge, and should therefore be applied within the social sciences. This implies that understanding social phenomena is to be seen primarily a problem of modelling and measurement, of developing an appropriate set of theoretical constructs and an accurate set of instruments. Sample surveys and controlled experiments are the primary data collection techniques. Positivism is concerned with replicability, internal validity, external validity, and reliability as quality criteria (Cecez-Kecmanovic, 2005; Johnson & Duberley, 2000; Orlikowski & Baroudi, 1991; Pather & Remenyi, 2004). It claims to be value-free, i.e. that there is a total disjunction between facts and values, that selection of the objects and methods of study can be determined by objective criteria rather than by human beliefs and interests, and that researchers are detached from the phenomena they study (Orlikowski & Baroudi, 1991). Positivism remains the dominant paradigm within information systems research (Chen & Hirschheim, 2004; Orlikowski & Baroudi, 1991; Walsham, 2013) and indeed within most scientific disciplines (Hirschheim, 1985).

3.2.3 Interpretivism

The interpretivist paradigm emerged historically in opposition to positivism in efforts to comprehend and explain human and social reality (Pather & Remenyi, 2004). It is often linked to the claim of Dilthey (later taken up by Weber) that human phenomena had to be understood in their social and cultural context and that the task of the social sciences is that of *verstehen*, of recognising meanings, understanding, contrasted with *erklären*, explaining, focused on causality, that is the approach of the natural sciences (Crotty, 1998; Johnson & Duberley, 2000; Willis, 2007). The roots of interpretivism are claimed to lie in the work of Geertz and others in ethnography, of Gadamer in hermeneutics, and

of Husserl and Heidegger in phenomenology, particularly the latter's concept of intentionality: the notion that all mental phenomena have reference to a content or direction towards an object (Crotty, 1998; Lee, 1991; Stahl, 2013). It is sometimes stated by interpretivists that the approach of the social sciences should be *idiographic* (Greek *ίδιος*, -α, -ον, "one's own" + *γραφω*, "to write"), focused on the individual, rather than *nomothetic*, concerned with the establishment of general laws. Interpretivism is based on the notion that "people create and associate their own subjective and inter-subjective meanings as they interact with the world around them" (Orlikowski & Baroudi, 1991, p. 5). Through such social interactions, meanings and norms become inter-subjectively real, and are perceived as a given social reality which presents to the individual in a fashion analogous to that of the natural world. The meanings and intentions of action are "retrospectively endowed" and are "grounded in social and historical practices" (Chua, 1986, p. 615). Interpretive research thus attempts to understand social phenomena through accessing the meanings that they hold for participants: it takes an insider (emic) rather than an outsider (etic) perspective (Morey & Luthans, 1984). Also it "does not predefine dependent and independent variables, but focuses on the complexities of human sense making as a situation emerges" (Myers, 1997, p. 245).

According to Walsham (1995, p. 376),

"... interpretive methods of research adopt the position that knowledge of a reality is a social construction by human factors. In this view, value-free data cannot be obtained, since the enquirer uses his or her preconceptions in order to guide the process of enquiry, and furthermore the researcher interacts with the human subjects of the enquiry, changing the perceptions of both parties".

The implication here is that not merely social reality but "all meaningful reality, precisely as meaningful reality, is socially constructed" (Crotty, 1998, p. 55). While embracing a form of realist ontology - objects in the world may be considered to be "always already there" (Crotty, 1998, p. 44, citing Heidegger and Merleau-Ponty, *passim*) - the doctrine of intentionality, which requires the interaction of subject and object, means that there can be no dichotomy between objective and subjective. Interpretivism therefore, unlike postmodernism, does not embrace a subjectivist epistemology. Regarding the relationship between natural and social sciences, interpretivists typically hold that "the social world is entirely different from the natural world, being constituted through language and meaning, and thus involving entirely different hermeneutic, phenomenological or social constructivist approaches." (Mingers, 2000, p. 6). The argument here has two foci: it can be an ontological one, the idealist view that social objects do not exist in the way that physical ones do (i.e. as subject-independent), and/or it can be an epistemological one, that "there is

no possibility of facts or observations that are independent of actors, cultures or social practices” (Mingers, 2000, p. 6). In the case of social phenomena a so-called double hermeneutic or subject-subject relation is required (Giddens 1976, cited by Crotty, 1998): an interpretation of social actors’ interpretations, involving interplay of lay and academic language. This is said to contrast with the task of the natural sciences researcher, who is able to study nature as it were from the outside, a subject-object relation, and to construct a theoretical meta-language, avoiding or minimising the use of lay language. According to Walsham, “interpretive methods of research in information systems are aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context” (Walsham, 1993, pp. 4-5).

Research methods within the interpretive paradigm include action research, case studies, ethnography, diary studies, phenomenography and grounded theory (Myers, 1997; Webb, 2008). Interpretive studies rely on naturalistic techniques for investigating the phenomena of interest, such as interviews, observation, and documentary analysis. It should be noted that “interpretive” is not at all coterminous with “qualitative”: interpretivist research can include quantitative data, and positivist research can include qualitative data (Myers, 1997). The procedures of interpretivism as a research strategy are characterised as inductive, emergent, and “shaped by the researcher’s experience in collecting and analysing the data” (Creswell, 2007). The researcher does not seek to generalise from the research setting to a wider population; rather, the intention is to attain a deeper understanding of the nature of a phenomenon, in order to inform other settings (Orlikowski & Baroudi, 1991). Social order is assumed (Chua, 1986; Hardy & Clegg, 2007). Klein and Myers (2001) provide an overview of types of interpretive research in information systems.

3.2.4 Critical theory

Scholars and practitioners within the critical theory paradigm tend to focus on the impacts of power relations in human societies. Its approach is rooted in the neo-Marxist critical social theory of the Frankfurt School, and its later development within the work of Habermas and of post-modernists such as Bourdieu and Foucault. Critical social theory is not a single body of work, but denotes a range of approaches and theories (Cecez-Kecmanovic, Klein, & Brooke, 2008; Myers & Klein, 2011). Key concepts include knowledge interests, communicative action, lifeworld (Habermas); genealogy of knowledge, panopticon, disciplinary power (Foucault); habitus, form of capital (cultural, social, symbolic) (Bourdieu) (Myers & Klein, 2011). Although, like interpretivism, the critical theory paradigm in social research emerged in opposition to positivism, the focus within the critical tradition is less on methodology than on axiology, the purposes of research being generally aimed at

uncovering such relations, and conveying to its readership both their existence and their disenfranchising of some groups while granting excessive power and resources to others (Willis, 2007); to this extent, its orientation is explicitly and consciously ideological. According to Stahl (2008), the most important defining feature of critical social research is its intention to promote emancipation. Alvesson and Deetz (2000, cited by Myers & Klein, 2011), identify three elements of critical research: *insight*, *critique*, and *transformative redefinition*. its general principles are summarised by Ngwenyama (1991) as follows: people have the power to change their world; knowledge of the social world is value-laden; reason and critique are inseparable; theory and practice must be interconnected; and reason and critique must be reflexive in practice. According to Cecez-Kecmanovic (2001, p. 143), while interpretive researchers within the information systems field aim to understand and describe multiple meanings ascribed to an information system and its impacts in one or more contexts, critical researchers:

“ ... go further to expose inherent conflicts and contradictions, hidden structures and mechanisms accountable for those influences ... [they] aim to reveal interests and agendas of privileged groups and the way they are supported or protected by a particular information system design or use. More generally, they aim to discover and expose attempts to design and misuse [information systems] to deceive, manipulate, exploit, dominate and disempower people. By doing do they aspire to help them resist these attempts, hinder such misuse of [information systems] and promote liberating and empowering IS design and use”.

Critical theory claims that the social reality experienced subjectively by actors within organisations is historically, socially, culturally, politically and materially conditioned and produced; it may be conceptualised as a series of “layers” (Cecez-Kecmanovic, 2005). Key concepts within critical research are *ideology* (a particular and dominant worldview that privileges certain interests while hiding this fact by making the present state of affairs appear “natural”), *hegemony* (the mechanisms by which this is achieved), *reification* (“the process whereby social structures become solid, become things, which then cease to be the subject of social negotiation” (Stahl, 2008, p. 3)), and *commodification* (the process by which, once something has become reified, it can then become a commodity, something to be bought and sold (Stahl, 2008; Stahl, Doherty, & Shaw, 2012; Stahl, Tremblay, & LeRouge, 2011)). Like interpretive research, critical research is idiographic in character (Myers & Klein, 2011); however, unlike interpretive research, critical theory assumes that social change, conflict, coercion and disintegration is endemic to human societies (Hirschheim & Klein, 1989). Critical social theory does not have a distinctive research methodology; it adapts interpretive research methods (e.g. ethnography, documentary analysis, interviews, focus groups) to its needs, while stipulating that these be of a practice-oriented, participatory and reflexive kind (Ngwenyama,

1991; Stahl et al., 2011). Myers and Klein (2011) suggested that critical researchers should organise their data collection and analysis around the core concepts and ideas from one or more critical theorists.

3.2.5 Critical realism

Several scholars in the information systems field have proposed the critical realism of Bhaskar (1978, 1998) and others as a possible philosophical solution to its methodological disputes (Smith, 2006); it is the philosophical position favoured by the researcher, to whom it has a strong intuitive appeal. Critical realism is characterised by a so-called transcendental realist ontology (a belief in the reality of the world independent of our knowledge of it, and of mechanisms of cause and effect within that world; the so-called *intransitive dimension*) combined with a form of epistemological relativism according to which it is held that knowledge is always socially constructed: different observers may apprehend different realities according to different *transitive* transactions - the varying paradigmatic, metaphorical or discursive conventions employed through their human agency (Al-Amoudi & Willmott, 2011; Johnson & Duberley, 2000; Steinmetz, 1998). A stratified ontology is proposed, whereby reality is said to comprise three layers: causal structures or generative mechanisms; the actual events that these generate or produce, and the subset of effects from these events that are mediated empirically, i.e. experienced or observed: According to Mingers (2000, p. 1261), these layers are known as the domains of the *real*, the *actual* and the *empirical*. "The real contains mechanisms, events and experiences, i.e. the whole of reality; the actual consists of events which do (or do not) occur, it includes the empirical, i.e. those events that are observed or experienced."

	Domain of real	Domain of actual	Domain of empirical
Mechanisms	X		
Events	X	x	
Experiences		x	x

Table 3.1 Stratified ontology of critical realism

Redrawn from Wynn and Williams (2012, p. 791), after Bhaskar (1975, p. 13)

Stratification is also held to exist within the realm of objects themselves, in that "causal powers at one level (e.g. chemical reactions) can be seen as generated by those of a lower level (e.g. atomic valency)" (Mingers, 2004c, p. 162). Individual phenomena are described as emergent from a particular level, but as not reducible to that level. Once emerged, a phenomenon has properties that are proper to it as a system at that level (Mutch, 2010). The domain of the real is thus to be

conceived of as “a complex interaction between dynamic, open, stratified systems, both material and non-material, where particular structures give rise to certain causal powers, tendencies or ways of acting” (Mingers, 2000, p. 1262). Both physical and social sciences are held to involve “socially mediated transitive transactions with the ‘common referent’, i.e. an *intransitive* reality” (Johnson and Duberley, 2000, p. 162). With regard to the subject matter of the social sciences, critical realism maintains that social structures are not simply a product of social discourses, but have distinctive, real properties (Ackroyd, 2004). For the critical realist, the enduring structures of social reality and human agency reciprocally presuppose each other, but cannot be reduced to, nor reconstructed from, nor explained in terms of each other. Society as a separate entity emerges from the activities of individuals (Mingers, 2004c). Social structure is a necessary condition of any human activity, but pre-existing structures are reproduced and transformed through human agency (Elder-Vass, 2008; Johnson & Duberley, 2000). Social structures can be considered causal in that they have an “objective influence which conditions action patterns and supplies agents with strategic directional guidance” (Archer, 1995, cited by Smith, 2006, p. 202).

This principle is elaborated within Bhaskar’s (1989, cited by Faulkner & Runde, 2013) Transformational Model of Social Activity (TMSA), in which he posits both a *duality of structure* (human agency and social structure are recursively organised, i.e. that social structure is constantly reproduced as an ongoing consequence of human activities, where those activities both presuppose and are conditioned by the structures that are being reproduced) and a *duality of praxis* (the reproduction and transformation of social structure is a generally unconscious and unintended consequence of human action). It features also in the work of Archer (1995, cited by Mutch, 2002, 2010) via her concept of morphogenesis. Archer argued that, in examining a particular social interaction, analysis must start not when the actual interaction itself takes place (time T2 to T3) but at time T1 when the related structural conditioning occurred, itself the result of human activities. The social interaction results in a so-called structural elaboration at time T4. This structural elaboration then forms part of the structural conditioning for the next morphogenetic cycle. For the purposes of analysis, both approaches hold apart the categories of agency and structure. It is thereby implied that social science is essentially similar to natural science, while incorporating modifications and differences of method reflecting the particular character of the social world (Mingers, 2004b; Sayer, 1992). In particular the nature of Giddens’s “double hermeneutic” is recognised: the theory that “social science is not only affected by society, but at the same time an effective agent in shaping society; that is, social science is internal to its ‘subject matter’ in a way natural science is not” (Giddens, 1984, cited by Özel, 2002, pp. 16-17).

Critical realism understands the aim of social science to be the identification of the structures which generate behavioural tendencies through the examination of social phenomena (Johnson & Duberley, 2000). The task of the researcher is thus to use perceptions of empirical events to identify the mechanisms through which underlying (real but unobservable) structures give rise to those events (Volkoff et al., 2007, citing Collier, 1994). "To the extent that individual human actors are components of the structures in which a given set of events takes place, they are considered as *bearing causal powers* based on their thoughts and beliefs [as to] how given actions are linked to consequences ... As a result, critical realism views an actor's reasons as the generative mechanisms which are the cause of a given action" (Wynn & Williams, 2012, p. 791). Other entities within the research environment, such as social structures, physical objects, and technological artifacts, are also considered to bear causal powers, capacities or liabilities. A liability may be described as "a susceptibility to the action of other entities" (Easton, 2010, p. 120).

The production of knowledge occurs, however in what is termed the *transitive dimension*; it is a social process and thus subject to epistemic relativity. Studies based on critical realism may therefore involve interpretive forms of investigation (Radulescu & Vessey, 2009). The position of critical realism is thus that, while our knowledge of the world is inevitably fallible and socially constructed, and it is not possible to establish an absolute foundation for knowledge, there are rational criteria for preferring some theories to others, on the grounds of providing better explanations (Johnson & Duberley, 2000; Mingers, 2004c; Sayer, 1992; Smith, 2006; Wikgren, 2005; Wilson & Greenhill, 2004). Critical realism shares with pragmatism the epistemological doctrine of fallibilism: that knowledge is never certain, but always hypothetical and subject to correction. A primary objective of social science research conducted in accordance with critical realist principles is to conceptualise and construct theories, and to develop explanations of phenomena through explicating their specific mechanisms: how they are generated by structures, actions and contextual conditions involved in a particular setting (Wynn & Williams, 2012). This corresponds closely with the aims and objectives of the present research, as framed in Section 1.5.

Causality and the identification of causal mechanisms is a primary focus in critical realism, which gives research conducted under critical realist principles a particular relevance to policy (Ackroyd, 2004). "Causes" here can include reasons for action or for thought (Sayer, 2000). This is a major difference from interpretivism, which rejects any notion of the causal power of the natural and social worlds, and which tends to generate explanations of phenomena in terms of how actors understand their roles in a particular social setting, and of how subjective meanings are developed and sustained (Smith, 2006; Wynn & Williams, 2012). The outcome of a mechanism is considered to be dependent upon context. The context-mechanism-outcome framework (Pawson & Tilley, 1997,

cited by Bygstad & Munkvold, 2011) may be applied in the description of mechanisms. Explanation of causal mechanisms within natural phenomena or social structures should be generated via a form of inference termed *retroduction*, which asks “what must be true in order to make this event possible?” (Easton, 2010). The process of retroduction is distinct entirely from generalisation, which charts the extent of phenomena (Carlsson, 2003, citing Layder, 1993; Sayer, 2004). Retroduction involves “the postulation of a hypothetical mechanism(s) or structure(s) that, if they existed, would generate the observed phenomenon” (Mingers, 2000, p. 1262). It is related to Peirce’s concept of abduction (Mingers et al., 2013), although focusing on causality rather than on the creation of new conceptual frameworks (Dobson, 2012). The component phases of the overall process has been summarised as follows: by as: “What is happening? Why is it happening? How could the explanation be different? And, so what?” (Mingers 2001, p. 246). Critical realists accept that patterns of causality may be complex, and that some causal mechanisms may be non-physical and non-observable (Angus & Clark, 2012). Explanatory theories need to include *enabling conditions*, *stimulus conditions* or *releasing conditions* for causal mechanisms, as applicable. The open nature of complex social systems makes it generally impossible to predict events that might arise from a given initial event or change in social structure; however it does not preclude the manifestation of a particular causal mechanism in different but similar settings, or the recurrence of the mechanism in the same setting; these so-called demi-regularities are taken to indicate the occasional realisation of a causal mechanism within those settings. The identification of widely differing outcomes across similar settings may also contribute to the understanding of causal mechanisms (Wynn & Williams, 2012).

A key question must be: what are the rational criteria for evaluating the causal explanations offered by scientists of observed events? How may the “generative mechanisms” proposed by scientists – or social scientists – be distinguished from fictions of the imagination, or fantasy, without involving a retreat into some form of idealism (the notion that “reality is in some way mental” (Lacey, 1976))? “What restrictions are there upon the mechanisms that can be invoked as causal explanation ... why not demons or witches’ spells?” (Halfpenny, 1995, cited by Johnson & Duberley, 2000, p. 156) How can science involve socially mediated transitive transactions with the “common referent” – an intransitive reality – without falling into the problems either of traditional forms of empiricism (“experience cannot provide us with knowledge of intransitive reality”) or of postmodernism and relativism (“science is exclusively self-referential, as in postmodernism”) (Johnson & Duberley, 2000, p. 162)?

Although he does not use the term, Sayer puts forward what appears to be a pragmatist form of argument to answer this challenge: “Knowledge claims involve practical commitments, that if one

does such-and-such, certain things will result". "Truth might better be understood as 'practical adequacy', that is in terms of the extent to which it generates expectations about the world and about results of our actions which are realised" (2000, pp. 42, 43). "They are realized because of the nature of the associated material interventions ... and of their material contexts. ... Although the nature of objects and processes ... does not uniquely determine the content of human knowledge, it does determine their cognitive and practical possibilities for us." (1992, p. 70). As well as stressing the theory-dependent nature of perception, the role of metaphor in constructing conceptual systems, and the difficulty of separating the conceptual and the empirical, Sayer emphasises the practical context of knowledge: "We develop and use concepts not only through and for observing and representing the world but for acting in it ... conceptual systems concern not only what we (think we can) observe, but what we can do and how we do it" (1992, p. 59). Other critical realists have proposed so-called *judgmental rationality* as a means of evaluating and comparing alternative explanations of phenomena, in which explanatory power in terms of existing knowledge becomes the criterion for selection and adoption (Wynn & Williams, 2012).

This "pragmatist" argument of Sayers invites comparison with the "pragmatic maxim" of Peirce: "Consider what effects, which might conceivably have practical bearings, we conceive the object of our conception to have. Then, our conception of those effects is the whole of our conception of the object." (Peirce, 1878, cited by Haack, 1976) However, for Peirce, the *entire meaning* of a concept is identified with "the conceivable practical consequences,—that is, the consequences for deliberate, self-controlled conduct,—of the affirmation or denial of the concept" (Peirce, 1904, cited by Haack, 1997). Put more simply, meaning is solely about "what works", experientially or practically (Haack, 2003); Peirce's form of pragmatism thus equates criteria and definitions of truth (Haack, 1976). This type of view is characterised as "instrumentalism" by Sayer, who regards its criteria of truth, which focus on outputs, as insufficiently rigorous. Sayer's own position is arguably closer to that of another of the American "classical" pragmatists, Dewey (Johnson & Duberley, citing Dewey, 1897, p. 17); Sayer's concept of practical adequacy maintains that inputs (assumptions, categories) to a theory are important as well as its outputs (usually predictions). It also requires theories to work in other contexts and to be consistent with other knowledge and practices.

Sayer (2004) believes critical realism to be compatible in principle with some post-structuralist or postmodernist social theories. Walsham (2006) believes an interpretivist research strategy to be compatible also with a critical realist philosophical standpoint; critical realism does, of course, have common ground with interpretivism in that it holds a view of social phenomena as concept-dependent and requiring interpretive understanding (Zachariadis, Scott, & Barrett, 2013). Critical

realism embraces the hermeneutic production of meaning (Bhaskar, 1979, cited by Wikgren, 2005) and accepts the necessity of a hermeneutic phase of inquiry.

Critical realism is said to support a variety of quantitative and qualitative research methods, on the grounds that it recognises the existence of different types of (physical, social, and conceptual) objects with different ontological and epistemological characteristics (Mingers, Mutch, & Willcocks, 2013; Zachariadis et al., 2013). These include ethnography, participant observation, interviews both structured and unstructured, descriptive statistics, and action research. The only methods effectively excluded are those based in strong social constructionism, such as discourse analysis (Georgaca & Avdi, 2011; McEvoy & Richards, 2003; Reed, 2005). Critical realism does not, however, offer a ready-made set of concepts which can readily be applied within subject domains (Mutch, 2010) or guidelines on the actual conduct of empirical research. (Raduescu & Vessey, 2009). The role of critical realism has rather been perceived as one of “offering guidelines for social science research and starting points for the evaluation of already established methods” (Danermark et al., 2001). Raduescu and Vessey (2009, citing Merton, 1968) have suggested that the research methods adopted in critical realism-based studies should be determined by the relative strength and availability of the mid-range domain-specific theories that relate to the research problem. According to their scheme, such theories determine the degree of so-called problem structure, which in turn should determine the degree of structure in the problem-solving method. They categorise the latter as follows: Type I: *structured* (strong domain-specific theory exists), Type II: *structurable* (extant theory is related only indirectly to the research problem, or is not readily identified as relevant), and Type III: *unstructured*. Unstructured problems require the use of research methods that are unstructured or exploratory in nature. They propose different schemata for the three types of problem; that for Type III, to which the present study is closest, is shown below in Figure 3.1.

Critical realism has gained ground within the information systems field as an underlying philosophy (Mutch, 2002, 2010; Raduescu & Vessey, 2009; Smith, 2006). Issue 37(3) 2013 of the journal *Management Information Systems Quarterly* was entirely devoted to theory building, research methods and applications of critical realism within information systems. It has been argued that critical realism, on account of its clear separation of structure and agency as set forth in Bhaskar’s TMSA and Archer’s concept of morphogenesis (above), and its implicit recognition of the materiality of technology, provides a sound basis for analysing the interplay between an organisation and its technology (Raduescu & Vessey, 2009; Volkoff et al., 2007). However, only a very small corpus of work, based upon qualitative case studies, makes explicit use of retroduction, as described above (Strong & Volkoff, 2010; Volkoff, Strong, & Elmes, 2007). Critical realism has been discussed by writers on LIS research methodology (Budd, Hill, & Shannon, 2013; Hjørland, 2000, 2005); however,

the researcher was unable to identify any explicitly critical realist studies within the information science field.

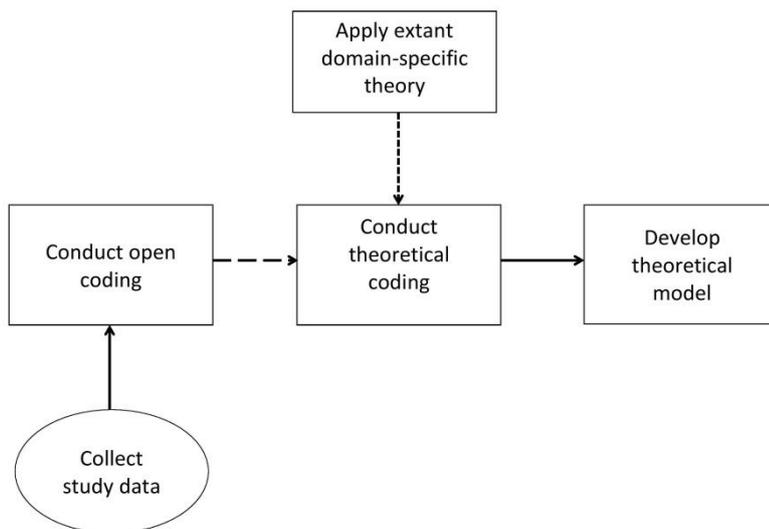


Figure 3.1 Unstructured research method with weak domain-specific theory (Type III)

Modified from Radulescu & Vessey, 2009, p. 8

Critical realism includes an emancipatory axiology (an ethical critique of social structures and mechanisms, based on principles of equity), although this is relatively undeveloped (Benton & Craib, 2011).

3.3 Research approach and design

Since the study was investigating factors impacting upon learning, and also the “practices, attitudes, values, and presuppositions” (and therefore experiences, perceptions, meanings, and understandings) of staff within NHS organisations relating to information behaviour and information security, the objectives of the research pointed clearly towards the adoption of a interpretive (and primarily qualitative) research strategy, using interviews of some form as the main data collection method. Two possible approaches were considered initially, ethnography and grounded theory.

Ethnography has been described as “the study of social interactions, behaviours, and perceptions that occur within groups, teams, organisations, and communities” (Reeves, Kuper, & Hodges, 2008). It is concerned with the meanings that participants in a social phenomenon or process assign to it (Cavaye, 1996), its focus being on culture rather than on individual experience (Roberts & Priest, 2010). Ethnographic interviewing and observation within an NHS Trust IT department was considered initially as a possible component of the study, since it could potentially have offered a rich and detailed picture of the putative IT subculture and of the decision-making processes of IT

staff. Such methods have been employed within studies of information security practitioners (Werlinger et al., 2009; Werlinger, 2008) and of NHS managers (Hyde et al., 2013; Matthews, 2009; Nicolini & Powell, s.d.). Such an approach was rejected, however, on the grounds both that the focus of investigation would be too narrow, and that the phenomena of interest would occur too rarely for time spent in direct observations to be productive, involving spending a disproportionate amount of time attempting to address only one of the main research questions.

Grounded theory is a method of qualitative enquiry in which data collection and analysis reciprocally inform each other through an emergent, iterative process (Charmaz, 2011). Radulescu and Vessey (2009) recommended grounded theory as an approach to analysing data in critical-realism-based studies in information systems where no single domain-specific theory can be identified *ex ante* as either directly or indirectly applicable to the research question. Its application in LIS research was described in detail by Mansourian (2006). This approach was therefore given initial consideration, as being a rigorous method generally considered suitable for theory development that appeared, at first sight, to fit the circumstances of the study. However, the main purpose of grounded theory is said to be to generate theories regarding social phenomena (Lingard, Albert, & Levinson, 2008). In particular, it can be used to discover social-psychological processes (Ploeg, 1999) and to explicate patterns of behaviour, particular where these are problematic for those involved (Glaser 1987, cited by Scragg, Shaikh, Robinson, & Mercer, 2017, p. 2). The research did not, however, have social processes or patterns of behaviour, as such, as a primary focus; hence, grounded theory would not have been appropriate to address the research questions (1.6) in their existing form.

A case study approach using a combination of qualitative methods was eventually selected as the most suitable research strategy, for a number of reasons. Case studies involve “intensive study of a single unit for the purpose of understanding a larger class of similar units ... observed at a single point in time or over some delimited period of time” (Gerring, 2004, p. 342). A case study should be of a “functioning specific” i.e. “a bounded and integrated system, with working parts and patterned behavior”, in which “consistency and sequentialness are prominent” (Stake, 1994, p. 236, cited by Pickard, 2007). Case studies lend themselves to investigations seeking to explain some present circumstance: “how?” or “why?” (Easton, 2010; Yin, 2009), using the case as a specific illustration (Creswell, 2007), which fits well with the overall research problem. They aim at a form of “rich” or “thick” description (Pickard, 2007; Wynn & Williams, 2012). They are appropriate for investigating phenomena where 1) a large variety of factors and relationships are included, which require to be disentangled, 2) no basic laws exist to determine which factors and relationships are important, and 3) the factors and relationships can be directly observed (Fidel, 1984). They can be used, as in this

case, where the boundaries between phenomena and context are not clear (Yin, 2009). In the information systems field, case studies have demonstrated their appropriateness for generating a “well-founded interpretive comprehension of human/technology interaction in the natural social setting” (Andrade, 2009, p. 44). Case studies are geared to exploring a complex situation in depth, since they “focus on a sustained consideration of activities and behaviour in a particular location” (Ackroyd 2010, cited by Wynn & Williams, 2012). They can be iterative, allowing the researcher to revisit the research site to test their understanding (Easton, 2010; Yin, 2009). A case study design, while basically linear in character, can evolve as a study progresses; it should not be too prescriptive initially, but should be allowed to emerge and respond to circumstances; the post-fieldwork plan especially should allow for considerable flexibility (Becker, 1970, cited by Fidel, 1984; Pickard, 2007).

Case studies use multiple sources of evidence, which should intersect in a triangulating fashion (Simons, 2008; Yin, 2009). The metaphor of triangulation within research methodology was proposed initially by Webb, Campbell, Schwartz, and Sechrest (1966, cited by Bazeley, 1999); it derives from techniques used in navigation and surveying, in which the location of a point may be determined by taking bearings to it from points at each end of a fixed baseline. These authors suggested that “the use of multiple data sources, methods, investigators, and theories contributed to greater reliability and validity of results in social science research” (Bazeley, 1999, p. 279). The aim of triangulation is to achieve a more accurate measurement and consequently a better approximation of a social phenomenon (May, 2010). Techniques or sources can be selected that are complementary, which have different biases or different strengths (Miles, Huberman, & Saldaña, 2014) or which aim to corroborate the same facts or phenomena (Yin, 2002, cited by Pickard, 2007, p. 86). Triangulation is not necessarily about corroboration, however; it may show divergences, which are potentially important in understanding a case (Simons, 2008). Methodological triangulation as a term often refers to the use of a combination of qualitative and quantitative methods, although it may refer equally well to a combination of qualitative methods (Shenton, 2004).

Case study as a research strategy is widely used within many social science disciplines (Creswell, 2007); for example, within the health information field they have been used within studies of health information services (Beverley, Booth, & Bath, 2003; Dowse & Sen, 2007; French, 2006; Wilkinson, Papaioannou, Keen, & Booth, 2009), information behaviour (Addison, Whitcombe, & Glover, 2012; Bawden & Robinson, 1997; MacDonald, Bath, & Booth, 2008), e-learning (Booth et al., 2005; Wong, Greenhalgh, Russell, Boynton, & Toon, 2003), information systems (Maguire & Ojiako, 2007) and information security (Fernando & Dawson, 2009; Kolkowska, Hedström, & Karlsson, 2009).

Authors on case study methodology have proposed differing categorisations of the types of case study. Stake (1995, cited by Baxter & Jack, 2008) distinguished between intrinsic and instrumental case studies; in the former, as the name implies, the case is of interest in itself, whereas in latter the case is of secondary interest, but is used to gain insight into an issue or to refine a theory. Yin (2009) distinguished between exploratory and explanatory case studies; the former is considered appropriate for addressing “what?” questions, whereas the latter seek to identify mechanisms and causal links via “how?” questions; it is however common for case studies to be both exploratory and explanatory (Tellis, 1997a). Levy (1988, cited by Tellis, 1997b) recommended the single-case explanatory- exploratory methodology as the most suitable choice for the investigation of information technology. The research questions in the present study (Section 1.5 above) were of both “what?” and “how?” types.

It was therefore decided to carry out an intrinsic, exploratory and explanatory case study using a combination of qualitative methods (semi-structured interviews and documentary analysis). The interviews were intended as far as possible to incorporate explication of critical incidents relating to information access (Urquhart et al., 2003). The study was planned to follow a nested or embedded single-case design, treating the NHS in England as the actual case (unit of analysis), with the individual Trusts (which provided clearly bounded organisational settings) as the nested sites of data collection (Thomas, 2011; Yin, 2009).

The choice of this particular form of case study design, and in particular the choice of sites to include, requires some explanatory comment. According to Thomas (2011), a nested case study differs from a multiple study in that it gains its integrity from the wider case. The case itself (the NHS in England) was considered intrinsic, since it was of inherent interest. The choice of sites, however, was instrumental in character; it reflected the considerations cited by authors on case study methodology in relation to selection of cases. According to Wynn and Williams (2012, p. 804), “the selection of a case usually reflects the existence of events which are representative of the phenomena a researcher is attempting to explain”. Creswell (2007, p. 75) recommended the selection of cases that show different perspectives on the problem, process or event at issue. Although the disparities had narrowed since the 1990s, IT infrastructure provision were widely recognised within the NHS LIS community as still being better developed within acute Trusts than within mental health or community health services Trusts. Anecdotal evidence indicated as well that there were wide differences between Trusts in overall corporate culture and climate, including prevailing attitudes to information seeking and evidence-based practice; also that their IT departments could vary considerably in levels of resource, quality of service and what might be

termed “customer focus”. Not all the phenomena which were of interest in this investigation were likely to be manifested within an individual NHS Trust. Tellis (1997a, 1997b) suggested that the selection of cases should offer the opportunity to maximise what can be learned, knowing that time is limited; selected cases should be “easy and willing subjects”. The selection of Trust(s) was intended to span the widest possible variation: in size, type of organisation (district general hospital, teaching hospital, mental health / community services), category of service (acute, mental health / community services), and in level of research and teaching activity, as described in Section 1.4.1. The inclusion of a large teaching hospital Trust located within a metropolitan area followed a strong recommendation from one of the pilot interviewees, P1, to do so on the grounds of there being major differences in culture between teaching hospitals and other acute general hospital Trusts. It was constrained in practice by considerations of geographical ease of access (proximity to the researcher’s home and quality of transport links) and the relative ease (or otherwise) of negotiating local research governance processes and gaining access to interview subjects. The three Trusts selected (a small district general hospital T1, a medium-sized mental health/learning disabilities/community services Trust T3, and a very large teaching hospital T4 with extensive research activity) were all located in the north of England. An approach to a smaller teaching hospital Trust (H9), located adjacent to one of T3’s sites, was not pursued, since a negative response was received from the Trust research manager to the researcher’s initial enquiry. The researcher subsequently approached T4, which, while offering the advantage of providing a wider contrast of organisation type and culture to the other Trusts than H9 would have done, was much larger, presenting issues in relation to data saturation (discussed further in Section 3.7.2 below).

Case study research is often thought not to tie in closely with any particular methodological approach (Cavaye, 1996). It is holistic in character rather than reductive (Verschuren, 2003). In terms of its methodological basis, it may be primarily positivist (Benbasat, Goldstein, & Mead, 1987; Dubé & Paré, 2003; Yin, 2009), or interpretivist (Klein & Myers, 1999; Oliver, 2006; Walsham, 1995a) in character, and its design may involve quantitative, qualitative or “mixed” methods. Easton (2010), Mingers (2004b) and Wynn & Williams (2012) argue, however, that critical realism fits well with use of the case study research design. They view the case study method, with its inherent explanatory focus and use of mixed methods and triangulation, as the best means of approaching the interaction of structures, events, actions and context in a manner that can identify and explicate the causal mechanisms which are the focus of interest (see section 3.1 above). Studying a limited number of NHS Trusts could be considered justified from a critical realist perspective, the intention being to “build an explanatory theory that matches the empirical facts as closely as possible”, and to “utilize the detailed causal explanations of the mechanisms at work in a given setting to obtain insights into

how and why a similar mechanism could lead to different, or perhaps similar, outcomes in a different setting” (Wynn and Williams, 2012, p. 804, citing Becker, 1990).

3.4 Research process overview

The overall process of the research is outlined in the flowchart and Gantt chart below (Figure 3.2, Figure 3.3). The flowchart illustrates the overall sequence and inter-relationships of the various processes of the data collection and analysis, while the Gantt chart provides more detail about the temporal sequence of the steps. It should be noted that data analysis began as soon as data became available; the ongoing analysis thereby both informed and was influenced by the later stages of data collection, as was desirable (Green et al., 2007; Thorne, 2000).

The external theoretical frameworks were applied only at the interpretation stage, i.e. was applied only after the data had been analysed and the results and background information written up in a near-final form, as described in Section 3.7. The overall process followed the recommendations of Eisenhardt (1989, cited by Andersen & Kragh, 2010) regarding the desirability of postponing consideration and discussion of existing theory until the later stages of a case study, as a means to minimise bias and undue limitation of the findings. It was thus comparable in character with Radulescu and Vessey’s diagram of an unstructured research process with weak domain-specific theory, as shown above (Figure 3.1). As indicated above, the success (or otherwise) of research governance applications informed the selection of Trust sites, and the nature of the data required a change in the proposed method of analysis.

3.5 Data collection

3.5.1 Interviews: introduction

Case studies typically use interviews as a major method of data collection (Yin, 2009). Approaches to interviewing for qualitative research range along a continuum from from the highly structured to the unstructured, according to the degree of control that the interviewer maintains over the interaction (Breakwell, Hammond, Fife-Schaw, & Smith, 2006) They are variously categorised by writers on research methods, as reviewed by Joungtrakul, Sheehan, and Aticomswan (2013).

It was planned to conduct interviews with a stratified sample (Pickard, 2007) of NHS staff within each Trust. The sample was to include one or more representatives of each of the following seven key professional groups who were known to hold roles relating to access to published professional information, and whose perspectives were therefore considered relevant to the study: participant

category 1) information governance, information technology, library and information services, training and development, human resources, communications; and participant category 2) education or professional development specialists from the medical, nursing, allied health, and pharmacy professions. (“Allied health” in the context of the NHS in England includes the following professions: art, drama and music therapists (arts therapists); chiropodists/podiatrists; dietitians; occupational therapists; orthoptists; physiotherapists; prosthetists and orthotists; radiographers, both diagnostic and therapeutic; and speech and language therapists (Health and Social Care Information Centre, 2016).

The study used semi-structured interviews as its main data collection method. Semi-structured interviews appeared to be the best means available within this context of obtaining the required detailed information from participants, while also providing an in-depth initial understanding of staff experiences, assumptions, values, attitudes and perceptions, perceived priorities, and rationales; that is, of addressing the “what?”, “how?” and “why?” questions of the study, while ensuring a degree of focus and specificity within the interviews and comparability of responses between members of the same group across the three sites (Patton, 1990, cited by Joungrakul, Sheehan, & Aticomswan, 2013).

One approach to semi-structured interviewing is to use an interview guide, which specifies the questions and topics and themes that must be covered and the way in which they should be approached with each interviewee, in a manner which allows flexibility and fluidity in the conduct of the interview, including the topics covered, the sequence of questions and the manner in which they are asked (Mason, 2003). The researcher considered that, under the circumstances of the study, a single guide covering all groups, or a collection of index cards, would necessarily have been highly complex in nature, containing numerous branch points and alternatives, and thus unwieldy and very difficult for her to use within the interview situation. For the sake of simplicity and practicality, she therefore developed a series of interview guides customised for each of the main staff groups. These included formulated questions that were specific to, and appropriate for, each group, but based on a common set of themes and sub-themes, as shown below in Table 3.3. These focused on strategies, policies, implementations of policies, technical issues, culture, attitudes and individual experiences related to online information behaviour, e-learning and use of social media. A customised interview guide was also developed for the NICE manager NICE-01. The basis for the development of these guides, the content of the questions, and the manner in which the first interview guide was piloted, are described in more detail in Sections 3.5.2 and 3.5.3 below.

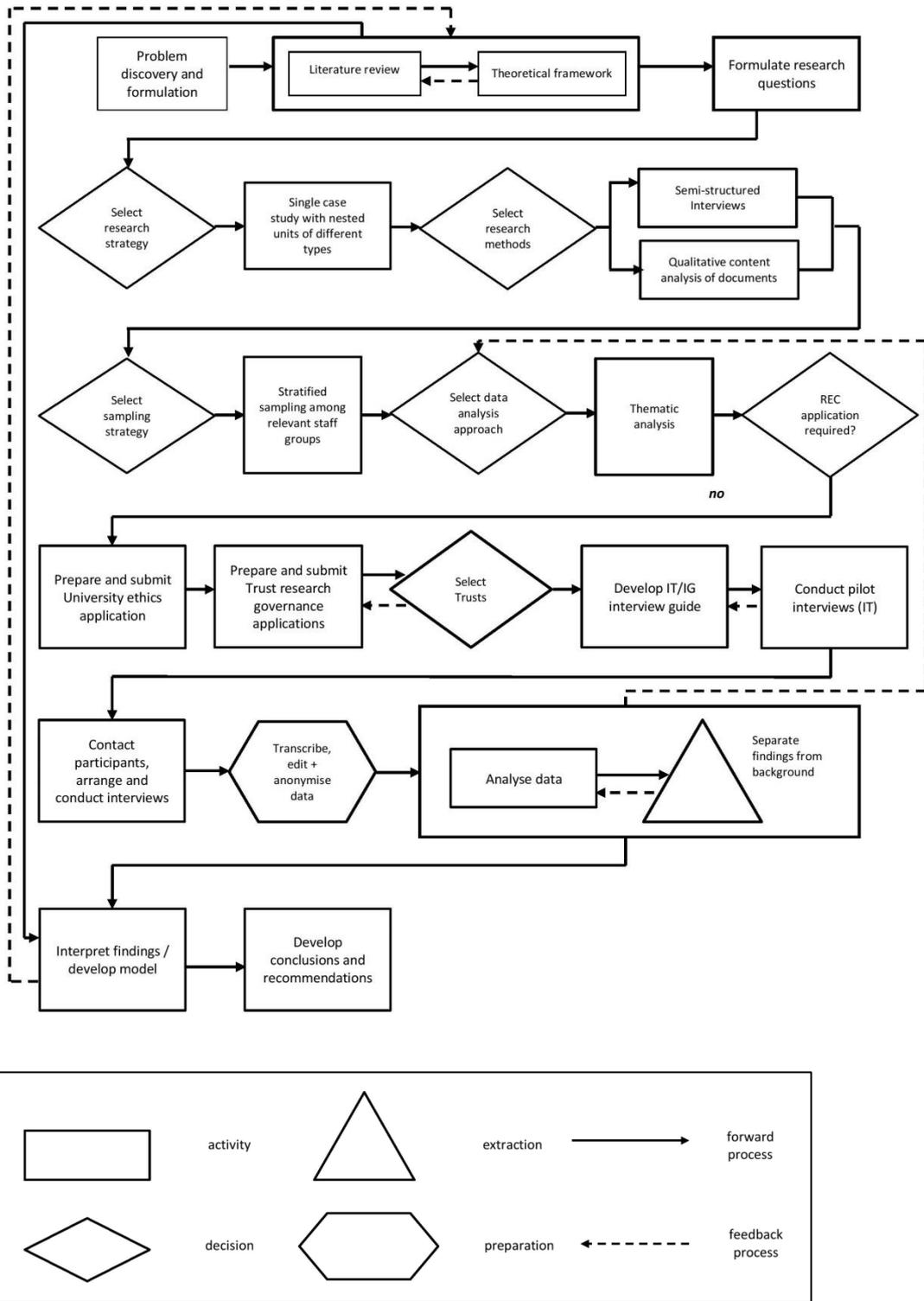


Figure 3.2 Research process flowchart with key to symbols

3.5.2 Interview questions

Patton (1990, cited by Joungtrakul et al., 2013) classified the possible types of interview question as follows (Table 3.2):

1	Experience / behaviour	Focus: what a person does or has done Aim: eliciting descriptions of experiences, behaviours, actions and activities that are in principle observable
2	Opinion / values	Aim: understanding a person's cognitive and interpretive processes Elicit: opinions, objectives, intentions, wishes, values
3	Feeling	Aim: understanding a person's emotional responses to experiences and thoughts
4	Knowledge	Aim: finding out what factual information the person has
5	Sensory	Aim: finding out what is seen, heard, touched, tasted or smelt
6	Background	Focus: the demographic characteristics of the person being interviewed

Table 3.2 Types of interview questions

The primary aim with participants in category 1) above (3.5.1) was to explore attitudes to and assumptions about information-seeking as part of professional work, and their understanding of their own roles and of organisational priorities in managing access to published information online, including e-learning material, within Trust networks (question type 2 in Table 3.2 above). The interviews with IT staff also provided the main means of obtaining relevant technical information about relevant aspects of the Trust's IT infrastructure, such as the detailed configurations of SWGs used, policies regarding PC hardware and software procurement and upgrading, and approaches to desktop management and browser security configurations (including virtualisation). The aim with members of category 2) was to gain their perspectives i) on possible problems with access to e-resources within the organisation, and on information technology staff practices and attitudes; ii) on organisational readiness, in terms of overall strategic commitment, and in particular of technical infrastructure and support, for e-learning (question types 1, 2 and 3).

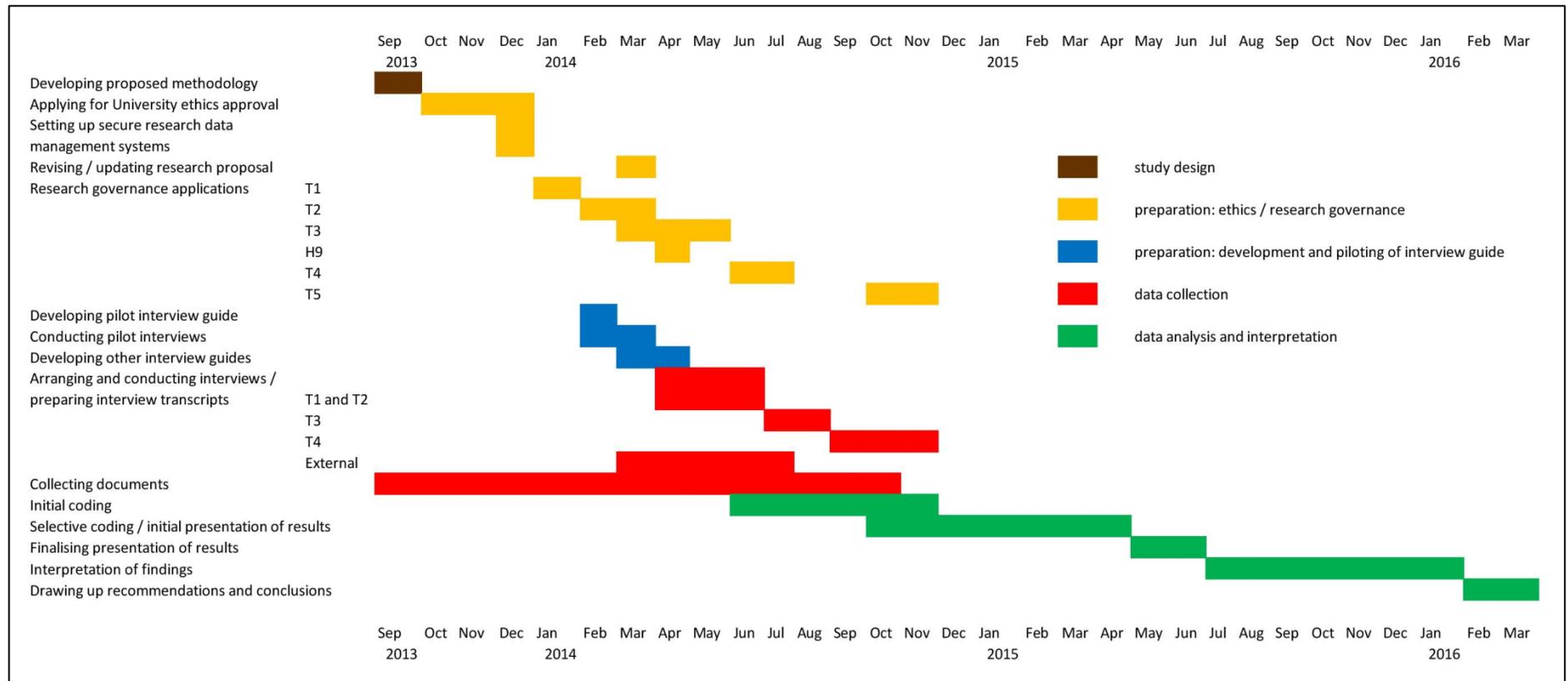


Figure 3.3 Research process Gantt chart

The seven groups of staff interviewed held widely differing roles and responsibilities with respect to systems and policies which bore on access to online learning resources and published material; these could be categorised as follows (Table 3.3):

Policy formulation	IT, information governance, communications, clinical
Policy implementation	IT, information governance, HR, T&D
System procurement and configuration	IT (SWG, DLP, spam filter), T&D (LMS), LIS (library system), NICE (link resolver, OpenAthens, core content)
System administration / intermediary	IT; HR (ESR); LIS (link resolver, OpenAthens, library system), T&D (LMS)
E-content creation	T&D, clinical, communications, LIS
Staff training provision	T&D, IT, LIS
End-user	All

Table 3.3 Differing roles of staff groups in relation to access to online published information

This required the issues of the research to be explored in differing ways with each of the groups, within the framework of the common themes (Table 3.4), leading the researcher to formulate specific questions which reflected their different organisational positions and responsibilities (Table 3.3).

The interview questions included all categories in Table 3.3 other than (5). In most cases questions did not arise directly from the literature as such, but from the researcher's prior knowledge and experience, informed by the literature) but the literature served to inform the ensuing discussion of the question with the participants, e.g. regarding the blocking of websites (2.7.3.4), and social media policy and organisational risk (2.8.4, 2.8.5) and the analysis and interpretation of the data. However, the following directly influenced the development of questions aimed at exploring security and governance issues with IT and information governance staff: Prince *et al.*'s (2010) framing of information access problems in terms of inappropriate risk management (2.7.3.4.2); and discussions of the information security and cybersecurity risks presented by users (2.7.2.1, 2.7.2.4.2), in particular the well-known quotation from Schneier (2000), "people are the weakest link".

IT services	Strategic priorities and procurement Quality of IT support and provision / Attitudes of IT staff towards end-users SWG implementation and administration Staff experiences of infrastructure-related problems, including availability and functionality Cultural attitudes to IT
Information governance and security	Security policies and practices – implementation and effects Sources of professional information and guidance re: cybersecurity / information security Information governance incidents and their impact Web / social media 2.0 policies and their implementation Attitudes to Web 2.0 / SoMe
Barriers to information seeking, use and sharing	Levels / quality of provision of LIS Other information systems and sources Problems encountered with provision of LIS services General problems encountered with access, use and sharing of online published information Attitudes to EBP and to information seeking, use and sharing Effects of barriers on information seeking, use and sharing
E-learning	Extent corporate, professional and academic e-learning use Platforms for e-learning Cultural aspects of e-learning Staff support for e-learning IT support for e-learning Problems with managing e-learning Problems with existing e-learning infrastructures
Web 2.0 / SoMe	Web 2.0 / social media policies and their implementation Attitudes towards social media Extent and nature of use of SoMe / Web 2.0, individual and corporate, in relation to communications strategies
Mobile devices	Use of mobile devices (own or Trust) for information purposes, including e-learning Cultural aspects of mobile device use Provision of Trust devices Level of support for use of own devices / provision of support

Table 3.4 Interview themes and sub-themes

3.5.3 Interviews: piloting

It is commonly recommended for semi-structured interviewing that the interview guide or protocol be piloted, the aim being to ascertain how well it will work as a research instrument within the main study. Pilot interviews using the guide may highlight ambiguities and difficult and unnecessary questions, may identify gaps in the coverage of the interview questions in relation to the research

questions, and may determine whether each question elicits an adequate response, They also provide the researcher with an opportunity to practise and improve interviewing techniques (Dikko, 2016; Turner, 2010; van Teijlingen & Hundley, 2001).

Initially, an IT-focused interview guide was prepared, and checked by supervisors. Two pilot interviews were then conducted using it to test its effectiveness and suitability (Arthur, Mitchell, Lewis, & McNaughton Nicholls, 2014); one was with a retired IT manager (P1), the other was the IT manager of a specialist acute trust (P2). IT managers were chosen for the pilot interviews, as IT managers in the Trusts were perceived by the researcher to be the most “critical” category of participant. Following these pilot interviews, changes were made as a result to the phrasing of some of the questions and their overall grouping and order; some questions were omitted as redundant, or combined with others. Further (very minor) changes were made as the study progressed; copies of all versions were retained for reference. Because the changes made to this interview guide were deemed to be relatively minor, it was decided to include the data from these pilot interviews, some of which were very valuable and informative, in the overall analysis.

3.5.4 Interviewee sampling and recruitment

Morse (1994, p. 228, cited by Andrade, 2009) defined the good interview participant as the “one who has the knowledge and experience the researcher requires, has the ability to reflect, is articulate, has the time to be interviewed, and is willing to participate in the study”. The precision and rigour of a qualitative research sample is assessed by “its ability to represent salient characteristics which enable detailed exploration of the central themes and questions which the researcher wishes to study” (Ritchie, Lewis, Elam, Tennant, & Rahim, 2014, p. 113).

In Trusts T1 and T3, potential representatives of the key staff groups specified in Section 3.3 above were identified initially via recommendations or suggestions from a senior librarian; in some cases the librarian actually contacted such potentially suitable participants on the researcher’s behalf and ascertained provisionally their agreement to participate. (The librarians’ offers to contact potential participants on the researcher’s behalf in their respective Trusts were accepted on account of the difficulties anticipated or experienced in recruiting participants; the researcher felt that potential participants would be more likely to accede to a request to participate in the research project if mediated via a Trust manager.) The research office at T1 was not able to assist the researcher in identifying potential participants. In T3, two participants within community nursing services were initially identified and contacted by the research manager at the researcher’s request; he also contacted a clinical psychologist, who was unwilling to participate. In Trust T4, the research manager

insisted that potential participants be selected by a junior member of the R&D support staff. In all three Trusts, efforts were made by the researcher herself also to identify potential participants via the respective intranets or websites. In T1, however, this was unsuccessful, as the staff information on the T1 intranet (to which she had been given access via the library staff) was not up to date.

The potential for bias in referring along a line of contacts who may give similar information is acknowledged (Erickson, 1979); however, the use of insider contacts and knowledge was needed here to supplement the researcher's initial selection of potential participants, as otherwise it would have been difficult for her to determine among the individuals listed within the available information sources the most appropriate people to interview (Bryman, 2012; Noy, 2008). It was appropriate particularly with IT staff, since, as Botta and his fellow researchers have indicated (Botta, Werlinger, Beznosov, et al., 2007; Botta, Werlinger, Gagné, et al., 2007), not only can they be difficult to recruit, as was the researcher's experience in T1, but also roles within information security can be widely distributed among staff members in a manner that cannot be readily ascertained other than via referrals or recommendations. According to Streeton, Cooke, and Campbell (2004, p. 38), "... this weakness [of depending on referrals] may be balanced by the benefits of providing contacts in otherwise researcher-inaccessible areas. Insider knowledge gained through this type of contact is of particular use in finding the best person to approach in an organisation, irrespective of their job title".

The initial contacts via the librarians in some instances meant that recruitment processes were not fully standardised. It could possibly have led participants to frame their understanding of the research topic primarily in terms of information services managed by the library, which was not the researcher's intention. In terms of identifying suitable potential participants, librarians may have been more likely to approach staff who were in regular contact with library services; however, the clinical participants sought were already likely to have been in regular contact by nature of their staff development responsibilities, and members of non-clinical staff groups via their specific work roles. Also, the highly stratified nature of the sample sought meant that the pool of potential participants available to the librarians was, in any case, limited. Ten participants in all were recruited through referrals from intermediaries: three in T1 (two via the librarian T1-01, another via the HR manager T1-03), six in T3 (all via the librarian T3-01), and two (one, T4-07, via the librarian T4-6, and the other T4-19, via the nurse educator T4-05) in T4.

Individuals identified initially were contacted by the researcher via email or letter with information about the study and an invitation to take part. In some instances, where participants asked for

specific information regarding the scope and nature of the questions, the relevant version of the interview guide was provided to participants in advance.

It was apparent from the literature review, from one of the pilot interviews, and from initial contacts with potential research participants that problems of access to online published information are a “site of silence”, that is, they are known about, but not paid attention to or discussed (Clarke, 2003; Sen & Spring, 2013). Some prospective and actual research participants (e.g T2-02) seemed to have difficulty understanding the nature of the enquiry. Several published studies (e.g., Hughes, Joshi, Lemonde, & Wareham, 2009) referred only briefly to technology- or policy-related barriers to information seeking and use, and did not attempt to describe or analyse them in any detail. To address the difficulty that participants might have in recalling, conceptualising or paying attention to the phenomena of interest, and to focus their reflections on them in advance of the interview, those who agreed to participate were sent two brief research reports: Prince, Cass, & Klaber (2010) and Technical Design Authority Group (2009), referred to subsequently as the “TDAG survey”. It was felt by the researcher that the TDAG survey could provide a useful checklist of information access problems; also that provision of this material could serve as a “trigger”, engaging the attention and interest of participants, and stimulating their recall and reflection in relation to their own circumstances, far more effectively than could her initial email invitation and information sheet alone. Trigger material is commonly used in problem-based learning as a means of engaging students (e.g. Murray & Savin-Baden, 2000). The perceived advantages of providing participants with this material were felt at the time to outweigh substantially the possible risk that the conclusions of Prince *et al.* (2010), in particular, might unduly influence their views. The TDAG survey report, being just a summary statistical report without comments or conclusions, was not thought to present a risk. However, it could be argued that this strategy could have been avoided; other approaches to addressing the perceived site of silence, such as developing possible probes within the interview guides to follow up on questions in more detail, or providing participants with a simple checklist to prompt recall of barrier phenomena, could have been adopted instead (*cf.* den Outer, Handley, & Price, 2012).

For clinical staff, LIS staff and T&D staff, the TDAG survey was used as a checklist. The interview guide for clinical staff included an invitation to comment on both articles, although this was intended as a subsidiary question, and frequently not pursued.

Only one participant (T4-10) offered any comment specifically on their content. The Trust-based participants' comments relating to information access problems, as described within the results

chapters, were all detailed and specific, avoiding generalisations. They also varied widely according to individual circumstances, and by Trust. Contrary to Prince *et al.*'s claims of robustness of infrastructure, they indicated a variety of IT infrastructure problems in addition to policy issues. Since the terms of the latter's analysis and conclusions (relating to risk management policy and platforms for delivery of e-resources) did not appear to be reflected within the results, it is suggested that the overall impact of sending participants the two articles is likely to have been limited.

Interviews were sought and conducted with key informants in selected external organisations whose importance was apparent from background information or indicated by participants: the National Institute for Health and Care Excellence (NICE), the local medical school, and a secure web gateway (SWG) vendor with a sizeable NHS market share. This particular SWG (identified within the results as SWG3) was in use within both T3 and the specialist acute trust where one of the pilot interviewees, P2, worked. To provide a broader perspective on issues in the NHS in England as a whole, it had originally been planned to conduct semi-structured interviews also with publishers of e-resources. In the event, however, all the researcher's attempts to contact publishers proved fruitless. The researcher's attempts to recruit a participant at the outsourced IT provider S3 were also unsuccessful.

3.5.5 Interviewing style and approach

The process of qualitative interviewing requires the researcher to be active and reflexive (Mason, 2002); Guba and Lincoln (1994, cited by Andrade, 2009) describe the researcher role as that of becoming a "passionate participant" through close interaction with interview participants. Roulston (2010) proposed a typology of conceptions of qualitative interviewing: *romantic*, *neopositivist* and *localist*. The "romantic" conception is described as follows: the interviewer endeavours to establish rapport with the participant and to establish a trusting relationship with them; is friendly, open, honest and forthcoming with participants; and may express their own interest in and involvement with the research topic. Multiple interviews may be used with particular participants as a means of establishing ongoing relationships. The interview itself is interactive and conversational in tone. The "neopositivist" approach emphasises the the adoption of a neutral role by the interviewer, who takes care to minimise possible biases via the formulation of effective, open, non-leading questions and by avoiding expressing opinions relating to the research issues. It tends to assume that "the interview conversation is a pipeline for transmitting knowledge" (Holstein & Gubrium (1997), cited by Alvesson (2003, p. 15). The "localist" approach, which shares certain features with postmodernism, but is also

associated with research approaches such as conversational analysis and discourse analysis, emphasises that interview statements must be seen in their social context; participants are not reporting external events, but producing situated accounts.

The researcher's own approach to interviewing lay somewhere between the "romantic" and the "neopositivist"; While closely focusing on eliciting information and knowledge, she adopted a conversational manner, seeking to generate rapport and trust with participants as a means to elicit rich data of high quality. Particularly with the IT managers, where shortage of time was a particular factor, not all questions in the interview guide could necessarily be pursued. For the interviews with IT managers in T1 and T3, which took place relatively late during data collection at the respective sites, she compiled and brought to the interview detailed lists of technical issues that had arisen in the course of earlier interviews in the respective Trusts about which she was seeking clarification. She did not conduct multiple interviews with participants. In some instances, notably with T1-01 and T4-20, missing information or clarification of ambiguities was sought from participants by email subsequent to the interview.

3.5.6 Conduct of interviews

The researcher compiled a checklist of essential items for the researcher to bring to interviews (site map where applicable, participant's telephone number and email in case of unexpected delays, recording devices, instructions for backup recording device, copies of the interview information sheet and consent form (Appendix E.3), copy of interview guide (Appendix F), research notebook, copies of articles sent to the participant for pre-reading). She used another brief checklist as a prompt to carry out standard tasks at the start of the interview (obtain consent, start recording devices, etc.) Interviews were conducted in the participant's office or in other suitable quiet locations which they had arranged in advance. Following the interview, an email was sent to each participant to thank them for their input and their time.

3.5.7 Recording and transcription of interviews

Face-to-face interviews were recorded using two password-protected portable devices concurrently, one as a backup.⁴⁹ As soon as possible thereafter they were downloaded to the researcher's

⁴⁹ This approach worked well other than for the interview with T4-05, for which the main recording device was afterwards found not to have been switched on and the recording from the backup device was found to be

(password protected and encrypted) home desktop hard drive and university file server. Kowal and O'Connell (2014) argue that all transcription is in principle selective, therefore that the choice of transcription method needs be appropriate to the specific purposes of a given research project. The researcher transcribed the pilot interviews and the initial three interviews at Trust T1 herself, but, finding this excessively time-consuming, subsequently used a transcription service recommended by one of her supervisors. This transcriber was familiar with the NHS via her work as a medical secretary, and produced work of good quality that required very few corrections, following an "intelligent *verbatim*" approach. In intelligent *verbatim*, the transcriber chooses which pauses and detail are relevant, but is careful to make sure that the exact wording of the dialogue is recorded, while omitting verbal fillers. This approach, which identifies the verbal content of the interviews, is the one generally used for qualitative research other than discourse analysis, and was therefore suitable for the study (Turner, 2010). Once received by the researcher, transcriptions were checked for accuracy and anonymised before being saved locally and remotely, and uploaded to NVivo for analysis. Interviewees were asked by email for clarification of unclear words or phrases where appropriate. A password-protected spreadsheet, which incorporated an anonymisation log, was used to track progress with arranging and conducting interviews and in processing interview recordings and transcripts (Burke, 2011). The anonymisation scheme adopted is described in Section 4.1 below.

The two (relatively brief and informal) telephone interviews were conducted using a recording application on the researcher's smartphone, and again downloaded as soon as possible thereafter to her home desktop hard drive and university file server. The two telephone interviews were not transcribed. Following the interview with the SWG product manager SWG3-01, the researcher discovered that a problem had occurred with her recording application, which had registered only the researcher's contributions to the dialogue and not the participant's. The interview with U3-Med-01 was relatively brief and informal, and accordingly was not deemed worthwhile to transcribe. For both telephone interviews the researcher's detailed contemporaneous notes were drawn upon instead for analysis purposes (*cf.* Halcomb & Davidson, 2006).

heavily affected by interference. The researcher herself attempted to transcribe this, getting as far only as 30% of the way through the audio file. Fortunately this covered the most critical content, the discussion of website blocking.

3.5.8 Documents

Documentary analysis offers a number of advantages as a research method. Within public sector organisations, such as the NHS, documents are generally widely available and easy to collect; the process of data collection is non-intrusive; they are readily compared across different organisations; they do not generally present issues of privacy, anonymity or confidentiality; and their preparation and content are not influenced by the research processes. The data they provide may usefully supplement, contextualise or clarify that obtained via other methods, e.g. interviewing (Shaw, Elston, & Abbott, 2004).

The following categories of documents were obtained for each Trust:

- Policy and guidance: communications and media, training and development, information security, information governance, Internet acceptable use policies, etc.
- Quality accounts
- Annual reports
- IT / Informatics department business strategy
- Library service, training department, communications strategies
- Professional strategies
- Website content
- Statements of values and behaviours
- Promotional material for SWGs (white papers, etc.)

Freedom of Information (FoI) requests placed via the “What Do They Know?” website⁵⁰ or directly to the Trust information governance department(s) were needed to obtain some of the policy and strategy material. Other material, however, was readily downloadable from Trust websites, or was provided by participants. The choice of the types of document to be included was determined by their roles and functions within NHS organisations in relation to access to published information. Comparable categories of documents were obtained for each Trust site. To provide contextual information, specific data relating to Trust activity and performance were obtained also from national NHS websites, as described in Section 4.1. Other documents, such as Health and Social Care Information Centre (HSCIC) Good Practice Guidelines, reports, and national policies in relevant areas

⁵⁰ WhatDoTheyKnow: <https://www.whatdotheyknow.com/>

(e.g. IT strategy, library and knowledge services, workforce development, e-learning, and mobile devices), were also obtained. It did not prove possible, as had been hoped, to obtain detailed technical documentation (as distinct from marketing material) for the different SWGs in use within the Trusts.

3.6 Data analysis

Framework analysis (Gale, Heath, Cameron, Rashid, & Redwood, 2013; Ritchie et al., 2014; Ritchie & Spencer, 1994; Spencer, Ritchie, Lewis, & Dillon, 2003; Spencer, Ritchie, O'Connor, Morrell, & Ormston, 2014) was initially preferred as an analytical method. It provides a clear "audit trail" from data to findings and conclusions, and can be carried out within a relatively tight time frame; it is an appropriate analysis approach for applied, policy-related work; and it was supported by the NVivo 10 qualitative data analysis (CAQDAS) software package, which the researcher was intending to use for her analysis.

In the event, the richness, heterogeneity and complexity of the data appeared to preclude its application; it appeared impossible to identify themes and sub-themes in advance in the manner it requires. Thematic analysis following the approach of Braun and Clarke (2006, 2013) was adopted instead as an analytical method. Braun and Clarke describe thematic analysis as a recursive process with six main phases: familiarisation with the data; coding; searching for themes; reviewing themes; defining and naming themes; and writing up. The researcher began initial coding of the material using NVivo during the latter phases of data collection, identifying, refining and linking the emerging themes via a process of classification and re-classification of codes at progressively more analytical / conceptual levels. In the course of data collection and analysis, the researcher wrote for herself a variety of memos in NVivo concerning possible questions, thoughts or issues arising within the research. Her analysis was informed by ongoing reading (Tuckett, 2015). To facilitate comparisons between the Trusts, and to gain a fuller initial picture, data from the three Trust sites and from the external participants were analysed together rather than separately.

Bazeley (2013, p. 191) suggests that "identifying themes ... falls somewhere in the process between coding and theory development". According to Green *et al.* (2007, p. 549), the generation of themes in thematic analysis "requires moving beyond a description of a range of categories; it involves shifting to an explanation or, even better, an interpretation of the issue under investigation ... specifically referring to the theoretical concepts relevant to the study". The researcher's initial open and axial coding of the data using NVivo had yielded 18 main categories, some of which contained a

higher number of sub-categories than was desirable, while others were more thinly populated (Boeije, 2010). After undertaking this process she was eventually able to identify several broad themes within the data. The problem then presented itself to her, however, of how to relate these and their associated categories to the detailed specific findings relating to barriers encountered by NHS staff in accessing information. As a strategy for doing this, she experimented, at her supervisors' suggestion, with a matrix format for presenting the results, as recommended by Miles, Huberman, and Saldaña (2014); she mapped the main themes identified via the thematic analysis (columns) against the main interview themes (rows). As a first stage, each cell of the matrix was populated with appropriate data from the coding scheme. During the later stages of this process, she added to the scheme a "background" row theme, to incorporate material relevant to the overall analysis which was not otherwise classifiable. This scheme appeared to work well as a basis for further analysing and structuring the data, and she used it as the basis for presenting the results in their eventual final form. Examples of the output of these processes are given in Appendix R. To provide a visual aid to the structure and sequence of the discussion of results, she drew detailed thematic maps (Figures 3.1, 5.1, 6.1, 7.1, 8.1, 9.1) for each major theme, as well as an "overview" map representing the findings as a whole (Figure 4.0).

Thematic analysis is an appropriate strategy for analysing documentary data, particularly as a method of providing background and context (Bowen, 2009; Coffey, 2014). Documentary analysis, combining processes of qualitative content analysis and thematic analysis (Bowen, 2009; Prior, 2003, 2010; Vaismoradi, Turunen, & Bondas, 2013) was selectively undertaken of the documents described in 3.5.8 above. The documents were analysed together with the interview data.

According to Bryman (2008, p. 551), "people who write documents are likely to have a particular point of view that they want to get across". The researcher attempted to bear in mind that documents, rather than straightforwardly representing organisational reality, constitute a distinct level of "reality" in their own right, possessing significance in terms of their intended readership and the purposes for which they were written (Atkinson & Coffey, 2010; Bryman, 2008; Prior, 2003, 2008). Documents may contain only a limited level of detail, and therefore offer a partial or superficial account of what they describe. Policy documents in particular may represent aspirations rather than realities (Shaw, Elston, & Abbott, 2004). They are also designed to address problems, and as containing (explicit or implicit) solutions to them, which require to be identified and analysed (Bacchi, 2009, cited by Hammond & McDermott, s.d.). Accordingly, she aimed to conduct the analysis of the semantic content at a latent, as well as at a manifest, level. The checklist for

acceptable use policies developed by Gallagher, McMenemy, and Poulter (2015) in assessing the AUPs of public library services was applied to the Trusts' AUPs as part of the process, as described in Section 8.2.

3.7 Interpretation and explanation of findings

Theoretical frameworks were not applied to the analysis of the data until after the presentation of the results had been finalised. A wide variety of possible theories within the fields of organisation studies and information systems were examined for possible “fit” and explanatory relevance, in a process of what has been described as analytical generalisation (Meyer, 2001, citing Eisenhardt, 1989). The discussion of the findings and development of the explanatory model (Section 11.1) was developed in tandem with an extensive revision of the literature review, which was extended beyond its initial scope (information behaviour, information security and cybersecurity, organisational culture, power within organisations) to cover perspectives on interprofessional conflicts and technological innovation; this material informed the content of Sections 11.4 and 11.5.

3.8 Specific quality issues

3.8.1 Introduction: quality and validity in qualitative research

Interpretive research approaches often adopt as its criteria of quality and validity *credibility, transferability, dependability, and confirmability*, together with *trustworthiness* (of reported observations and of interpretations – the extent to which the investigator’s constructions are empirically grounded in those of the study participants) - and *authenticity* (Lincoln et al., 2011; Patton, 2002). The measures described below (3.7.2) and in the account of the design and conduct of the study (3.3 - 3.5) aimed to fulfil these criteria.

3.8.2 Number of interviews conducted

Under ideal circumstances the researcher would have expected to cease conducting interviews with a particular group of participants once it was felt that data or theoretical saturation had been reached, i.e. that redundancy or replication of data was occurring, no new findings or insights were being generated, no new themes were being identified, and no issues were arising regarding a category of data (Francis et al., 2010; Glaser & Strauss, 1967; Guest, Bunce, & Johnson, 2006). It can, however, be difficult to establish the point at which data or theoretical saturation has been achieved, and there are few extant guidelines relating to this (Baker, Edwards, Adler, Becker, & Doucet, 2012). It can depend in practice on a number of factors, including the quality of the data,

the nature and complexity of the research topic, and the amount of useful information obtained from each participant (Morse, 2000). Pan and Tan (2011) suggested that 15 interviewees per organisation should be a minimum number to aim for, with the overall number of interviews not exceeding 50 (Ritchie et al., 2014). In the present study, the researcher carried out 45 interviews with a total of 48 participants (three of the interviews involved pairs of workforce development staff): 15 participants in T1 and T2, 15 in T3, 15 in T4, with three external participants; further details are given in Table 3.1. It should be noted that the number of NHS Trust staff working within a particular area was in some cases very small: within library and information services, for instance, none of the Trusts had more than five professional members of staff, while the training and workforce development departments generally had fewer than ten. In several instances, just one key individual within each professional group was identified as having educational or staff development responsibilities. Regarding the degree of data saturation achieved, it appeared to the researcher that a reasonably clear overall picture was emerging from T1/T2 and T3, whereas the size and complexity of T4 as a teaching and research institution inevitably meant that, while the main impacts of web security measures and social media policies (which were Trust-wide) were clear, a considerable amount of local detail may have been missed, particularly where information use by clinical researchers was concerned.

3.8.3 Audit trail

Audio files and written transcripts of interviews, successive versions of interview guides and copies of all email and hard copy correspondence with participants and research managers were retained. Research notebooks were kept, recording issues arising in interviews and other relevant matters. The anonymisation log and progress monitoring spreadsheet were mentioned above (Section 3.4.4). Queries run in NVivo on the contents of documents and interview transcripts were saved. Memos were written during the process of analysis, as detailed above (Section 3.5).

3.8.4 Member checking

It is considered desirable, for reasons both of research ethics (fairness to participants who have freely given their time and energy to participation in a study) and of accuracy, to incorporate some form of member checking of research findings (Pickard, 2007). Member checking may be defined as “the practice of taking research products back to those researched for review and evaluation” (Locke, 2008). The relational complexities and epistemological ambiguities of various different approaches to sharing study findings with participants were comprehensively discussed by Locke and Velamuri (2008). They stated that participant transcript review, while it allows participants the chance to amend or clarify information they had provided in the original interview, also has

potential disadvantages, such as a bias created by inconsistent data sources, or the loss of data when a participant decides to withdraw valuable material; also, the process is time-consuming. They observed only marginal gains in accuracy of data from the process.

Rather than sending each participant a copy of their interview transcript for review, a brief narrative synopsis of the findings was submitted to all participants for review and comment once the full report of the results had been completed. No disagreements or negative comments were expressed, although the librarian T3-01 asked for more detail regarding some of the reported findings which related to her own service.

3.8.5 Triangulation

The study used two qualitative methods, allowing only limited possibilities for methodological triangulation. However, data triangulation, i.e., detailed assessment and comparison of information between different groups of participants and individual participants within the same organisation, and comparison between documents and interview reports, was intrinsic to the research design; it was carried out as far as possible as part of the analysis (see Section 3.3 above). The wide divergences that appeared to be occurring in some instances between documentary sources, such as policy documents and reports, and *de facto* practices as described in interviews by participants, were important findings in themselves (e.g. regarding Web 2.0 and social media access in T1: 5.5, 9.2.1, and encryption of USB memory sticks in T4: 5.2.1).

3.8.6 Other quality issues and measures

A great deal of background information, as provided in Chapter 4 and elsewhere, was gathered in an effort to ensure that descriptions of the research participants and their organisational settings were sufficiently detailed to allow for transferability of findings, without indirectly identifying them or their organisations. Other quality issues have been discussed elsewhere within this chapter: adequacy and appropriateness of data (sampling issues, numbers of interviews collected, and data saturation), piloting of the interview guide, and transcription quality.

3.9 Position of the researcher

Given the emergent nature of knowledge within interpretive research, and the numerous ways in which a researcher's values can impinge upon the research process (Bryman, 2008), the researcher needed to be self-reflective on her own position in relation to the subject matter of the research and hence to demonstrate reflexivity (Steier, 1991). Her background knowledge of the research setting as a former LIS practitioner provided an important basis for the design and conduct of the study

(Reed & Procter, 1995); within these authors' typology, her position could be described as "hybrid". She acknowledged that her professional identity affected both her own perceptions and perceptions by interview participants of her (Bourke, 2014). With a professional background as an NHS library manager, she was aware of a strong commitment to evidence-based health care (Isetta, 2008) and information literacy development (Brettell & Urquhart, 2012), and, in terms of general professional values as a librarian, a commitment to freedom of inquiry, as a vital aspect of professional autonomy as well as a basic social and cultural right (Byrne, 2005; CILIP, 2005; IFLA & UNESCO, 2006).

She was also aware that the library and information profession is both female-dominated, while the information technology workforce, by contrast, is heavily male-dominated (Munn, 2011; Reid, Allen, Armstrong, & Riemenschneider, 2010), with a culture that may be hostile to women (Harvey, 1997; Kirk, 2009); both groups are heavily subject to negative stereotyping (Akbulut-Bailey & Motwani, 2011; Blackwelder, 1996; Green, 1994; Joshi & Schmidt, 2006; Lutz, 2005; Trauth & Quesenberry, 2006). She also bore in mind gender imbalances within many of the health professions (Zurn, Dal Poz, Stilwell, & Adams, 2004), suggesting the possibility that gender stereotyping could contribute to conflicts between information technology staff and groups of clinicians. More recently she had become aware of the political context of evidence-based practice (McLaughlin, 2001; Rycroft-Malone, 2006; 2005), and of the significance of information systems as an arena of conflict between organisational groups and subcultures, in particular between clinicians and managers within the NHS (Adams & Blandford, 2005b; Currie & Guah, 2007; Nord & Nord, 2007; Potter, 2007).

She recognised, in principle, a general need for information security practice to "balance the competing rights, interests and requirements of different stakeholders" (Broucek, Turner, & Zimmerli, 2010, p. 190) and believed that the maintenance of effective cybersecurity / information security and appropriate use of computing resources should be not solely a technical matter, but the concern and responsibility for all staff within an organisation, being closely aligned with business requirements and organisational values (Inglesant & Sasse, 2010, 2011). She acknowledged also, however, that her experiences with information governance and security in her former NHS library manager post, while providing extensive background knowledge and insight into the general issues of the research, had sometimes been negative, and had considerably influenced her thinking.

Previously to undertaking the study, the researcher had been employed for four years (between March 2008 and May 2012) as the library manager of a large mental health and learning disabilities Trust in the north east of England. It should be noted that this was not the mental health and community health services Trust T3 in the study. Forensic services (both mental health and learning

disabilities) were an important element of this Trust's overall provision, occupying more than half of one of the three main hospital sites. It also provided prison in-reach and forensic adolescent psychiatry services. This characteristic of its services could in itself have led to a strong emphasis on security.

Two very serious information governance incidents took place during the researcher's time in post. The first of these involved the distribution of pornographic images via email, some of them illegal, among staff and patients in the medium secure unit; the second involved a loss of patient records via portable media. In consequence of these incidents, as well as policy changes, a notable shift appeared to take place in the organisational climate in relation to information governance and security. Her experiences of its effects led to her proposal for undertaking the present research.

3.10 Ethics

The ethical issues of the study were those that are intrinsic to the practice of social research in general, which Savin-Baden and Major (2013) categorise as being concerned overall with 1) efficacy of design 2) excellent treatment of individuals 3) transparency of process, and 4) plausibility of products. They included those of what Guillemin and Gillam (2004) term "research in practice". The researcher has to the best of her ability and knowledge fulfilled her general duty to safeguard the interests of interview participants through adhering strictly to the legal principles of data protection and to other aspects of good research practice, including 1) the provision of clear information to participants in advance about the study and its risks and benefits; 2) fairly obtaining and recording informed consent using paper forms retained on file; 3) managing research data securely; 4) safeguarding the anonymity of the participating organisations and the anonymity and confidentiality of individual survey and interview participants, including eliminating as far as possible, through the use of generic role descriptions for participants (Section 4.1) and through substitutions of specific information occurring within quoted sections of transcribed interviews and documents, any risk of their being identified indirectly (Huws, 2004; Israel & Hay, 2006). She has also fulfilled the duty of reporting and disseminating the research findings in a manner consonant with intellectual property law, in particular by seeking the requisite copyright permissions before reproducing illustrations and tables (Huws, 2004). It was anticipated that the relative sensitivity of information security as a research topic might lead to difficulties in recruiting interview participants or in establishing effective relationships with them, or to restrictions being placed on the use of the information being made available to the researcher. However she did not appear to encounter any particular problems of this

sort, other than that she found it impossible to obtain any IT system documentation, either from vendors or from any of the Trusts (Kotulic & Clark, 2004).

NHS Research Ethics Committee approval via the Integrated Research Application System (IRAS: <https://www.myresearchproject.org.uk>) was not required for this research, since it did not involve patients in any way; this was established via the Health Research Authority decision tree (<http://www.hra-decisiontools.org.uk/ethics/>). However, local research governance approval needed to be negotiated for each participating Trust. The administrative processes varied considerably in complexity and required lead time. One minor complication encountered by the researcher was that the allied health professionals working within Trust T1 were at the time all employed by another acute Trust, T2; thereby requiring the researcher to obtain research governance approval at T2 as well as at T1 in order to interview three participants within this category.

Copies of the Information School Letter of Approval and Research Ethics Review Outcome, and the participant information sheet and consent form, are included in Appendix E. Copies of correspondence relating to research governance approval requests, and the research approval documents from the individual NHS Trust sites, which included a Research Passport for T3 and T4, are not included, on the grounds that, since the document layouts were potentially recognisable by anyone familiar with communications from the respective research offices, even in a “redacted” form, anonymity could thereby have been breached.⁵¹

3.11 How results are reported

3.11.1 Preliminaries

Within the report of this study, the individual Trusts are referred to as follows:

District general hospital Trust: T1

(District general hospital Trust employing AHPs in T1: T2 – see comments in Chapter 3)

Mental health Trust: T3

Teaching hospital Trust: T4

Other Trusts referred to are assigned numbers similarly.

⁵¹ These can be made available to the examiners for checking in confidence if required.

The community health services division of T3 is designated as T3-WPH. Individual hospital sites may be designated with two-letter suffixes to the Trust designation, e.g. T1-LH or T4-IN.

Universities are assigned numbers beginning with U, e.g. U11. Individual university departments may have faculty codes assigned to them, e.g. U3-Med is the medical school of university U3. NHS or NHS-related bodies have codes that begin with S, e.g. S3. The clinical systems in use within T3 are referred to as C1 (mental health) and C2 (community services), and the secure web gateways (web proxies) used in each of the Trusts T1, T3 and T4 are designated correspondingly as SWG1, SWG3 and SWG4. The particular publishers or aggregators referred to are assigned the codes Pub1, Pub2, Pub3, Pub4 and Pub5.

Key documents are also assigned reference codes:

T4 had separate policies governing Internet and email use and computer and network security. The former is designated as AU4Int; the latter as AU4Sec. Acceptable use policies of the other Trusts are numbered AU1 and AU3. Social media policies, or media policies addressing social media use, are similarly designated SoMe1, etc. The social media guide produced in T4 for researchers is designated as SoMe4-Res. Annual reports and quality accounts are designated AR1/14-15, QA3/13-14, etc., where the numerical range denotes the year covered by the document.

Participants have both short-form and long-form designations, as exemplified by the following:

Long-form designation: [job role], [Trust], [participant number]

e.g. Occupational therapist, T2, 1

Short-form designation: [Trust]-[participant-number]

e.g. T2-01

Extensive use is made of verbatim quotation from interview participants in the reporting of results (Corden & Sainsbury, 2006). The long form is used in the attribution of quotations. Where a participant is quoted several times in succession, only the final quotation carries the attribution. The short form acts as a form of subsequent reference to the participant and as the unique identifier for that participant within the text. The assigned generic job role descriptions are intended to be informative as to an individual's roles and responsibilities, but sufficiently general as to preclude any risk of their being identified indirectly. Where, as was the case in several instances, a job role or title applied to only one person within a Trust, a more general designation has been provided. In some

cases this may indicate a role more junior in character than the participant's actual one. In the first reference within the chapter to a particular participant, the person is described as follows: "the IT manager T1-12", "the records and governance manager T3-03", etc. Thereafter they are referred to simply as T1-12, T3-03, etc.

Participants' comments have been edited to remove hesitations, repetitions and verbal fillers ("sort of", "you know", "I mean", "kind of", "like"). In some instances the recording device skipped a few words, as indicated in the transcription; here a tentative reconstruction of the missing word or phrase has been made from the context, and indicated in non-italicised characters, e.g.:

"we can't ... [18.48 – skips] *use it sensibly*" reconstructed as:

"we can't ... trust staff to *use it sensibly*"

A table listing the participants for each Trust by category of role is given below (Table 3.5).

Comments made in emails from other Trust staff members or external correspondents are cited in a few instances. The Trust staff members are assigned codes in a similar manner to the interview participants; external correspondents are assigned codes beginning with E, e.g. E6.

3.11.2 Structure

Following a description of the organisational contexts and background within the case study Trusts in Chapter 4, the arrangement of the results in Chapters 5 to 9 broadly follows a matrix structure: the major themes emerging from the data are mapped (rows) against the key themes of the end-user interviews (columns). The themes of the rows, which constitute the subject matter of the chapters, are as follows: information access and barriers (5), professional education (6), organisational dynamics and professional norms (7); information governance and security (8) and communications policy (9). The column themes, which constitute the sub-sections within each major section, are: 1) IT infrastructure, 2) published information resources, 3) e-learning, 4) social media, and 5) mobile devices. The background material in Chapter 4 derived in some instances from interviews, as well as from documents and general fact-finding. A final results chapter (Chapter 10) presents a tabulation and summary of the key findings.

On account of the lack of content in some areas, and the need to accommodate specific content in others, it was not possible to establish a uniform numbering scheme across the results chapters.

Role	T1 (T2)		T3		T4	
librarian	1	T1-01	1	T3-01	2	T4-06 T4-07
IT manager	1	T1-11	1	T3-06	1	T4-20
IT staff member	-	-	1	T3-17	-	-
records/governance manager	1	T1-09	1	T3-03	1	T4-09
senior governance and risk manager	1	T1-12	-	-	-	-
communications officer	1	T1-03	1	T3-12	1	T4-03
clinical tutor (medical education)	1	T1-06	1	T3-02	-	-
medical education administrator	-		1	T3-21	1	T4-11
AHP clinical lead	(3)	(T2-01) (T2-02) (T2-03)	-	-	2	T4-08 T4-10
senior nurse manager	1	T1-07	-	-	-	-
clinical teacher (nursing, HCAs, AHPs)	1	T1-08	3	T3-07 T3-19 T3-20	2	T4-05 T4-12
non-clinical teacher	-		1	T3-04	-	
training / e-learning officer (e-learning specialist)	2	T1-05 T1-10	2	T3-05 T3-10	3	T4-01 T4-02 (T4-22)
pharmacist	1	T1-04	1	T3-18	1	T4-04
consultant (surgeon)	-		-		1	T4-21
human resources manager	1	T1-02	1	T3-09	-	-
Total	12 (3)	-	15	-	15	-

Table 3.5 Interview participants within Trusts by job category

Colour-coded thematic maps are provided. An overview map (Figure 5.1) illustrates the main themes and links between column areas across row themes. More detailed maps illustrate the background and organisational context (Figure 4.1), and the content of each of the row themes (Figures 5.2, 6.1, 7.1, 8.1, 9.1). Within the theme colour, sub-themes and sub-sub-themes are indicated with

successively lower levels of saturation. Direct thematic links are denoted with solid lines, indirect links with dashed lines. Where applicable within the overview map, the solid lines denoting row theme links are colour-coded using the same scheme.

Table 3.6 (below) lists other participants interviewed as part of the study:

Interview type		Code	Role
Face-to-face	Pilot interview	P1	Retired IT manager, teaching hospital Trust
Face-to-face	Pilot interview	P2	IT manager, specialist acute Trust
Telephone		U3-Med-01	E-learning lead
Face-to-face		NICE-01	Senior manager, NICE
Telephone		SWG3-01	Product manager, SWG3 vendor

Table 3.6 Non-Trust participants

The colours used in the thematic maps are as follows (Table 3.7):

Information governance	Khaki
IT infrastructure	Grey
Published information resources	Blue
E-learning	Crimson
Social media	Orange
Mobile devices	Purple

Table 3.7 Thematic map colour code

3.12 Summary

This chapter began by setting forth an account of methodological principles in general and of the main research paradigms (positivism, interpretivism, critical theory and critical realism) which are believed to have been relevant to the study. It put forward an argument for the use of a case study approach based upon a critical realist epistemology. It continued with accounts of the overall research approach, of the specific methods adopted, including the specific measures taken to ensure methodological rigour. It then set out how the background to the study and its results are presented within Chapters 4 to 10.

Chapter 4. Background and organisational context

It should be noted that this chapter covers both background information derived from Trust documents and material derived from interviews which could not readily be incorporated within the matrix structure of Chapters 5 to 9 (3.6).

4.1 General information about the Trusts

4.1.1 Introduction

T1 was categorised as a small acute and community services Trust and associate teaching hospital. T3 was comparable in size with other mental health Trusts within its NHS England area. *While T3's services included two low-secure forensic inpatient wards and a forensic community support service, forensic services were not a large element of the Trust's services overall.* It provided both community and residential learning disabilities services, including an inpatient treatment and assessment unit and respite care facilities. T4, by contrast, also an acute and community services Trust, was among the largest in the country in terms of staff size, though not in terms of numbers of beds. It was a major teaching and specialist centre, treating approximately one million patients each year across its hospitals. It had grown within the last two years through its takeover of a neighbouring acute Trust which had been in financial difficulties; the technical and organisational processes involved would not have been complete at the time of the study. Some general information about the Trusts is provided in Table 4.1; *figures given are for the financial year 2014-2015, and taken from annual reports, unless otherwise indicated.*

T1 was nearing completion with several major capital projects, including the building of new operating theatres and critical care facilities. The workload for the training department had hugely increased; in relation to the opening of one of the new facilities it had faced an enormous workload delivering face-to-face training for new staff, leading to the researcher's interview with the training officers being delayed for two months. No capital projects on a comparable scale were in train at T3, though re-provision of several services was planned. At T4, a large-scale Public Finance Initiative (PFI)-financed rebuild of several of its specialist hospitals had been completed within the previous five years, along with the provision of new education facilities.

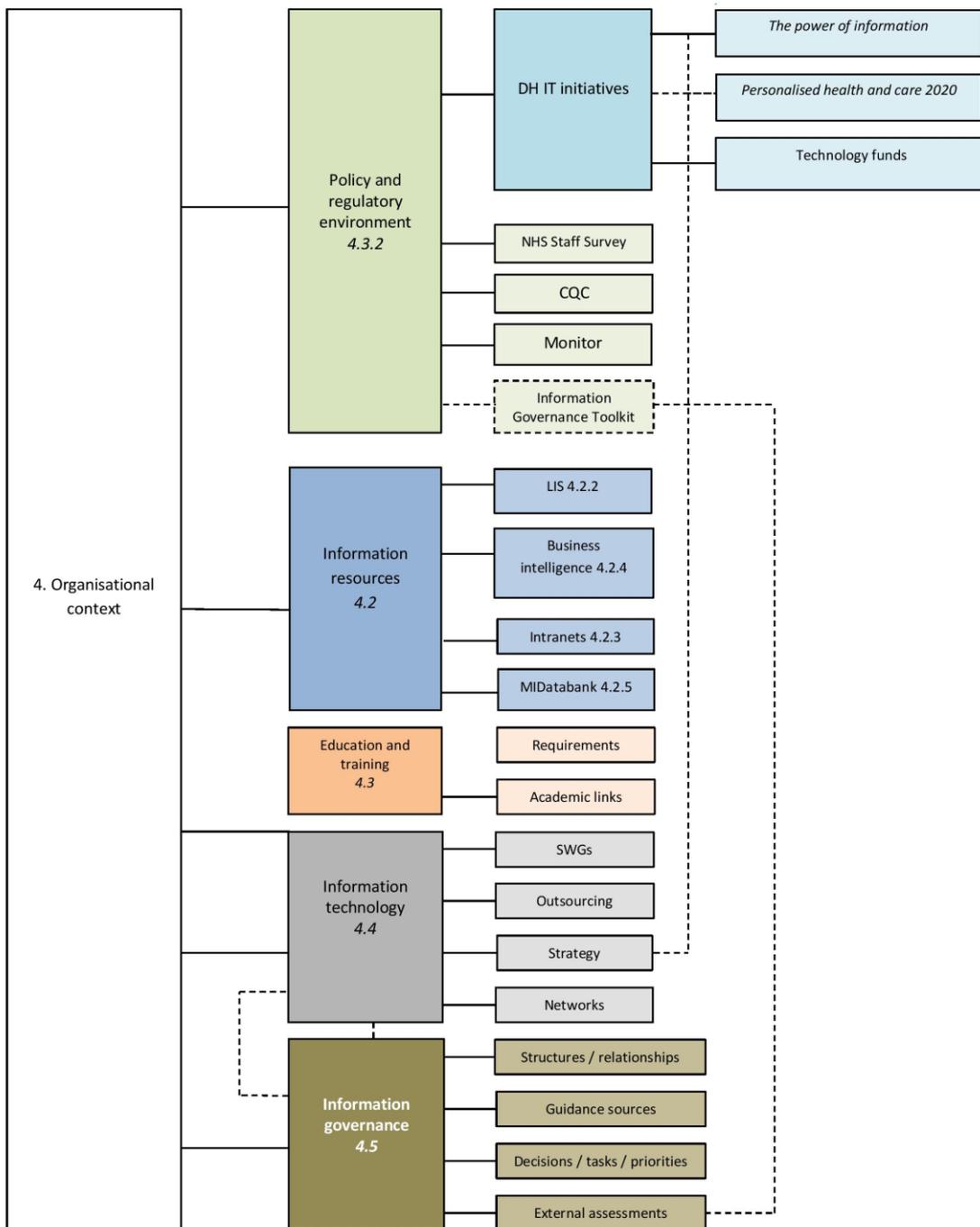


Figure 4.1: Background and organisational context

At the time of the study it was in process of building another general hospital to replace existing premises, and planning redevelopments of its A&E, outpatient and research facilities. It also planned to invest substantially in its IT infrastructure and systems. The reconfiguration of services following the takeover was not yet complete. Public consultations were taking place on a proposal for major restructuring of health services within T4's geographic area.

4.1.2 Policy and regulatory environment

4.1.2.1 National events and policy initiatives

Within the public domain, a range of information relating both to performance of the Trusts and to their strategic planning was readily available. The sources available included strategy documents, annual reports, quality accounts, national statistical reports, and ratings from regulatory bodies.

Organisational dynamics within the three Trusts reflected the influence and impacts of contemporary national events and policy initiatives. These include the publication of the second Francis report into failings of care at Mid-Staffordshire NHS Foundation Trust (Francis, 2013), subsequent reports on health care assistants and patient safety commissioned by the government of the day (Cavendish, 2013; Keogh, 2013; National Advisory Group on the Safety of Patients in England, 2013), and the policy responses thereto (Department of Health, 2013b, 2014).⁵²

The profound impact of the Francis and other reports was apparent in the strategic focus of the acute Trusts, as described in their annual reports and quality accounts, on organisational culture, core values and behaviours and staff engagement as a means of promoting quality of care and patient safety; on aspects of patient safety in general; on the reporting of incidents; on the training of nurses and health care assistants; on mortality rates; and on staffing levels (Davies & Mannion, 2013; Dromey, 2014; Steven, Magnusson, Smith, & Pearson, 2014). T1 had conducted public consultations on the findings of the Francis report and their implications for the Trust's services. T4 had undertaken an in-depth review and gap analysis of the reports, and developed an action plan to implement their recommendations. It had also made efforts to improve its level of staff engagement.

National events had also included publication of the report of the inquiry into abuse of patients at Winterbourne View Hospital (Department of Health, 2012e), bearing on the quality of care provided for patients with learning disabilities and challenging behaviour within health and social services, and hence relevant to T3's learning disabilities in-patient services (4.3.1). Recent national initiatives in information technology (Department of Health, 2012d; NHS England, 2013a; Wyatt, 2012) and dementia care (Department of Health, 2009a, 2012b, 2013a) are reflected also in these documents.

⁵² <http://www.engage.dh.gov.uk/francisresponse/>

	T1	T3	T4
Date established as FT	2008	2007	2009
Population served	300,000; small and medium town and rural	>1 million; mixed urban and rural	>500, 000; large urban; population of region for tertiary services
Sites	District general hospital, other hospital, intermediate care centre, community health services	>90 sites approx. including inpatient and community-based facilities; non-clinical services (IT, training suites) separately located	Six specialist and general hospitals providing secondary and nationally commissioned specialist services; community health services
Number of beds (third quarter 2014-15)⁵³	>550	>350	>1200
Clinical specialties	Acute, child health, maternity, intermediate care	Adult, children's and older persons' mental health; low secure in-patient forensic mental health; learning disabilities; substance misuse; community-based physical health	All acute specialties; dentistry; community health services; child and adolescent mental health
Number of staff	3500 approx.	>3300	>10,000
Income from patient services	>£170 million	>£150 million	>£1,000 million
Operating surplus / (deficit)	(£1.1 million)	>£1 million from normal operations	>£120 million

Table 4.1 Trust background information 2014-15⁵⁴

⁵³ Figures taken from KH03 NHS England Bed Occupancy Data: <https://www.england.nhs.uk/statistics/statistical-work-areas/bed-availability-and-occupancy/bed-data-overnight/> [accessed 23/01/2017]

⁵⁴ The information provided was derived from a variety of documents relating directly to the Trusts, including public websites

4.1.2.2 Organisational performance

Table 4.2 provides selected quality metrics relating to the Trusts' services. All the Trusts faced financial challenges resulting from national funding constraints on public spending and increasing demands on services. In respect of financial management, T1 was in deficit, while the other Trusts were in surplus. T1's deficit in terms of comprehensive income from patient care activities for the previous financial year (2013-14) had been much higher, at over £14 million. T1's financial problems, and its strategic priority of reducing management costs (AR1/13-14) are likely to have related to the observed low staffing levels in non-clinical services (communications, information governance, training, research support and human resources) (*cf.* the discussion in Section 11.4 below). Anecdotal evidence suggested that T1 for many years had experienced medical staff shortages, commonly attributed to its relative lack of prestige as an associate teaching hospital. T3's level of research activity was high in comparison with T1's; as indicated by its research department's levels of activity, including its proactive approach to supporting researchers and to publicising Trust-based research locally, T3 appeared to have a relatively strong research culture. As indicated by numbers of studies and patient recruitment, clinical research activity was declining at T1 and T3; at T4 it was increasing at T4 in terms of studies recruiting, though not in overall numbers of participants. There were indications within T4's communications strategy and annual reports of problems with organisational cohesion and staff engagement, with individual hospitals tending to function as discrete communities; a range of actions to improve staff engagement had been taken by the board following relatively poor NHS staff survey scores a few years previously. Staff engagement scores from the NHS Staff Surveys which did not differ greatly between the three Trusts, were all higher than the national mean for NHS organisations, and showed slight improvements from 2014 to 2015; to preserve anonymity, the figures are not given. There were indications in Trust documents that staff cohesion was perceived to be an issue at T4, and also that staff tended to identify with, and be loyal to, their individual hospital rather than to the Trust as a whole. A few years previous to the study, T4 had engaged a management consultant to improve its staff engagement scores, which at the time had been below the national mean.

External awards may be taken as an approximate indicator of organisational performance. Within the period 2013-15, T1 had also won a national award from a professional association for one of its high-profile clinical services. In terms of national awards, T3 appeared to be a high-performing organisation: it had won several for its people management and for its clinical and patient information services. One of its board members had also recently won a prestigious national award.

While a number of awards had been made to both clinical and non-clinical services at T4 during 2013-15, there were considerably more recipients of awards among individual clinical and research staff.

4.2 Information resources

4.2.1 Introduction

Participants were asked at interview about their use and experiences of their Trust's library services. Trust intranets, business intelligence systems and a medicines information system were mentioned by respondents as being important information resources for their work.

4.2.2 *Library services*

While the scope of health professionals' information behaviour is evidently not limited to resources provided or managed by NHS libraries, they provide an important resource to inform many areas of NHS work, both clinical and non-clinical. A description is therefore offered in this section of the three Trusts' library services by way of background. Other aspects of library services are discussed in Section 5.3 below. T1's library was managed by the Trust in a partnership with a local university, U2, and with T2. U2 provided funding for a member of staff and provided computer facilities and its own book stock, which was maintained separately from the Trust book stock. The library at T4 was based within a postgraduate centre on the Trust's main hospital site and was able to offer walk-in access for staff and visitors to the university e-resources, offering considerable advantages to the staff working there.

T3's library employed four professionals, including an outreach librarian shared with T2; it had been established in 2005 by the present library manager, who had built it up subsequently. It ran largely as a virtual service, although it held a small number of books at one of its sites, and provided local acute Trust libraries with psychiatry textbooks as a means of promoting psychiatry as a clinical specialty to medical students on rotation. (Psychiatry was a relatively unpopular clinical specialty, and there existed a national shortage of psychiatrists at all levels. One strategy commonly adopted by Trusts in addressing this was to promote psychiatry to undergraduate medical students by optimising their experiences of psychiatry rotations.) The library manager was peripatetic between sites, and fulfilled a clinical librarian role as well as a management one. She was assisted by a part-

time assistant librarian, a part-time library assistant, and a temporary clerical assistant. The Trust's knowledge manager was also officially part of the library team.⁵⁵

T4's library had two sites, one at each of the main acute hospitals. It was both well-staffed and very well stocked; five professionals were employed there. As well as providing services to staff of the Trust and students on placement, it provided some access within the terms of a local co-operation and access scheme to other NHS staff and students working or studying within its locality. The library manager was a member of a national working group on health library collections, and was a recognised expert in this area. The OpenAthens administrator for the area Local Education and Training Board (LETB) was employed by the library.

All libraries necessarily used the link resolver and EduServ OpenAthens authentication system procured centrally for NHS libraries in England by NICE to provide an authentication service for nationally- and locally purchased electronic content (see Section 1.4.5 above). The Health Databases Advanced Search (HDAS) interface for e-resources (1.4.5) was used to varying degrees. Librarian respondents alluded to the known problems with the functionality of HDAS rather than discussing them in any detail. The library at T4 had procured the EBSCO Discovery Service,⁵⁶ which provided an alternative search interface to a library's holdings, and Elsevier's ClinicalKey service⁵⁷ which provided a point of care search engine as well as much valuable content. Access to the relevant aggregators' "native" interfaces was available via OpenAthens, although this was not mentioned by participants. Librarians did, however, identify several specific administration problems with OpenAthens (see Sections 1.4.5, above, and 5.3, below).

The nature of T4, as a teaching hospital and constituent organisation of a major research centre, provided many of the more senior clinical staff with access to information resources above and beyond those of the Trust library, such as those of the nearby universities.

⁵⁵ Staffing information relating to the libraries in the study was checked via the Health Library and Information Services Directory, <http://www.hlisd.org>

⁵⁶ EBSCO Discovery Service: <http://www.ebscohost.com/discovery/about>

⁵⁷ Elsevier ClinicalKey: (<http://www.elsevier.com/elsevier-products/clinicalkey>)

		T1	T3	T4
CQC overall rating ⁵⁸		(1/15) Good	(6/15) Good	(6/16) Good
Monitor rating		3 Green	4 Green	3 Green
Clinical research activity ⁵⁹	2013/14	>490 patients >45 studies recruiting	>875 30 studies approx. recruiting	>15000 (patients and volunteers) >300 studies recruiting
	2014/15	470 patients approx. >40 studies recruiting	>850 20 studies approx. recruiting	>10,000 (patients and volunteers) >310 studies recruiting
Information Governance Toolkit rating 2014-15 ⁶⁰		80% / 42 out of 45 satisfactory at level 2 or above / Red	94% / 44 out of 45 satisfactory at level 2 or above / Red	75% / all satisfactory at level 2 / Green
Information governance incidents 2014-15		Not reported in QA1/14-15	Two serious incidents at SIRI Level 2 – no regulatory action taken by ICO	212 (all types – none at SIRI level 2 or above) – 66 reported by staff

Table 4.2 Selected Trust performance measures for 2013-15

Some clinical researchers would in addition have had access to e-resources provided by the major medical charities funding their work, although this was not mentioned by any of the participants.

⁵⁸ See Chapter 1, Section 1.4.1

⁵⁹ Data taken from NIHR Research League Table: <http://www.nihr.ac.uk/research-and-impact/nhs-research-performance/league-tables/league-table-data.htm>
[accessed 26/01/2017]

⁶⁰ See Section 1.4.4

4.2.3 Intranets

All of the Trusts had intranets. Two of the Trusts were engaged in implementing new intranets. In both, the process was perceived by participants to be lacking in transparency and contested between departments. The content of T3's was managed by the communications department, with back-end support from the IT department. However, the Trust's knowledge manager was reported to be leading on implementing a new intranet using Hadron 8020, based on Microsoft SharePoint 2010.⁶¹ (The Hadron intranet implementation is discussed also in Section 6.2, particularly in relation to e-learning.) The Trust was already using SharePoint 2007 for its existing intranet. The strategic aim was to move to distributed authorship and management of intranet content, although there were perceived uncertainties as to how this should work in practice and what content was appropriate to be included:

"When we get the new SharePoint the execs. are very keen, or the exec. lead is very keen that actually we all own it, it is not just owned by Comms., who will dictate where everything goes and what you can and can't do ... whether that will happen I don't know, but she is very keen that -- at the moment, you know, they are deciding what we can all put there, and -- but actually they don't know, they don't know what is appropriate and what is not." (Medical education administrator, T3, 21)

The existing intranet was accessible to mental health staff but not to staff working within community health services on the outsourced network.

T1's existing intranet was described by the librarian T1-01 as "not particularly good". According to the senior governance and risk manager T1-12, it was managed by the Trust's IT services, with the communications officer being responsible for management of much of the content. The clinical teacher T1-08 reported that, although the search tools within the intranet were reasonably good, it could be difficult to find particular documents on it. The researcher had been given access to it herself by the library staff for the purposes of researching possible participants, and found that much of the contact information for services was out of date. The library had been involved in authoring content for and usability testing of the Trust website, and was running training sessions on use of the existing system for newly recruited Spanish nurses. The new system, which used the same

⁶¹ Hadron: <https://www.cloud2.co.uk/solutions/hadron/>.

content management system as the Trust website, was being implemented and managed by the IT department, with completion of the project expected by November 2015. T1-12 was keen on making the intranet as simple and straightforward as possible for clinicians to navigate:

“... We are trying to streamline ... getting all our policies and guidance and clinical pathways in one place, because at the moment, they are in different places on our ... intranet.”

“... It is IT understanding the language of clinicians and making it work ...”

(Senior governance and risk manager, T1, 12)

The library was anticipating having a *de facto* role in managing the content, although this was not mentioned specifically by T1-12:

“They haven’t rolled it out across the Trust, and we’re currently trying to – to support the IT department when they do it, that we’ll actually help add content to it and manage it on behalf of the departments, and ... I’ve done some work on metadata for leaflets before, as well. We’re not exactly embedded in the process, but we’re not off the radar, either ...”

(Librarian, T1, 1)

Access to the existing T1 intranet required a login to the Trust network, and was hence not available to student nurses other than via a staff member’s login (T1-01). However, the AHP clinical lead T4-08 reported that the intranet at T4 was available on the Trust library computers to students and visitors without any login being required. The pharmacist T4-04 described it as being “really good”. Available resources included the Trust library catalogue, which was not available via the web. The consultant surgeon T4-19 mentioned that they also included a comprehensive collection of resources for medical training.

4.2.4 Business intelligence services

The consultant surgeon T4-19 attached considerable importance, as an information source, to a central intelligence service integrating internal Trust clinical and corporate performance data. He found it of particular use in reviewing mortality and related clinical indicators. Nothing of this sort was mentioned by participants at T1. An FoI response from November 2014, however, indicated that the Trust used the QlikView business intelligence system.⁶² The medical education administrator T3-

⁶² <http://www.qlik.com>

19 reported that the implementation of a business intelligence infrastructure had been previously planned at T3, but was never fully implemented.

4.2.5 MiDatabank

A pharmacist at T3, T3-18, reported using MiDatabank heavily for drug information searches.⁶³ MiDatabank is a Windows application commonly used to record, manage, store and search enquiries. According to T3-18, it incorporated links to particular web search tools within it. He described it as a powerful tool on account of its cross-referencing capabilities. T3-18 was responsible for teaching other pharmacists how to record the results of queries.

4.3 Education and training

4.3.1 Education and training priorities

General requirements for NHS staff training are discussed in 1.4.2. Specific issues relating to education and training are reported in Chapter 6.

The senior nurse manager T1-07 emphasised the strategic importance of learning from adverse events as a priority for training activity within T1:

“... One of our big challenges, we know, is that we need to work hard to encourage our staff to learn from ... things that haven’t necessarily gone right here. So if something has gone wrong on one ward, how do we make sure that that same issue doesn’t happen again on the ward next door to it?”

She mentioned also that it was difficult to get staff away from the ward to undertake training, leading to an emphasis on ward-based training.

In T1, a critical report on the quality of care delivered to patients with dementia had led to the establishment of mandatory e-learning on dementia care for nurses. The report had found that staff felt that they did not have the appropriate training in understanding the needs of patients with dementia, and that senior staff were not always familiar with the most recent guidance on caring for

⁶³ <http://www.midatabank.com/About/SummaryofMiDatabank.aspx>

these patients. Some Trust initiatives to improve the quality of support provided to these patients were still at the planning stage or had started very recently.

“... There is also as much pressure on other types of training so ... and that tends to be, pushed through from clinical need, so dementia, so we know there is a huge increase in the numbers of patients with dementia, we know that we are getting -- 40% of our patients at any one time have probably got a form of dementia ... that is a huge number, we have got to make sure that our staff understand how to care for patients with dementia, so there are e-learning modules around for dementia ...”

(Senior nurse manager, T1, 7)

No similarly-driven training initiatives were reported at the other Trusts.

4.3.2 Academic and research links

Pre- and post-registration training for health professionals was delivered by higher education institutions as contracted by Health Education England and co-ordinated locally via its 13 LETBs (Davies, 2013; Health Education England, 2015a). All pre-registration students were supernumerary. Placements within a Trust, of varying lengths, were co-ordinated by practice education facilitators in consultation with the relevant university. In order to provide students with the required access to Trust systems and to educational resources, such placements required to be supported by Trust IT and library services (*cf.* Sections 2.4.5, 5.2.1, 5.2.2.3, 5.6, 6.2).

As reported by T1-08, a local university U2 had about 180 (T1-08) pre- and post-registration nursing and midwifery students at T1, where the main hospital site T1-LH was also a university site. One of the medical schools within the region, U3-Med, used T1-LH as one of its 18 associate teaching hospitals for undergraduate medical students' clinical rotations. According to the librarian T1-01, another university, U4, had diagnostic radiography and dietetics students on placement within T1; a radiography clinical tutor was in post. Pharmacy students from another local university, U6, undertook placements at T1-LH, and a member of the university teaching staff from U6's pharmacy department was partly based there. There were also considerable numbers of AHP students from a range of other universities. The AHP clinical lead T2-01 stated that the hope and expectation within T2 was that these students, once qualified, would consider applying for posts within the Trust, so placements were generally offered to students who lived locally. The number and length of AHP placements varied considerably by profession (T2-01).

U2 also had students from its mental health branch on placement within T3, and undergraduate medical students from U3-Med undertook their psychiatry rotations there. As reported by the clinical teacher T3-07, there were also small numbers of occupational therapy, physiotherapy, speech and language therapy and podiatry students on placement within T3. Unlike some other mental health Trusts, T3 had only a very few trainee clinical psychologists undertaking extended placements as part of professional doctorate programmes, and there were no Improving Access to Psychological Therapies (IAPT) trainee cognitive-behavioural therapy (CBT) practitioners based within it.

T4 had total responsibility for U3-Med medical students during the clinical years of their training. It also provided placements for large numbers of students from the other local universities U3, U9, and U15 studying nursing, midwifery, physiotherapy, occupational therapy, dietetics, and biomedical science. According to the AHP clinical lead T4-08, physiotherapy placements lasted for five weeks.

T4 was extensively involved in joint NHS and academic research structures. T2 was a member of the local Academic Health Science Network, and listed as such on its website (NHS England, s.d.) AR3/14-15 mentioned partnership working with an Academic Health Science Network, although it was not listed as a member on the website of the local one. T1 did not appear to be involved in any research partnerships of this nature.

4.4 Trust IT services

4.4.1 Strategic and operational priorities

The T4 informatics strategy was focused heavily on the replacement of “legacy” patient administration and other clinical systems, and on implementing an e-prescribing solution. The long-term aim was to develop and implement an EPR system that provided a single “clinical view” of the patient, bringing together information from multiple systems. The Trust had previously been committed to implementation of the Lorenzo suite of clinical and administrative systems as part of the National Programme for IT in the NHS (NPfIT), but the vendor had conspicuously failed to deliver, and T4 had left NPfIT shortly before the programme was dismantled nationally as a whole. Other priorities for T4 informatics were integration of systems following the incorporation in 2012 of a neighbouring acute hospital and its community services into the Trust, and further development of an already highly successful business intelligence service (*cf.* Section 4.2.3 above). According to the strategy document, an EPR in one division of the Trust was due to be piloted from April 2014. T3 and T4 did not have any plans to integrate access to point of care information resources within the EPR

workspace. T1-01 was hoping to integrate evidence summaries, however, within T1's proposed EPR system.

According to the IT manager T1-11, the (hugely detailed) T1 strategy had been developed in consultation with an external contractor, which had carried out a series of interviews with staff at various levels. T1-11 himself had provided technical input, but not been involved in developing the document. It also was strongly focused on implementing a full EPR system across the Trust as required by the local CCGs, which, according to T1-07, the Trust did not have at present. However, its haematology and medical imaging systems were fully electronic, e-prescribing had been partly implemented, an electronic handover system was in use within emergency care, and an EPR system had been implemented within one specialist service. A self-rating of T1's informatics services using the Informatics Capability Maturity Model (ICMM) (Health and Social Care Information Centre, s.d.) and National Infrastructure Maturity Model (NIMM)^{64 65} was referred to in its 2012 IT strategy; this had rated the Trust at Level 2 or Level 3 on all of its indicators for ICMM, and Level 3 for NIMM, with the intention of progressing to Level 4. The full results of these assessments were not publicly available. No mention was made of ICMM or NIMM in either of the other Trusts' IT strategies. Following a successful trial, T4 had been an early adopter of an electronic recording and alerting system for clinical observations (AR4/14-15). The mental health service of T3 already had an established EPR system, one commonly used within mental health and community services, designated here as C1. Its community services used a well-established primary care system, designated here as C2, managed by the outsourced IT services provider S3. T3 and T4 had both successfully bid to the Nursing Technology Fund (NTF) (1.4.3) for mobile technology-based systems to support community-based staff at the point of care. T1 had not bid in the first round of the NTF, but T1-07 reported that it planned to bid in the second round for mobile devices with which to record clinical observations, which could then be uploaded to the EPR system. When the results were announced, however, T1 was not listed among the successful bidders.

The IT manager T3-06 cited the senior management team meetings of the Trust's locality services, to which he was regularly invited, and the meetings of the user groups for key applications such as C1 and C2, as the main conduits of input into the Trust's IT strategy. Otherwise, he said he was made

⁶⁴ ICMM: <http://content.digital.nhs.uk/article/4931/Informatics-Capability-Maturity-Model-ICMM>

⁶⁵ NIMM: <https://digital.nhs.uk/NHS-infrastructure-maturity-model>

aware of other issues via the IT helpdesk. T3-06 had plans to replace the outsourced T3-WPH network with an in-house solution, which he believed would yield improved performance at lower cost.

The need to upgrade PCs from Windows XP before the end date for extended support in April 2015 presented an operational priority for all the Trusts. Microsoft support for Windows XP had ceased in April 2014; however, an additional support package, including security updates, for Windows XP had been purchased for the entire UK public sector for a further year (Gibbs, 2014).

At T1, 50% of the PCs were still running Windows XP (T1-11). The IT managers at T3 and T4 both reported that they were migrating to Windows 7 at a rate of about 80 machines per week, aiming to have completed the process before the end date for extended support in April 2015.

According to an email from the library manager T2-04, T2 was still using Windows XP, but a modernisation programme was planned involving upgrading all PCs from Windows XP to Windows 7. At T3, a programme of upgrading users' PCs had been undertaken, but a degree of rationalisation, to one user per device, would have been required to achieve this target (T3-06). Large numbers of the PCs at T4 were due for replacement, and T4-20 was not sure whether the funding for this was going to come from any source other than from departmental budgets; *cf.* the discussion of IT hardware procurement in Section 5.2. No plans for the migration to Windows 7 had been publicised (T4-09, T4-10). The lack of funding for migration from Windows XP presented the possibility that the project could not be completed on time for the scheduled end of UK public sector support in April 2015, thereby presenting a serious potential security risk (Worth & Neal, 2015).

The T1 IT manager (T1-11) reported that about 80% of the Trust's computers (n=1800) were running Office 2010, with the remainder running Office 2003, for which support was also due to cease in April 2015. All of T2 was mostly using Office 2007, but some staff had Office 2010 (T2-04). The older versions of Microsoft Office in use at T1 and T2 were reported by several participants as causing format incompatibility problems.

At T2 the planned modernisation programme was to include updating to Office 2010 (T2-04). T1-08 expressed the view that many of the problems that she and her colleagues had encountered while hot desking within the Trust were related to file format incompatibility issues.

A mixture of different versions of Microsoft Office was also reported to be in use at T4, but the participant who mentioned this (T4-04) said that she was not aware of any problems of this nature.

Other areas of background information relating to the Trusts' IT services are discussed elsewhere within the results chapters. Local procurement of hardware and software is covered briefly in Section 6.2, and in more detail in Section 7.2.2. User support is discussed in Section 7.2.3.

4.4.2 Outsourcing

Outsourcing arrangements for IT security, which at the time were relatively common within NHS IT services (Sophos, 2016b), were highly relevant to accountability for and local control over the provision of IT services, bearing on the findings of Chapter 5 and Chapter 8 in particular. However, T1, T3 mental health services and T4 did not outsource any of their IT services; all were managed in-house. The IT service for the community health services division of T3, however (referred to hereafter as T3-WPH) was still outsourced to an external commissioning support unit (CSU), referred to as S3. This arrangement was a "leftover" from T3-WPH's previous location within a primary care Trust (see Section 1.4.1, above). IT services at the Trust (T2), which employed the allied health professionals in T1, were wholly outsourced to the same provider. S3 also provided the IT service for the local authority social services departments operating within the Trust area.

4.4.3 Internet connectivity and wireless networks

T1 and T3 used the standard shared N3 connection to the Internet via the N3 Internet gateway (British Telecommunications, 2012). T4, however, as was typical of teaching hospitals, connected to the Internet via a network link to its main partner university, U3, and the Joint Academic Network, JANET, providing a higher bandwidth connection. High bandwidth traffic (e.g. YouTube) and inappropriate traffic was restricted. Wireless networks were provided in all three Trusts. Those in T1 and T3 were reported to be of varying quality according to location. In addition to the main Trust network, T1 had a postgraduate centre network, to which undergraduate medical students connected when using their iPads. In T4, medical students connected to an eduroam network provided through the use of a direct connection between the Trust and U3 (Teague, 2014). T4 had also implemented a Bring Your Own Device (BYOD) network specifically set up for staff to connect to using their own mobile devices (T4-20). This provided facilities to access personal information management, but not "line of business", applications. At the time the study was being conducted, this was in process of being implemented across all Trust premises. Neither of the other Trusts had any current plans for BYOD implementation, although T1-11 stated that BYOD was being "looked at"

within the current financial year. He did not anticipate a large uptake, however, on account of the requirement to implement a MDM system on personal devices. An expensive retro-fit of eduroam Wi-Fi had been required following the redevelopment (see Sections 4.4.1, 6.5); according to T4-20, it was not available fully across the site. U3-Med implemented a MDM system on student iPads, enabling them to be remotely wiped if lost. According to T4-20, T4 did not implement a full MDM system on personal devices connecting to the BYOD network, but required that users set up a PIN code protection and remote wiping facility.

4.4.4 Secure web gateways

General features of secure web gateways (SWGs), a type of web proxy, are discussed in Section 2.7.3.4.1 of the literature review. The SWGs used at the three Trusts all used a combination of blacklisting and real-time content classification using proprietary “engines”.

The IT manager, P2, referred to his Trust’s use of a particular SWG, designated hereafter as SWG3, for which several case studies of NHS implementations were available on its website. One of these referred to the need for clinicians to access information which might be inappropriate for other users, and to significant problems, both for the IT department and for clinicians, caused by the over-blocking of legitimate health websites by the predecessor SWG. The vendor’s product manager, SWG3-01, with whom the researcher conducted a telephone interview, stated his opinion that over-blocking was a huge problem for the NHS, whereas, by contrast, in the primary and secondary education context, under-blocking of inappropriate material was the main concern. SWG4’s website also included case studies of NHS implementations. By contrast, no references to over-blocking were made in any of the documentation for SWG1 and SWG4, the focus of which seemed to be solely on preventing inappropriate web use. SWG3-01 made the observation also that not everything that is illegal or potentially illegal (Section 2.7.3.1 above) can or should be blocked; compare the discussion of the role of AUPs in Section 2.7.2). P2 was not aware of any instances of blocking of legitimate websites within his Trust.

The device implemented at T1 was one rated as a market leader by several different technology research companies; it is referred to hereafter as SWG1. The vendor was based mainly in the southern United States. Anecdotal evidence and informal web searching indicated that the company’s web, email and data loss preventions solutions were in fairly widespread use within the NHS. It afforded the ability to set time quotas for usage of particular applications, which T1’s IT department implemented to limit the usage of social media websites, cloud storage and other online

applications within the Trust network; it also offered “granular” controls on social networking availability (see Section 9.2.1). According to T1-12, all members of staff had the same level of web access; no policies specific to particular staff groups had been set up. The quotas were flexible in that users had the ability to request more than their quota for particular business purposes, with their usage subsequently being audited. T1 had accepted the default categorisations of web content available within SWG1 (T1-12). The SWG1 website offered a facility for analysing security threats posed by particular URLs or IP addresses and reporting incorrectly categorised websites, although this was not readily accessible via the company home page; it is unlikely that end-users within the Trust would have accessed it.

The T1 IT department did not appear to have publicised across the Trust this setting of time quotas for certain web applications. For the only participant who mentioned receiving a quota notification (the pharmacist T1-04), it had come as a total surprise:

“I tried to ... access YouTube and I got a message I never had before, that said I had a quota of 60 minutes. I don't know what that is over, and I could use 10 minutes for accessing this site or sites of this nature.” (Pharmacist, T1, 4).

One cannot but conjecture as to what extent the setting of time quotas had been discussed and agreed within the relevant integrated governance committees.

T3 used the same SWG as P2; it is referred to hereafter as SWG3. Its vendor had offices and a manufacturing presence both in the United States and in the United Kingdom, and was a leading player in the education market. SWG3, in a similar fashion to SWG1, afforded the ability to set time quotas on particular websites and read-only controls on social networking applications, although these facilities were not reported as having been implemented at T3. It also offered the facility to set bandwidth limitations by policy, which was used within T3 to limit the speed of YouTube downloads (T3-06) (see above, Table 1.5.2). It offered comprehensive reporting facilities, with an extensive range of reporting templates available. The IT manager T3-06 mentioned an aspiration to set up different access levels for different categories of user according to job role, using another facility available with SWG3, but had not implemented such a policy. SWG3 also offered a facility for delegated temporary unblocking of blocked content to selected users and managers, although use of this was not mentioned at T3.

T4 used a British-manufactured SWG, referred to here as SWG4. In the IT's department's evaluation exercises it had narrowly beaten SWG3 as the preferred choice of SWG on account of its load-balancing facilities, which at that time SWG3 had lacked (T4-20). T1 had formerly used SWG4; the IT manager T1-12 felt that SWG1 was "really good" compared to SWG4, which the Trust had used previously, and which, in his view, was "cheap and cheerful". SWG4 did not, according to the available documentation, provide fully granular controls of social media, although it did offer a "read-only" facility. (According to the release notes on the vendor's website, fully granular social media controls were not implemented until October 2014, when a new version was issued.) It afforded the facility to set up multiple access policies customised to the needs of specific groups of staff, although the T4 IT department was not making use of this. Filtering sensitivity levels were apparently set within T4 for the numerous categories of proscribed content as recommended by the supplier. The health services case study provided by the company made no reference to possible over-blocking, nor to the nature of clinical information needs, and focused solely on enhancing productivity and security through the enforcement of acceptable use policies. An educational reviewer of SWG4 had commented on an online forum that it did not in his opinion provide enough of the detailed features felt to be required to keep students safe without affecting their ability to use the Internet as a resource for learning (2012). All three SWGs offered the facility to set up user profiles offering different levels of access for different staff groups. None of the IT departments, however, had implemented different levels of access across their Trust.

4.5 Information governance

This section provides background for the findings relating to information security and information governance reported in Chapter 8.

4.5.1 Information governance structures

Within T4, the information governance function was closely integrated with informatics.⁶⁶ The role of Senior Information Risk Owner (SIRO) for the Trust lay with the executive director of finance. Primary responsibility for information governance lay with the associate director of informatics. An information governance group was in existence, the role of which was to monitor compliance and

progress against the information governance agenda and the Information Governance Toolkit (IGT) (Section 1.4.4). The head of information, information governance managers and representatives from major clinical divisions were represented on this group *ex officio*. (The records and governance manager T4-09 reported that, since coming into post, he and his colleague had striven to include the divisional representatives as a means of better embedding information governance across the Trust; the group had previously been very small and informatics-based.) Specialist staff from other departments, such as information technology, health records, data quality, clinical coding and risk management, were invited to attend meetings as required. The information governance managers also acted as the Freedom of Information leads for the Trust. The group reported to a patient records board, which in turn reported to an IM&T strategy board, which had direct input into the Trust board. It could also report directly to the SIRO and to the medical director, who was designated as Caldicott guardian. Recently a Head of Risk Governance and Control had been appointed, to whom the information governance managers had begun to report. However they themselves had no direct reporting links either to the Senior Information Risk Owner (SIRO) or to the Caldicott guardian, which they felt to be unsatisfactory (T4-09).

T4-09 was aware from his conversations with colleagues in other local Trusts that the information governance function could sit in different places within the organisation: planning, finance, IT, governance, or other corporate areas. He felt that the close identification of information governance with informatics in T4 was fundamentally wrong:

“We don’t think informatics is the right place for it. We think it is a corporate function that should fit more in the risk side. Because although a lot of it is informatics that tends to force the issue, the thinking it is just about informatics and information systems in IT and that was how it used to be here, which is very wrong, they forget everything else out in the divisions and departments.”

Related to his observations about its organisational position, T4-09 felt that information governance did not have the prominence within T4 that it warranted. He was particularly concerned not to be involved in the development of the Trust’s new EPR system:

“I don’t think personally that IG has really had the prominence within this organisation; it has more been seen as an afterthought ... rather than an enabler, something that underpins everything that should be going on across the organisation, not just in informatics.”

“I think generally it’s the understanding of involving IG in developing new systems and technologies. I think it’s never really been considered. We get more and more requests now, more and more people are coming to us, but they are looking to develop their own EPR in-house here, we have not really had many instances of involvement with that to date. It is ongoing, being written, but when we keep mentioning it, and I have touched upon issues, but nobody has really sat down and said, ‘This is what we need to consider for an EPR’, it is almost like it will be an afterthought ((laughs)).”

He had been successful, however, in getting information governance embedded in the management of some smaller projects: see Section 7.2.3.8, below.

Within T3 the overall strategic plan, however, was one of integrated risk governance, following Department of Health guidance (Deighan & Bullivant, 2006). Here again the role of SIRO for the Trust lay with the executive director of finance, although it was possible for it to be held by other executive directors. The head of clinical governance acted also as the information governance lead. Much of the operational responsibility for information governance lay within the role of a single records and governance manager (T3-09), including compilation of IGT annual returns. According to her and the HR manager T3-03, this role could include, for instance, ensuring information governance compliance of proposed new software, data curation in joint working, and devising appropriate security questions to allow staff to identify themselves over the telephone to corporate services such as IT, payroll and HR. In connection with her IGT role, T3-09 had jointly rewritten the IT acceptable use policy (AU3) with the head of IT, replacing a previous one which was very out of date (T3-03). Responsibility for information governance was devolved to managers across the Trust with respect to their specific roles and functions, particularly for corporate services, e.g. to human resources managers for governance issues relating to smartcard management and access to staff records, with T3-09 acting in an advisory role. This structure meant in practice that she was often operating in isolation (T3-09).

The main decision-making body for information governance within T3 was a records and clinical systems group, of which T3-09 and the IT manager T3-06 were members *ex officio*. (There had originally been a standalone information governance group, but it had merged with the health records group and the clinical systems group to form the current group (T3-06)). Standing agenda items at its bi-monthly meetings included the following: breaches of confidentiality, inappropriate access to electronic clinical systems, system security, subject access requests, and freedom of

information requests. Its remit included policy-related issues, such as external requests for access to the Trust network, and the approval of policies (T3-03). It did not routinely consider website blocking issues (T3-09). The records and clinical systems group reported to a patient safety and effectiveness committee, which in turn reported to a quality committee of the Trust board. The communications officer T3-12 reported that in this Trust the Head of IT role occupied by T3-06 was perceived as the provider of a service; T3 no longer had a “head of informatics” role as such.

Information governance at T1 also sat within an integrated risk governance structure. Here a records and governance manager (T1-09) reported to a senior governance and risk manager (T1-12), whose role pulled together all aspects of risk management, including patient safety, manual handling, health and safety, fire safety, clinical governance, information governance, management of policies and procedures, clinical audit, and research and development. The post holder also managed the Trust risk register and board assurance framework, and acted as deputy Caldicott guardian. The role of Caldicott guardian was fulfilled by the medical director, who also held responsibility at board level for IT. As with T3, the information governance manager held responsibility for IGT annual returns and for compliance with information rights legislation. The information security role within integrated governance, giving responsibility for planning and supporting information security assurance, was assigned to the two most senior managers in IT. Information governance risk assessment was owned by the information governance committee and IT security policy by the IT security committee. The information governance committee, on which risk and governance managers from every clinical division of the Trust were represented (T1-12), was accountable to an operational integrated governance committee, which in turn was accountable to a strategic integrated governance committee, which then provided input to the board of directors. According to T1-11, the information governance committee was responsible for developing policies and periodically conducted surveys among Trust staff on the impact of information governance policies; however, the response rate was only about 1% (30 out of a possible 3000)(T1-09). Possible amendments to policies were discussed in information governance team meetings, which were held regularly (T1-11).

4.5.2 Information governance working relationships

T3-03 referred to good working relationships with the IT department, with no issues of concern. T3-09 also referred, as an example of effective working relationships, to the consultative processes involved in some joint work between IT, information governance and HR on suitable security questions with which staff members could identify themselves to helpdesks.

T4-09 described working relationships with T4's IT department as poor, despite their physical proximity within the same building. He gave three examples, one relating to the use of e-mail encryption software, where the IT department had purchased an email encryption solution which they had not publicised, for which information governance had eventually written the procedure, which had not been their responsibility. Another example also related to encryption software:

"...The other day someone e-mailed us about wanting to send some notes electronically on a CD and how did they go about encrypting that. What did they need to do? And we just explained that national guidance was: it needed to be encrypted to a minimum of 256-bit, but in terms of a technical solution they had to speak to IT about what IT solution was available. The two-way process isn't there. IT don't tell us what is available, we passed them to them, but that would be it ..."

As his third example, T4-09 cited the fact that the IT department did not inform him of their staffing structure, which meant that he had no idea who held which responsibilities relating to information security. This made it very difficult to obtain information to provide evidence for IG T returns, for instance.

T4-09 felt there were tensions generally between the information governance function and IT:

"I think we are seen as the stumbling block in everything we do. We are there to help people, and IG should underpin everything, but we are just seen as a barrier. People think we are awkward, but we need to balance that. It needs to be lawful, it needs to be secure, we need to keep it confidential, we don't want to stop people doing the jobs, but we need to visit all those things." (Records and governance manager, T1, 9)

He concurred with the researcher's suggestion that communication from the IT department to end-users was also poor.

From the IT side in T4, however, relationships were viewed as working satisfactorily. The IT manager T4-20 reported that the only contact he had with information governance staff was if there had been a security breach, and an investigation by IT was needed:

"No, only if there is a breach ... they come to me and we do the investigation. We do the investigation technical side of things so as to pull out any data that is required by the governance team."

He reported that this worked well:

"There doesn't seem to be any issues there. We have a couple of guys in the information governance team, we, quite often they ask us for ... discovery searches on a particular user's mailboxes for any reason if there has been a security breach ..."

(IT manager, T4, 20)

T1-12, a senior governance and risk manager, felt that T1's structure basically worked well. It was useful, she felt, that both IT security and integrated governance reported to the same executive director. However, she felt that integrated governance and IT could work more closely together, particularly where policy development and updating (AU1) was concerned:

"I am not sure we are always on the same page, if I am being truly honest ... I think they see themselves very much as the technical guys sometimes ... and you do the governing bits ..."

"I think it's very ... particularly when we are trying to get policies up-to-date, so policy updates ... business continuity plans, disaster recovery plans, so we are very process driven, version control, timescales, you know... and also write it in a language we can understand."

(Senior governance and risk manager, T1, 12)

T1-11 provided an example of a project relating to ambulance Trust use of N3 on which IT had worked jointly with governance on setting up shared use.

On the matter of policy development, T1-11 spoke as follows:

"We tried to put it in one giant IT policy ... there is always discussion with governance around what is in the IT policy. They would always like to tighten things down ... there is issues around how can you send patient information off site, and historically... it has always been if it's one person's ... data you can send that in an e-mail, any more than 10 it needs to get ... encrypted and sent, and so there was all these ... little, I wouldn't say arguments but there was always ..."

He characterised his own general stance on information security as essentially a pragmatic one:

"... my main ... role is making sure that things keep on working here, systems work, and [the] network ... works, people can come in, log on to the computer, and do their job, and that is ... what my ... role is in its basic terms. And the more tighter [sic] we have the security, the easier my job becomes, but it is not really very pragmatic to ... think that everybody will have

the same desktop, everybody will have the same restricted access; no, you can't ... do that, and so, the approach that we ... take is firm: ... everyone will have AV, everybody will have updates pushed out to them, but if some people ... require access to different things ..., we will allow that as long as it is followed up by the correct documentation, so that we can approve that."

T1-11 and T1-09 both felt that relationships between information governance and IT, despite minor niggles involving communication, were positive:

"We work well with governance ... we have got a good relationship with them ... we have regular meetings with them to discuss these sorts of issues that we have."

(IT manager, T1, 11)

"There is a good awareness here, and I run the information governance committee and IT sits on that." (Records and governance manager, T1, 9)

T1-11 also mentioned the drawing up of information sharing agreements with external suppliers as an area of joint working between IT and information governance.

4.5.3 Sources of professional information and guidance

When asked by the researcher about her main sources of professional information and guidance in making decisions about information security and information governance, T3-03 reported referring to cases in her own past experience, and to the regional network of information governance managers.

P2, one of the pilot interviewees and an NHS IT manager, also spoke of the existence of local networks of information governance managers and their importance as a source of information and advice. In his experience they included people both from policy backgrounds and from technical information security backgrounds. The communications officer T3-03 mentioned the Trust solicitors and the national network of Caldicott guardians as possible additional sources of information and advice about information governance issues. The Health and Social Care Information Centre in her experience did not function as a useful resource: "None of my colleagues have ever been able to get an answer out of them for anything".

On the information security side, T1-11 referred to information bulletins produced by CERT and by security specialist vendors. Other than that, he was dependent upon previous experience, knowledge of security incidents that had occurred in the past, and discussions with colleagues, also the security bulletins recommended by the Trust's internal and external auditors. He was not aware of security material produced by the Health and Social Care Information Centre (HSCIC). T4-20 referred to bulletins from the HSCIC regarding security breaches, and HSCIC good practice guidance; otherwise he used Google to search for security information when required.

4.5.4 Decision making, tasks and priorities

On account of the different perspectives represented, it is interesting to compare the characterisation by information governance and IT staff of joint working with the views of T1-02, a human resources manager. T1-02 perceived the attitudes both of IT and information governance staff as very risk-averse (compare the comments of the senior nurse manager T1-07 and discussion of these in Section 9.2.3 below). In her view they preferred to block access to resources via technical means rather than to trust the staff to any degree, while monitoring and controlling the access to and use of them:

“The emphasis is very much on, well, we just won't give people access because then that completely minimises the - the risk there, and we just won't worry about the other stuff because – actually, that's not – you know – that's too hard ((laughs)).”

She said that in her experience, despite the existence on paper of swingeing penalties, people were not disciplined for breaches of policy such as sharing smartcards:

“We've got it written into policies that ... if you access - things that you shouldn't be accessing, then ... you'd be dismissed. I mean, I've written something myself about the use of smartcards around the implications of poor usage. There isn't a huge amount of monitoring ... on things like that, and ... sitting within the HR Department, I've never come across anybody that's been disciplined for leaving a smartcard in - in a machine, or ... so all of that kind of – there's talk, but – “

As well as noting a lack of emphasis on information management, T1-02 observed that the IT department felt under-resourced to manage anything other than clinical systems:

“... Their focus is very much on the implementation and maintenance of clinical systems ... so once you step outside of that, they then, they don't feel they've got the resources to do it, so there's a gap. We aren't putting enough resources into our own infrastructure outside of the ... clinical departments, and IT don't really think that they're resourced to do it either...”

(Human resources manager, T1, 2)

T1-09 felt that the information governance function was underdeveloped in T1 and across the NHS as a whole compared with other sectors; indeed she felt that there were no effective records management policies and practices in place within the Trust. In their roles she felt she and her assistant faced an uphill task in dealing with enquiries and attempting to ensure awareness of and compliance with information governance requirements:

“IG is quite under-developed in the NHS in particular... really in terms of... profession it is not as embedded as other ones like ... HR and finance, it should be up there and respected at that level.”

“It is an upward struggle all the time to make sure that staff are, are complying with information governance ... in that respect that is what I mean by it being a fairly new profession; it is not as well, I don't know if respected is the right word, but it is not as well acknowledged, so we don't have as much resources as other areas, so ... that is our biggest challenge trying to...” (Records and governance manager, T1, 9)

T1-12 wished to draw attention to the enabling role of information governance within the Trust, for instance in a recent successful implementation of electronic prescribing, and to counter negative perceptions of the governance role. T1-09 would have liked to be able to do more on the communication and education side to embed an information governance culture within T1:

“I suppose that the communication and the educational side would be brilliant if we could expand that because that would start to change the culture a bit more rapidly, the more communication you get out there the better it is.” (Records and governance manager, T1, 9)

By contrast, T3's records and governance manager, T3-03, was positive about her Trust's information governance performance and culture. She summarised general attitudes within T3 towards staff information-seeking access to published information as follows:

“I think this Trust has had a fairly relaxed attitude towards it because our IG performance has been good, and maybe that’s the reason, I don’t know, ... but I think there is this ... assumption that staff will behave decently unless they prove us otherwise.”

(Records and governance manager, T3, 3)

In terms of the range of possible attitudes to end-users, this appears noteworthy as an indication of a relatively positive and trusting one.

IT managers were asked about their perceived priorities in information security. For P1 and P2, securing patient data was the highest strategic priority:

“... In order to access patient-level data ... the highest security ... processes, both technological and administrative, need to be in place ... and I can’t stress that enough”

(Retired director of IT, P1)

“The main focus where information security is concerned is ... related to patient-identifiable or person-identifiable data ... “. (IT manager, P2)

P2 identified cybersecurity as a priority:

“There are other priorities, obviously ... in terms of ensuring that we are protected against ... computer virus attacks ... and other information security breaches which could potentially cause disruption or data loss or ... actually in some cases have a direct impact on the provision of services to patients – if ... information systems aren’t available ... because they have been affected by some kind of security breach ... “. (IT manager, P2)

For T1-11, the priorities in technical information security were operational and related to what he termed “basic housekeeping things”: keeping antivirus software signatures up to date, ensuring that Windows security updates were automatically rolled out to end-users’ PCs, reviewing and monitoring the logs generated by the intrusion prevention system, monitoring the emails relating to malware generated automatically by the antivirus system, setting up access rights correctly for vendor access to new systems in accordance with the N3 code of connection, implementing and monitoring data sharing agreements with other organisations, and ensuring that IT trainers carried out security training for end-users.

T3-06 was less sanguine than his information governance colleague T3-03 about possible staff breaches of acceptable use policy. He was sure that some staff in the Trust were misusing IT

facilities. In order to monitor and report usage of Trust resources more closely, and to combat misuse more effectively, he would have liked to appoint an information security lead, rather than distribute information security functions between three or four different posts, as at present. He said that his staff budget, however, did not permit this. T3-06 stated that the most pressing practical security issue he faced was establishing the whereabouts of the desktop and laptop computers for which his department was responsible. The Trust lacked an RFID tracking system for computer equipment, and ownership of it was frequently contested with the clinical services.

T3-06 felt that clinical services were sometimes reluctant to pay for upgrades and replacements when they were required:

“... I have been trying for some time within this organisation to ... effectively for the ICT department to deliver a desktop service, and we take responsibility for that desktop estate ... and ensuring that it is fit for purpose, so we have nine-year-old machines connecting to the network, the services have the budget, they say that they don’t.” (IT manager, T3, 6)

This scenario invites comparison with T4-10’s and other accounts of “legacy” hardware and distributed procurement responsibilities in 7.2.2. It was evident in these situations that the importance of providing staff with sufficient PCs of adequate specification and performance was insufficiently recognised by budget holders, who viewed the equipment as “theirs” and possibly resented what they perceived as interference from the IT department. It leads to a wider question of overall ownership and governance of IT within the organisation; (*cf.* Andriole, 2015).

T4-20 felt that his main priority in information security was just “to keep on top of everything”, which was difficult owing to lack of resources:

“I think the difficulty is really keeping on top of every area that we have to cover such as e-mail security. There are times when we need to spend a day on ... say the [trade name] e-mail filter, just to check and update and to keep on top of everything, but unfortunately due to resources we are unable to do that so and again there is, the same with the web filter to go through any suspect ... sites that have been accessed, or for any reason there was a breach in security, with the user going to a site that they shouldn’t have been, then it is really having time to investigate further on those.” (IT manager, T4, 20)

T4-20 expressed the view that information security risk management in particular was an area that could be improved:

“Managing the risks is again -- we could manage the risks better, but a resource, resources are much more of a constraint really to do that. I would like to be able to manage risk a lot better than we currently do ... it is staff resources. That is the main constraint.”

This, he said, would involve him undertaking more monitoring of web traffic and investigating security risks and issues more thoroughly. The risks, he felt, were primarily of the introduction of malware on to the Trust network, which he felt presented an increased risk where staff members were accessing inappropriate sites:

“... Because I am quite sure that staff ... on this site do go to sites they shouldn't be. It is not a case of really... because they are doing that it is creating more risk for us, because these sites potentially have malware attached to them and it is to be able to fully monitor the traffic that comes in and out of this Trust.” (IT manager, T4, 20)

In view of the findings of research investigating the relationship of web-borne malware infection rates to user behaviour (see literature review, Section 2.6), it is interesting here that T4-20 and T3-06 both expressed the belief that staff members' accessing of websites proscribed by their Trust's AUPs, but not blocked by the SWG, was putting their Trusts significantly at risk of malware infections.

T4-09 felt that senior management attitudes to information governance and security within T4 were generally lax, and that improvements would likely result only from a major data breach involving ICO sanctions:

“The person who came here as the Trust Secretary, in another Trust where she had been she was the SIRO, they had three major breaches, in a short space of time got fined on the back of it, and that gave that organisation the kick they needed. But we say a lot here, that is the kick we need. It is not the right attitude, because we shouldn't be in that position, but that is the only way you get these things across the bow of the people who need to know about them. If the Board aren't interested they will soon look up from the parapet when they see a fine coming in at up to £100-200,000.” (Records and governance manager, T4, 9)

His suggested that previous recent data breaches had had only a limited impact on Trust policy and practice.

In some of the interviews, participants in IT services and information governance offered comments on Schneier's dictum, "Users are the weakest link" (Schneier, 2000). The responses varied widely in nature. The ease with which email could be sent to the wrong person by staff working under pressure was uppermost in T4-09's mind:

"I have sent stuff to the wrong person by e-mail; it is easily done, and when you are pressurised and trying to do everything it is very easy to just get one digit wrong in somebody's e-mail, because we have so much technology as well to assist us in our lives -- that often causes the problems, though." (Records and governance manager, T4, 9)

The security risks presented by phishing emails were cited by T4-20 in his account of a recent incident in which a phishing message had evaded the spam filter, but had been detected and disinfected before it had caused any damage. T3-03 described to the researcher an incident where PII had been inadvertently sent to the wrong person, whose email address had auto-completed in her email client. Her response to this had been to conduct training on the use of email within the department concerned.

P1, in the course of describing how he had dealt with incidents of Internet abuse at his former Trust, offered a striking statement: "People assume that abusing the Internet is an IT problem ... it isn't an IT problem, it's a management problem". Some of the participants in IT and information governance were asked for their comments on this. For T3-06, it indicated the manager's discretion in managing abuse of the Internet:

"I would agree with that ... but obviously there is an element of, there is always that caveat within that policy, it is at manager's discretion as well." (IT manager, T3, 6)

T1-02 was led to contrast the view expressed in the comment with how she perceived the approach within T1, particularly in relation to social media:

"Here we have an IT ...-led - approach to computer misuse, so things are very tightly controlled, often blocked, and – ... that's the approach that this Trust takes, which in terms of ... cultural progress down those sorts of, like – ... thinking about social media and the uses of social media, ... it's really restrictive." (Human resources manager, T1, 2)

Social media issues are discussed in detail in Section 9.2 below.

4.5.5 Internal and external assessments

None of the Trusts had had action taken against them within the last two years by the Information Commissioner's Office (ICO) in respect of breaches of the Data Protection Act, though T4-09 reported that a number of recent data breaches were under investigation.

The ICO was reported by T1-09 to have recently conducted an audit of information governance at T1. Areas for improvement identified were secure storage and transport of patient records, the currency of the information asset register, and clarity of risk ratings. It was also observed that the information governance structures of the Trust were "quite complex" and that the SIRO did not sit on some relevant committees, thereby hindering a clear oversight of key issues. T1's IGT assessment report overall score for 2015 was 80%, but with a "red" rating, only 42 out of 45 requirements being rated at level 2 or above, the same as the previous year (T1QA/14-15). Information governance incidents reported by participants related to patient notes left in a supermarket (T1-01, T1-02; according to T1-09 they were handover notes) and a breach of confidentiality by a clinical staff member via Facebook, which had resulted in her dismissal (T1-01, T1-07, T1-02). A junior doctor then working at T1 was also reported to be under investigation for inadvertently uploading patient-identifiable information to an open access website in the course of his previous work at another Trust (T1-06). According to T1-09, the handover notes incident had not had a major impact on information governance policy: her predecessor had reviewed and tightened up procedures relating to handover sheets, and publicised them heavily. The policy response to the Facebook breach of confidentiality is discussed in Section 9.2.1.

Information governance arrangements in T3, in particular its IGT submission, had recently been audited by an internal audit agency (S15) and received a "significant assurance" rating; relatively few areas of improvement had been identified. Its IGT report score overall in 2014-15 was 94%.

According to T3-03, reportable information governance incidents included the inadvertent sending of 61 unanonymised staff records to a local authority recipient in a spreadsheet, and the accidental sending of a staff record via email to a member of the public with the same name as a Trust staff member (the email system had stored the former's address) (T3-03). These incidents were described in detail in AR3/14-15; both had been rated at SIRI Level 2, but in consequence of the Trust's prompt response, no regulatory action had been taken against it by the ICO. An incident had also occurred with the physical health services extranet whereby a web editor had uploaded in error a document containing patient contact information to the public-facing element of the extranet that should have been uploaded to the internal-facing one (T3-06). A penetration test of the T3 network had been

conducted at the end of 2012, with another planned for the end of the financial year 2014-15. The IT manager T3-06 reported that in 2012 the Trust Wi-Fi had been given “a clean bill of health”.

The IGT report score overall for T4 in 2014-15 was 75%; all indicators were at level 2, which had achieved the rating of “green” (satisfactory) from the grading scheme. The only external audit of information governance arrangements appeared to have been one relating to a national clinical database which the Trust had formerly hosted. A number of information governance incidents were stated by T4-09 as being currently under investigation, including some which had needed to be reported to the ICO; details were not disclosed. Information governance incidents were reported in detail within the annual report for 2014-15: one table indicated that a total of 207 information governance incidents had occurred during the year, all at SIRI Level 1 or below (see Section 1.4.4, which appears inconsistent with what T4-09 had reported). Elsewhere in the report it was stated that 66 information governance incidents had been reported by staff, as compared with 49 the previous year. Internal audits undertaken during the year had given information governance a “limited assurance” rating in April 2014, but a “significant assurance” rating at a follow-up review in September 2014. The information governance managers in T4 were perceived by clinical staff (e.g. T4-08) as being very helpful and knowledgeable in dealing with information sharing and FoI queries.

4.6 Summary

This chapter has presented basic information about the Trusts, background information relating to national and local policy drivers and to organisational performance, and contextual findings relating to the main topical themes under which results are presented in the chapters that follow. A substantial section on information governance and security was included, covering structures, working relationships, sources of professional information and guidance, decision making, and external assessments. This relates more directly to the research areas of interest of this thesis; information governance and security are discussed also in Chapter 8. A thematic map (4.1) illustrates the contents of the chapter. Chapters 5 to 9 go on to present the main findings of the research; Chapter 5, which follows, presents the findings relating to barriers to information seeking, use and sharing.

Chapter 5. Findings: barriers to information seeking and use

5.1 Introduction

As previously stated (Section 3.10), the findings overall are presented in a series of chapters (5-9) covering the main themes which were identified in the course of data analysis, as follows: information access and barriers (5), professional education (6), organisational dynamics and professional norms (7); information governance and security (8) and communications policy (9). A final results chapter (10) presents a tabulated synopsis of key findings, and relates the findings for each Trust to background material and performance data in order to present a holistic view. An overview thematic map is given below (Figure 5.1).

The present chapter discusses barriers to information seeking, use and sharing which relate mainly to aspects of IT infrastructure. These are represented in Figure 5.2 below. It should be noted that much of what follows has relevance also for e-learning (discussed in Chapter 6). Issues specific to e-learning are discussed separately in Section 6.4. IT problems are described as reported by end-users.

While it is understood that end-users' reports of IT problems are likely to involve confusions or misunderstandings, or lack of knowledge, the reports are important in what they indicate about roles and relationships between stakeholders, and prioritisation of issues, as well as about the state of IT provision and use within the NHS.

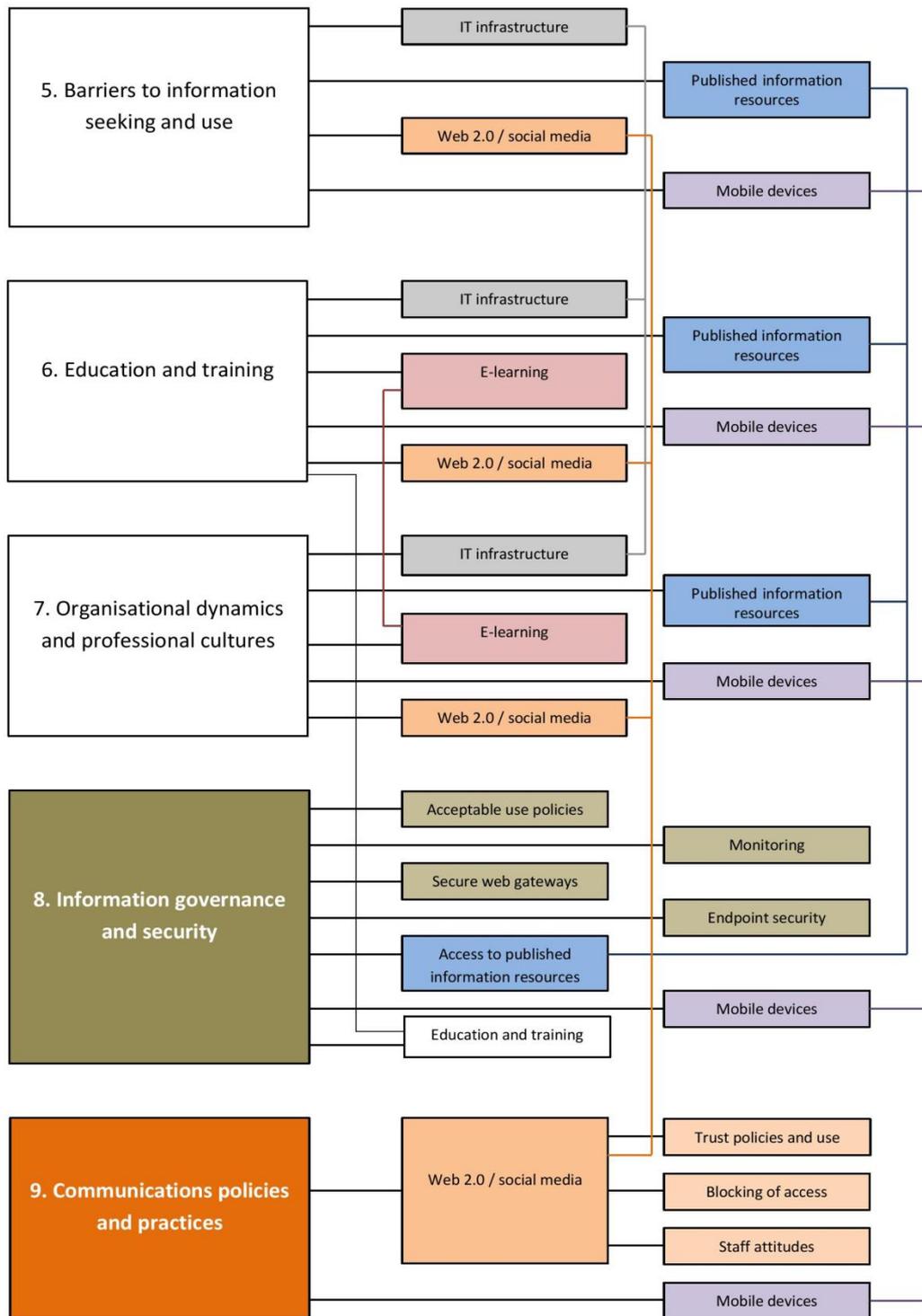


Figure 5.1 Overview thematic map

5.2 Trust IT infrastructures and their management

Within Trust networks, negative effects upon access to published information were experienced in respect of:

- Network access, availability and performance (5.2.2)
- “Legacy” software etc. (“legacy” hardware is discussed in 7.2.2)
- System policies and permissions (e.g. inability to download updates to browser plugins, or files of a particular type)
- Insufficient numbers of PCs in clinical areas

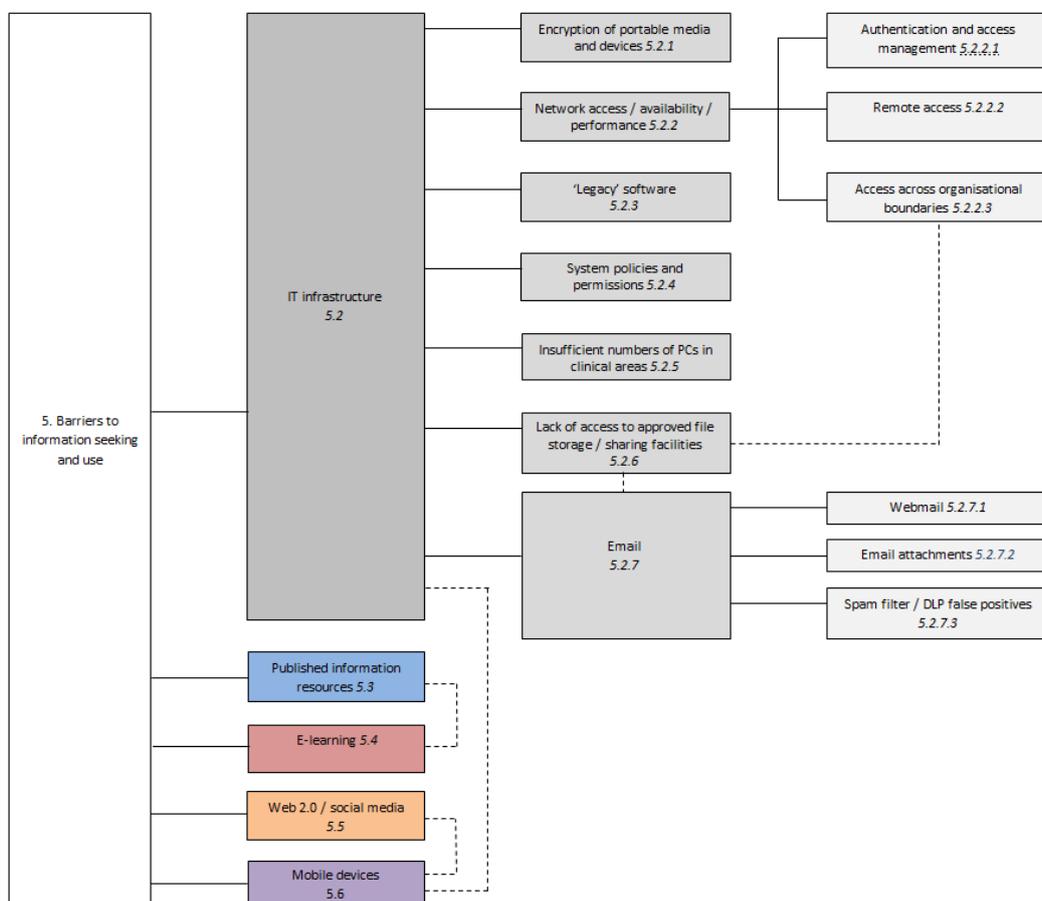


Figure 5.2 Barriers to information seeking and use

Negative effects upon storing and sharing information were experienced in respect of:

- The requirement to use encrypted portable media and devices (e.g. laptop and tablet computers, mobile phones, USB memory sticks)(5.2.1)
- Lack of access to approved cloud storage, internal file storage or external institutional file storage
- Issues with webmail
- Issues with email attachments
- Spam filter and data loss prevention system false positives

Blocking of websites, being related specifically to information governance and security, is discussed in Chapter 8.

5.2.1 The requirement to use encrypted portable media and devices

The requirements of national NHS policy regarding the encryption of portable media and devices were described in Section 1.4.4. However, it is apparent from the study findings reported below that there were wide variations between Trusts in how, and how effectively, the requirements were being implemented.

A confusing situation was encountered at T4 regarding encrypted USB memory sticks. The Trust's code of practice for the use of IT (AU4Sec) stated clearly that "*Trust approved USB pens can be obtained through the Informatics Service Desk*", and that "*Sensitive data must not be stored on any removable media unless the device meets the Trust's encryption standards*". T4-20 informed the researcher that, "We use; we deploy IronKeys ... and encrypted USB devices". An e-learning specialist (T4-22), however, stated that encrypted USB memory sticks were no longer being issued by the IT department. He had apparently attempted to order one via the helpdesk, and was told they did not have any in stock and probably were not going to order any more. He was not aware of any facility for encrypting existing memory sticks. On account of the large file sizes of some of the content he was using (video clips, etc.) he had begun using his own portable hard drive to transfer files, the use of which was not blocked on Trust PCs.

Difficulties in obtaining Trust-approved USB memory sticks could act as a barrier to saving, storing and using information retrieved online, and also present a security risk. Staff at T1 and some staff at T4 reported restrictions on access to, or bureaucratic hurdles to obtaining, encrypted USB memory sticks. The IronKey devices used at T4 had apparently cost about £80 each, which could have been

prohibitively expensive for some services (T4-09). Encrypted memory sticks were not available to students on placement in T1, creating problems for them working on case presentations at home (T1-04). In T3, difficulties in obtaining USB memory sticks were not reported; they appeared to be readily available to staff who needed them. However their use away from NHS sites for non-core purposes (e.g. research or study) required specific permission from the information governance manager (T3-03). In T1, permission was required from the IT department or from information governance for any use of encrypted removable media away from Trust sites.

The requirement to use encrypted USB memory sticks commonly caused inconvenience to visiting presenters on NHS sites, who were obliged either to use their own laptop for the presentation or to email it in advance (P1). The encrypted USB sticks themselves were perceived to have inherent limitations, mainly relating to slow loading of content, causing problems when giving presentations at events (T3-21). T3-21 complained that hers could not be used on her Macintosh at home. T4-10 felt that the use of USB memory sticks for transferring information was old-fashioned in an era of mobile devices and widespread use of cloud storage:

“... I just think, ‘Oh wow, in this day and age, I am still carrying sticks around!’ which actually goes back, doesn’t it, to your point about a tablet? If I am going to work at [H15-WH] I essentially have to take a stick of stuff to that ... we are still there, we are still at that point.”
(AHP clinical lead, T4, 10)

A specific learning and simulation issue involving USB memory sticks is reported in Section 8.6.

5.2.2 Network access, availability and performance

5.2.2.1 Authentication and access management

Anecdotal evidence suggested that policies controlling the availability of network logins, including generic logins, could present barriers to accessing and using published information. This could particularly affect library services, restricting the services they were able to offer to NHS staff from other organisations under reciprocal access agreements. The issue of network access is discussed in more detail in Section 6.2 below.

5.2.2.2 Remote access

All the Trusts in the study provided remote access to their systems using Microsoft Virtualization Desktop Interface (VDI)⁶⁷ or Virtual Private Networks (VPN) via authentication tokens, although in practice within T1 the facility was reported to be generally available only to “consultants and people like that” (T1-01). It was readily available in T3; several participants referred to using it. Remote access was not mentioned by participants in T4, although its availability was confirmed by reference to the relevant policy document. In T1, problems with it affecting user profiles were reported. It was unclear from T1-08’s comments whether this was an issue that had been reported to or was being addressed by the IT department. Problems of this type were not reported in the other Trusts.

5.2.2.3 Access to systems across organisational network boundaries

A number of general problems accessing systems across organisational boundaries were reported. T2 staff working on T1 sites reported problems accessing some T2 systems from within the T1 network, particularly the NLMS for e-learning (T2-01, T2-02).

In T3, where the community health part of the Trust (T3-WPH) was on an outsourced network, problems were reported of inability to access the Trust intranet. Also, in addition, T3 e-mail addresses in Microsoft Outlook did not auto-complete on PCs linked to the outsourced network, slowing the process of inserting addresses. A community nurse educator at T3 (T3-20) indicated that access to T3’s systems from local authority premises or GP surgeries, where many of the staff were situated, often presented a problem, since it could depend entirely on the relevant organisation’s information security policies, over which the Trust had no control.

The radiographer T4-12 reported an inability to access U9’s databases or Blackboard (VLE) site from within the Trust network. The situation she described appears to reflect failures of communication and project planning, notably between the Trust and university IT departments, regarding provision of access to the university resources from within T4’s network. Enabling students on placement to have access to their university databases and Blackboard might have required merely some simple

⁶⁷ Virtualization Desktop Infrastructure: <http://www.microsoft.com/en-gb/windows/enterprise/products-and-technologies/virtualization/operating-system/default.aspx>. (VDI hosts the desktop environment in a virtual machine (VM) that runs on a centralized or remote server (“What desktop virtualization really means,” s.d.), (“What is desktop virtualization?,” s.d.)

changes to firewall settings; *cf.* the arrangements for e-journal access at T4 described in Section 5.2 below. It would have been interesting to find out more about this pilot project.

5.2.3 “Legacy” software

“Legacy” software, in particular older versions of Microsoft Office and the Internet Explorer browser, and the now-obsolete Windows XP operating system, was still widely in use within all of the Trusts. An account was given in Section 4.4.1 above of their respective plans and processes for upgrading.

Users were also likely to have encountered a variety of problems with displaying web-based content owing to lack of browser support for front-end web technologies such as Cascading Style Sheets (CSS), HTML 5, and JavaScript (“Can I use... support tables for HTML5, CSS3, etc.,” *s.d.*; McCarthy, 2013). In T2, the standard browser was due to be updated from IE6 to IE7, and the library computers had been upgraded to IE8; however, Google Chrome was not standard on library staff computers, leading to “a problem with functionality with some databases” (T2-04). The NLMS content required pop-ups to be enabled. Some web applications required particular versions of Java to be installed on the user’s PC (T1-10). Lack of the appropriate browser add-ons, notably Adobe Flash and Adobe Shockwave, could also present problems. A particular issue relating to browsers and library services is discussed in Appendix J, and a support issue with Java versions on users’ PCs and e-learning is reported in Section 6.2.

All these problems, in particular the continuing use of older browsers and Java versions, would have presented some level of security risk (*cf.* Sections 2.6, 8.4), as well as hindering access to and use of published online information in varying degrees. It should be noted that legacy systems for software used in different departments within hospitals and the NHS had long presented a major problem also for sharing patient data across departments, e.g., radiology systems, pathology, etc. (P. A. Bath, personal communication, 2016).

5.2.4 System policies and permissions

Issue 5.2.3 above is generally often linked with that of system permissions or system privileges, in particular those required to download files of certain types, including software updates, or to enable security permissions relating to browsers or browser add-ons, e.g. enabling pop-ups or JavaScript. (Software downloads were specifically prohibited within the Trust’s AUPs.) T1-08 spoke of inability to enable cookies when required, inability to download ActiveX controls, lack of required Adobe

software configurations or versions, and incompatibility of applications with Windows XP as hindrances to accessing e-resources.

T4-22 spoke of a system locking policy on Trust laptops that interfered with presentations, and presented a particular hindrance for external presenters:

“In effect they have had these carte blanche rules that say, for instance ... any computer that we have in the Trust, has to lock itself out if you don’t use it, it locks itself out after ... 10 minutes ...

He felt that staff in the IT department were being inflexible in their response, insisting that laptops be networked when this was not really necessary:

“ ... What happens when we have external people coming in to present? Because, quite clearly, as soon as we are going to leave the room it is going to lock itself out, so the only thing we can then do is to give them our password, so that is instantly against everything so ... ” (E-learning specialist, T4, 22)

The work of this specialist in promoting and sharing current work in e-learning development was thereby being adversely affected.

5.2.5 Availability of PCs in clinical areas

It was mentioned also by T1-03 that nurses on the wards were unlikely to be able to access the Internet owing to a shortage of computers. The shortage of PCs on the wards at T1 and their constantly being in use for clinical systems updating was referred to also by T1-07; it underlay the decision to purchase tablets for e-learning (Section 6.6). Shortages of PCs in T4 were referred to also, by the AHP clinical leads T4-08 and T4-10.

A cluster of frustrating issues were reported relating to information storage and sharing and the use of email to transfer information resources. These are discussed in Sections 5.2.6 and 5.2.7 below.

5.2.6 Access to approved storage

Board members at T1 had available to them a cloud storage solution called Content Locker (AirWatch)⁶⁸ which had been implemented as part of the Trust's mobile device management (MDM) solution. This was intended for board members and divisional general managers to use with their iPads (T1-11). BoardPad, a secure collaboration and document management solution, provided a similar function for senior managers in T4 (T4-20)⁶⁹. These applications were not available to other staff. A "quota" was applied by the T1 secure web gateway to the use of personal cloud storage applications such as Dropbox, OneDrive etc., i.e. the use of them was "rationed", even for work purposes (T1-11). Some staff, e.g. T1-04, had found them to be blocked entirely. Staff at T4 were able to use Google Drive for file storage and sharing, although T4-20 stated that he would have preferred to block it on security grounds. To do so, however, would apparently have been difficult for technical reasons. Access to Dropbox, however, was blocked (T4-04). T1-01 reported that junior doctors and others had difficulty accessing their personal Trust network drives from home or from a university network; the facility to use virtual private network (VPN)-based remote access via a secure token tended to be limited to consultants. Generally staff were unable to access their Trust network drive from within the university network and *vice versa*. Since access to Dropbox and other web-based cloud storage and sharing applications had been blocked, staff generally resorted to email as a means to share information with colleagues or to transfer content between Trust and external filespace (e.g. T4-22). T4-04, a pharmacist, reported that the inability to use Dropbox presented a significant hindrance to sharing information with colleagues outside the Trust. T4-03, a communications officer, raised the matter of possible data protection issues with popular cloud storage applications, i.e. that the data centres might not be situated within the European Economic Area, and hence that use of them to store personal information could breach the eighth principle of the Data Protection Act. The discussion of the risks of shadow IT in Section 2.8.3 may be recalled.

5.2.7 Email

5.2.7.1 Webmail

As we have seen (1.4.3), the Trusts in the study (other than T2) used domain-based email rather than NHSmail. Anecdotal evidence suggested that it was common for junior doctors within some Trusts to use services such as Doctors.net.uk rather than Trust email addresses or NHSmail. Access

⁶⁸ Content Locker: <http://www.air-watch.com/solutions/mobile-content-management/>

⁶⁹ BoardPad: <http://www.boardpad.com/>

to webmail applications was allowed within T4; The IT manager T4-20 said that he would have preferred to block it on security grounds, but to have done so “would [have] cause[d] a riot”; it “would have caused the users too much pain”. According to T4-03, Hotmail had been blocked at one point, but doctors had complained about it *en masse*, so the decision to block it had been rescinded almost immediately. Remote access to Trust email via Microsoft Outlook Web App was available to all staff. T4-08 reported that, at one stage, it had not been possible to download and read attachments in Hotmail messages. In T1, remote access to Trust email via Microsoft Outlook Web App was available to all staff via a login on the Trust intranet (T1-03, communications officer). T1 also allowed webmail (T1-09). T2 blocked access to all webmail applications (T2-03, T2-04). T3 allowed the use of webmail applications, but not for Trust business; they were only to be used with a line manager’s permission. It was stipulated in AU1 that attachments to webmail emails must not be opened, on account of the possibility of their containing malware. AU1 also required the exclusive use of Trust email for Trust business.

5.2.7.2 Email attachments

In view of the high level of use of email for transferring files (see above, Section 5.2.6), limits on email attachment size presented problems for some users. All the Trusts in the study ran their own Microsoft Exchange mail servers, with limited use being made of NHSmail. T1’s size limitation for email attachments was stated by the IT manager T1-11 to be 22 MB. This high limit was apparently intended to allow for the large size of tender documents sent out by the supplies department and of reports considered by board members. T4-19, a consultant surgeon, reported occasions when emails with attachments to his work email from his home email had been blocked; he did not know why this had happened, but the matter had been resolved via a call to the IT helpdesk. The pharmacist T4-04 reported experiencing difficulty sending presentations from her Trust email to her home one, even splitting them across several messages. She was unsure what the attachment size limit was within T4. The same issue was also reported by T4-22, an e-learning specialist, whose work involved transfer of large video files. He said that he thought the attachment size limit was 10 MB. A related problem was the inability to create or send compressed files in the .zip format; these were blocked by the Trust email filter as a potential security risk. (Email attachments of this type were widely recognised as a method of spreading malware: Great White North Technologies (s.d); WinZip (s.d.)). He had resorted to using his own portable hard drive to transfer files between networks; he was able to do so on account of the non-blocking of USB ports within the Trust (see below, Section 8.5).

5.2.7.3 Spam filter and data loss prevention false positives

The clinical tutor T1-06 reported a problem relating to attachments in email circulars received from Public Health England (PHE). The attachments were encrypted, with a password sent separately, and the Trust spam filter had blocked the email providing the password. PHE, when it was initially established, had not been “recognised” as legitimate by the Trust spam filter, unlike its predecessor body, the Health Protection Authority. T1-12, a senior risk and governance manager, also reported occasions when legitimate incoming email had been blocked as spam.

Several participants (e.g. T1-07) reported occasions when they had been unable to send out emails. According to T1-11, T1 had implemented a data loss prevention application called Proofpoint.⁷⁰ T4 had also implemented a DLP solution, but used it for monitoring the possible sending of patient-identifiable data, not for blocking (T4-20).

In describing these issues, and also their inability to access information resources, participants tended to refer to “the firewall”; they did not distinguish between possible different security applications. They also tended to attribute their experiences of false positives to the robustness and strength of the application concerned, or failed to distinguish the attributes of sensitivity and specificity (see Section 2.7.3.4.1 above, and Appendix L):

“I am told our firewall security is that military spec that some stuff can’t penetrate through, we have problems with people ... trying to send us stuff sometimes because of our level of security.” (Senior governance and risk manager, T1, 12)

“We can’t always access some of the university databases from here because of the firewall...I understand why the NHS protects its firewall because you do get a load of rubbish through etc., and we have got a lot of patient sensitive information ... but that ... has been a problem.” (Radiographer, T4, 12)

The senior nurse manager T1-07 spoke also of difficulty sending information caused by “the firewall”. It would have been interesting to explore in more detail how IT staff represented security applications (SWG, DLP, spam filter, IDS, firewall etc.) in discussions and in Trust documents, and also non-technical participants’ constructions of cybersecurity measures at their respective Trusts.

⁷⁰ Proofpoint: <https://www.proofpoint.com/>

These would be expected to reflect the content of their previous discussions with IT staff members, as well as contemporary media coverage and their independent reading.

5.3 Published information resources

Most clinicians reported making use of e-resources made available by Trust libraries and accessed via an OpenAthens login. Participants tended to equate “using the library” with “visiting the library” (e.g. T4-04) and did not always appear to realise that access to the full text e-journals they habitually accessed and used was administered by their Trust library (e.g. T4-19). T1-04 reported only two occasions when she had been in contact with the library, both related to a need to obtain a book which was available only in hard copy. The AHP clinical lead T2-02 spoke of using an online current awareness and full-text e-journal service from the British Dietetic Association which obviated any need to use the Trust library’s services. The radiographer T4-12 mentioned a comprehensive collection of e-journals and other material available to members of the Society of Radiographers. The physiotherapist T2-03 stated that access for physiotherapists to electronic content was poor, affecting his ability to answer clinical questions in a timely fashion, that neither Trust library service (i.e. T1’s or T2’s) could provide the full text online of many physiotherapy and rehabilitation journals, and that access via document supply was not really adequate. There were apparently two physiotherapy research facilitators with a link to U6 who were sometimes able to obtain articles for other staff. This participant, however, did not appear to be aware of the walk-in access to some of U2’s journals available within T1’s library on the university computers.

T1-08 reported that the NHS Evidence search interface for bibliographic databases, Healthcare Databases Advanced Search (HDAS) was very prone to crashing, resulting in wasted time. The overall problems with the functionality of HDAS (described in Section 1.4.5 above) were acknowledged by NICE-01, a senior manager at NICE, as raising major questions about strategic responsibility within the NHS for the overall quality of IT infrastructure provision within Trusts, which was perceived to be a major contributory factor:

“... I am the person that gets shouted at when these things don't go right, so I would come back into my organisation and say, 'This is ridiculous, you know; we need to do something about this.' Eventually ... we did start to test and we did go out to NHS libraries and look at HDAS on the system, and we could see the difference, then we started to realise actually this performance difference, is massive ... so ... that was initial -- so you are talking three years ago that ... I recognised that, but I think it had been recognised obviously long before that, but it was something that I was quite passionate about -- was trying to address, because we needed ...” (Senior manager, NICE)

NICE-01 stated that she had wished to pursue the matter at policy level, but owing to her uncertainty regarding lines of responsibility for IT infrastructure, had felt unable to do so.

T4-04 reported making considerable use of Google in her research for teaching sessions:

“See, I am a bit of a Google fiend, I have to be honest, which is quite unusual for pharmacists because usually we are very -- as a profession we are quite scornful of people who Google ... I am perhaps a bit maverick in that I do love a bit of Google -- (Pharmacist, T4, 4)

All the library managers in the study other than T2-04 reported that they or their staff had access to the appropriate browsers to manage the link resolver and OpenAthens (see Appendix K). T3-06 could not recall seeing the letter sent from NICE, however. The standard browser within T3 was IE8; the upgrade to IE8 had apparently taken place across the Trust just as the new OpenAthens interface was implemented, hence the library service avoided major problems at the time of the transition. The Chrome browser was available as an alternative browser within T3 should one be required (T3-01). In T1 the standard browser was Internet Explorer 7 (IE7), but the library staff had been given access to Google Chrome (T1-01). Browser availability was not mentioned by librarian participants at T4; however the researcher was informed that, while IE7 was standard within the Trust, Chrome and Mozilla Firefox were available as alternative browsers for people whose work required them (T4-04).

Librarian participants (T4-06, T4-07, T3-01 and E10) reported a number of ongoing problems in accessing e-resources that were affecting all the libraries, NHS or otherwise, using the OpenAthens system. These included problems with a major general medical journal published by Pub6. When attempting to log in to the content of two major scientific and medical (STM) publishers, Pub2 and Pub3, at article level via OpenAthens, readers were being taken back to the publisher's home page, and needed to use their browser search history to locate the correct page again. In attempting to

access content at article level of another publisher, Pub1, either OpenAthens authentication was failing or users were being taken to the home page rather than to the correct article page, as with Pub2 and Pub3; Pub1 was not believed to have implemented OpenAthens. Several infrastructure changes had occurred at once for library services, namely implementation of a new link resolver and of OpenAthens, making it difficult to identify where problems were occurring; publishers which had implemented OpenAthens had experienced teething problems, and confusion was reported to have persisted for about 18 months overall (T4-06).

T4 library conducted monthly IP checks for its e-resources (T4-06, T4-07). T4-07 was not able to use the DNS *ping* function to check availability (*ping* was presumably blocked by T4's firewall), but noted any changes to IP addresses and passed them to a named person within the IT department who was responsible for managing the Trust firewall, for him to make the necessary changes to settings. This was normally done very quickly, sometimes within the hour. She reported that IP address problems mainly affected Pub1, occurring as often as weekly.

T1-04 drew the researcher's attention to a significant problem at T1 with access to an essential reference guide for prescribers and dispensers, the British National Formulary, generally known as the BNF.⁷¹ It was available in print, online, as an e-book, and as a mobile app. The BNF was updated monthly online via NICE Evidence Services, and via the NICE BNF mobile app. The print edition was updated every six months. However, NICE purchased hard copies and distributed them to Trusts only once a year (T1-04, T3-18). The shortage of PCs on the wards in T1 has already been noted (5.2.5), and departmental policy precluded the use of mobile devices within clinical areas (see Section 7.6, below):

"... Most of the wards have three terminals ... one of which is the ward clerk's domain and you are not allowed to touch that; you are fighting for them with doctors, and as an internal thing within pharmacy, we are not allowed to take smartphones on to the ward."

(Pharmacist, T1, 4)

The result was a lack of access on the wards to the most current version of BNF, leading potentially to the use of out-of-date print editions; this could have led to problems during CQC inspections, and could potentially have resulted in patient safety incidents (*cf.* National Pharmacy Association, 2016).

⁷¹ British National Formulary online: http://www.bnf.org/bnf/org_450080.htm

According to T1-12, a senior risk and governance manager, efforts had been made at T1 to address the problem by making the BNF available via any Trust PC. She said that the possibility was also under consideration of providing tablet computers which had the BNF app installed on ward drug trolleys for quick reference by nurses. T1-08, however seemed to think that this or a similar proposal had been discounted on grounds of cost. T1-08 was clear that having the electronic version of the BNF available via Trust PCs was not sufficient for nurses preparing to administer drugs to patients:

“... It is not accessible. When you are in the clinical room getting the drug ready, you would have to come out of there -- you would have to try and get on to a computer, you would have to then get on to the intranet, you would have to access that, and that, is too many steps for staff to consider ... yes, the tablet was too costly and that was then ... put aside.”

(Clinical teacher, T1, 8)

T3-18 reported that the electronic version of the BNF was available there on all Trust PCs via an icon on the desktop. However, he had also raised concerns with the Trust senior management about the lack of ready access to the BNF within T3. T3's mobile devices policy also precluded the use of personal smartphones in clinical areas. (The BNF could not be accessed via the Trust's BlackBerry devices.) T3-19, who was responsible for the professional development of school nurses and health visitors, reported that access to the BNF was a particular problem for community nurses undertaking domiciliary visits.

While library services at all three Trusts were provided with adequate IT infrastructure to manage the provision of e-resources, the library staff at T4 mentioned a problem in managing the library pages on the Trust website, which they were supposed to be able to edit:

“I think what happened was from my understanding ... they had a content management system and they just migrated along the internal pages on to the external ones, but they don't work the way they should do.” (Librarian, T4, 6)

Clearly this presented a hindrance to the library's promoting its resources and services effectively. It is possible that other Trust services with an external web presence were also affected.

5.4 E-learning

Use of e-learning resources specifically for purposes of information seeking was not mentioned or discussed by participants. This at first sight is an odd finding, given the overall wide availability of e-learning resources. It is possible that participants did not categorise them separately from others when considering their use of online information resources.

5.5 Web 2.0 and social media

It should be noted that the researcher found that the term “Web 2.0” was not readily understood. While she asked them about access to and use of particular applications which are frequently classified as “Web 2.0”, she accordingly used the term “social media” rather than “Web 2.0” in discussions with participants.

In T3, a clinical tutor reported that he and his trainees were unable to download externally-produced podcasts, indeed to download anything other than PDF documents (T3-02). The medical education administrator T3-20, however, indicated that it was bandwidth problems that gave the appearance of podcasts being blocked; they were in fact just very slow to download. There had, however, been an instance where a podcast had definitely been blocked, and T3-02 had asked the IT department for it to be unblocked and been refused; he was unable to ascertain the precise reasons given for maintaining the block on this content, although his recollection was that an intellectual property issue was involved; if validly applied, this would in principle have provided a legitimate reason for blocking access. At both T1 and T3, plans were in hand to use internally-produced podcasts to disseminate information, making them downloadable from the planned new intranet sites (T3-20, T1-12). Downloading of externally-produced podcasts was not reported to be blocked within T4 (T4-10).

The library at T4 had developed social media platforms to support information seeking – a Pinterest⁷² site with infographics, and a library website/ current awareness portal using the WordPress blogging platform.⁷³ Staff who were not approved to access social media from their

⁷² Pinterest: <https://www.pinterest.com/>

⁷³ WordPress: <http://www.wordpress.com>

desktop PCs were able to access these sites via personal mobile devices using T4's Bring Your Own Device (BYOD) network (T4-06).

Other than the viewing of YouTube videos for educational purposes, very little use of social media and Web 2.0 resources or applications within workplaces was reported. According to T3-12, researchers within T3 frequently used Twitter to disseminate their research. An AHP clinical lead in T4, T4-10, reported that the only information-related use of Trust Twitter feeds there at present was to publicise research. T4-04 reported that professional online forums were often the preferred method of information sharing and professional networking for AHPs. However, T2-02 reported that those of her professional association were not accessible within T1, and in any case use of them would not be encouraged at work.

In terms of different categories of Web 2.0 and social media applications and their availability status within each of the Trusts, the findings are set out in Tables 5.1 and 5.2 below. The categorisation employed of Web 2.0 and social media types is that of Kaplan and Haenlein (2010), which focuses on different types of information content; see above, Section 2.4.1. The findings are discussed further within Chapter 9. It should be noted that some types of Web 2.0 applications relevant to information behaviour, such as social bookmarking (tagging), folksonomies, recommender systems and RSS, were not mentioned specifically by participants.

5.6 Mobile devices

The libraries at T1 and T3 were actively involved in supporting the use of mobile devices for information seeking. A list of medical iPhone apps that had originally been produced by a library assistant based in the acute Trust H12 (locally to the main T3 site) was being maintained by the library staff at T1 (T1-01). They had changed the list to a spreadsheet format, and were now, since they lacked the requisite clinical expertise themselves to review apps, were focusing on including apps that were recommended by university departments or which had received good reviews in journals. They were looking for a national organisation to take over its management. T1-01 mentioned that the Department of Health had recently indicated an intention to create a similar

resource for clinical apps. T3-19, who was unaware of this list before it was mentioned to her by the researcher, stated that she felt it would meet a significant need.⁷⁴

The library at T1 supported both iOS and Android devices (T1-01), there being considerable personal use of Android devices in the Trust. Library staff participated in an iPad online user support forum run by H3. There was a library iPad which had been procured via funding from T2. Library staff had been trained in its basic functions; it was also used by the outreach librarian to conduct training sessions, and for testing apps related to information products. T1-01 anticipated that Trust tablets procured for clinical use might also be used as e-readers.

The library staff at T4 did not mention supporting mobile devices as such. The social media websites maintained by the library, which staff often accessed using mobile devices using the Trust BYOD network, were mentioned above (5.5).

The IT manager P2 suggested to the researcher that use of personal mobile devices, in conjunction with wide availability of 4G and later-generation mobile networks, would in a few years' time entirely resolve problems of access to information for NHS staff. The e-learning specialist T4-22, however, remarked that newer NHS buildings, on account of their energy-efficient manner of construction, often blocked access to mobile networks (Hamblen, 2008; Ofcom, 2014). Installation of signal-boosting devices would therefore be required in future in order for staff to be able to use their own devices.

One participant in T3 (T3-19) stated that her team's Trust-issued mobile phones were "archaic" and did not provide any web browsing facilities. T4-10 stated similarly that the mobile phone she was obliged to use was a "Nokia brick" with very limited functionality. This represents a degree of disempowerment in her work as a clinical manager through the failure to provide her staff with adequate technology to support their work; the discussion of factors relating to staff empowerment and engagement in 2.5.5.3 is thus relevant here.

T1-08 had observed a group of her students (U2) using their mobile phones and tablets to find e-resource to address a task she had given them, rather than (as she had expected) going to the

⁷⁴ A site was later created on NHS Choices for patient apps, but subsequently abandoned.

library, and finding information very quickly: “it was instant access to the information they needed”. Mostly, participants had not observed much use being made of mobile devices for information seeking. T4-08 stated that she had not observed colleagues or students using mobile devices to access educational or professional reference material, nor was she aware of any educational initiatives involving mobile devices. T3-19 reported that she did not use her own iPhone for work-related information-seeking, preferring to use her desktop PC. She was aware of other staff downloading and using the BNF iPhone app. She also expressed her enthusiasm for health apps aimed at patients to provide them with necessary information to manage their conditions. T4-10 reported that, despite shortages of PCs available to students on placement, she was not aware of any students using their own mobile devices to circumvent this. The clinical tutor T3-02 stated that he had observed colleagues in meetings using their own smartphones to look for information, but that it was more usual to use laptops, which could connect to the Trust Wi-Fi in most areas. The BlackBerry devices issued to staff by T3 were not suitable for accessing the Internet, owing to their slowness and small screen size.

5.7 Summary

In summary, this chapter discussed participants’ accounts of barriers to accessing information arising from problems with network access, availability and performance, “legacy” software (operating systems, browser and Java versions), system policies and permissions, and insufficient numbers of PCs in clinical areas. Students on placement, in particular, could be affected by policies relating to network and system access. Access to the BNF was affected particularly by a shortage of PCs in clinical areas, and the lack of an alternative means of access to the most current version. Participants also reported problems with particular national systems: in respect of access to e-learning, relating mainly to limitations in the functionality of the NLMS, and in respect of access to and use of published information, with the functionality of HDAS and OpenAthens, creating potentially serious barriers to effective literature searching and retrieval of full text. They reported experiencing problems with storing, using and sharing information which related to the implementation of requirements to use encrypted portable media, coupled with lack of access to appropriate alternatives in terms of network or cloud storage. They also cited a variety of email-related problems: with webmail, with email attachments, and with spam filter and DLP system false positives.

	T1	T3	T4
Podcasts	Trust was starting to use podcasting on intranet	Sometimes unable to download from web / appear blocked owing to inadequate bandwidth – but podcast content planned for new Trust intranet (T3-21)	Podcasts created by SLTs for ENT training (T4-10)
	Availability of externally-produced podcasts not known	Podcasts produced internally for training purposes (T3-10) and used for PG medical education – but T3-02 mentioned an external one being blocked	Participants unclear about availability of externally-produced podcasts – thought not to be blocked (T4-04)
File storage and sharing applications	Time quota set for use – ‘personal storage’	Not mentioned	Dropbox blocked Google Docs OK
Web conferencing	Skype prohibited and blocked as ‘peer to peer’ application	Skype blocked WebEx, GoToWebinar used	Able to access Elluminate (Blackboard) – used by U9
Start pages / portals	Not mentioned	Not mentioned	Accessible to users - LIS had several Weebly formerly blocked

Table 5.1 Access to Web 2.0 applications

	T1	T3	T4
Blogs / Microblogs	<p>Unable to access or create blogs – prevented library using for current awareness purposes or film club</p> <p>Time quota set for use of Twitter. Trust was starting to use for corporate communications but individual use not encouraged</p>	<p>Restrictions not mentioned on general blogs</p> <p>Twitter, Facebook: users and would-be bloggers should seek advice from Communications before using professionally</p>	<p>WordPress blogs formerly (maybe still) blocked</p> <p>Issuing of Twitter handles required permission from divisional director</p> <p>Twitter blocked by default</p>
Collaborative projects e.g. wikis	Restrictions not mentioned	Restrictions not mentioned	Restrictions not mentioned
Social networking services	<p>Facebook: time quota set for use</p> <p>Originally blocked entirely following breach of confidentiality by clinical staff member and misuse by nurses</p> <p>LinkedIn and other 'professional' sites accessible</p>	<p>Facebook blocked</p> <p>LinkedIn and other 'professional' sites accessible</p>	<p>Access to Facebook etc. blocked on PCs but not on users' mobile devices – Trust has a BYOD network and policy.</p> <p>Some staff approved to use social media for work purposes.</p> <p>LinkedIn and other 'professional' sites accessible</p>
Content communities	<p>Time quota set for use of SlideShare – 'personal storage' category</p> <p>Prezi formerly blocked as presenting possible confidentiality risks – now has time quota set</p> <p>Time quota set for use of YouTube</p>	<p>SlideShare not mentioned</p> <p>Prezi - restrictions not mentioned – IT manager unsure of policy – Communications provides training on use of Prezi</p> <p>Specific permission required to access YouTube on main Trust network - NB bandwidth limitation statement in place – 10s pauses</p> <p>Trust had own YouTube channel; YouTube not available at some outlying sites</p>	<p>Status of SlideShare unclear</p> <p>Prezi blocked</p> <p>YouTube reported as blocked (T4-04, T4-05) but this denied by IT manager – had formerly allowed access to content tagged as 'educational' but now allowed all</p> <p>LIS has Pinterest site – infographics collection</p>

Table 5.2 Access to social media applications

Considerable variation was apparent across the three Trusts in respect of access to Web 2.0 and social media applications commonly considered important as resources for information seeking and sharing. The findings indicated that Web 2.0 applications other than Skype were accessible for the most part. However, certain types of social media content were effectively blocked in two out of the three Trusts: blogs and microblogs (T1, T4) and content communities (T3, T4). Trends in the gradually increasing use of podcasts, and in increasing acceptance of the educational value of YouTube, were observable. However, the restrictions on use of SlideShare and Prezi obviously created problems for sharing content, and are difficult to account for. Further aspects of some of these issues are discussed in subsequent chapters.

Regarding mobile devices, the overall picture was thus one of use predominantly of personal, rather than Trust-issued, mobile devices, with varying levels both of usage and of support. Mobile devices were not being used for information purposes or for e-learning to any great extent.

Chapter 6. Findings: education and training arrangements

6.1 Introduction

Following on from the previous chapter on barriers to information seeking and use in generally, this chapter gives an account of barriers to information seeking and use which related specifically to formal and informal education and training activities undertaken by Trust staff and students on placement, in particular to e-learning, and to their effects. It is in fact largely concerned with issues relating to e-learning and to IT infrastructure, as set out in Figure 6.1.

6.2 IT infrastructure

As reported in Section 1.4.6, a considerable strategic and operational commitment had been made centrally and locally to e-learning within the NHS in England. However, adoption of e-learning by NHS organisations as a means to deliver education and training, and the widespread requirement that e-portfolios be used to record learning activities of whatever kind (T1-04) was perceived by clinical and training staff as tending to increase pressure on already-scarce IT facilities. Inability to access desktop computers on the wards was widely reported. A variety of other problems with computer hardware and networks, which impacted upon the effective delivery of e-learning, were mentioned by participants across all the Trusts. These included lack of webcams and hence inability to support teleconferencing (T1-04); near-obsolete PCs that had a hardware specification that was inadequate to run particular e-learning modules (T1-10); available screen resolutions too low to view the totality of content on screen (T4-22, T2-02); other issues with hardware or peripherals, such as lack of sound cards (T1-06), lack of speakers or headphones; other indeterminate problems with sound (T3-20); and lack of network bandwidth hindering or precluding the download of podcasts (T3-21) or the viewing of video clips (T3-19).

Underlying the “ageing PCs” issue often appeared to be a decentralised approach to the procurement of PCs and peripherals, coupled with local funding pressures; this is discussed further in Section 7.2.2. (The issue, as well as the blocking of websites needed for clinical information seeking, was discussed in a *Guardian* newspaper article by May (2014), who observed that new clinical software was widely expected to run on ageing computer infrastructure that could not adequately support it.) It is pertinent that the T1 IT manager (T1-11) expressed the view that the Trust’s use of Microsoft’s Virtualization Desktop Infrastructure (VDI) (see Section 5.2.2.2 above) permitted older PCs to continue in use; the Trust no longer had an agreed life cycle for PCs.

According to a FoI request response, full implementation of VDI was not expected to be completed until November 2015. T1-11 did not appear to be aware of the problems experienced with inadequate hardware specification, as described by training staff.

In T1, the training officer T1-10 reported that while it had been possible to access the NLMS system from home to undertake e-learning, completing a module did not always register on the system, thus effectively rendering the remote access facility useless. The same problem was reported also by T1-08 in relation to the mandatory learning for nurses. A problem with completed training registering on the NLMS was also reported at T3, requiring the system to be manually overridden. This suggests the possibility that the remote access functionality within the NLMS may have been inherently unstable.

New doctors at T3 were required to undertake a web-based induction programme produced by the local deanery, but hosted externally by a private e-learning provider. During the previous year this had malfunctioned: either some content was not visible when it should have been, or completion of the module did not register (T3-21). It was anticipated that the programme would be abandoned following a merger with another deanery, and that just the Core Skills Framework would be used.

In those Trusts which used the NLMS, new starters who were not yet registered as Trust staff on the Electronic Staff Record (ESR) could not access e-learning which could be required pre-induction. T1-10 was hoping to arrange trial access to an e-learning portal as a possible alternative, and to obviate the non-registration problem described above with remote access.

The “new starters” problem was addressed in T3 by providing a two-day face-to-face induction session conducted by subject matter experts. If a new member of staff missed this for whatever reason, it was difficult to arrange for them to repeat it or to undertake the equivalent e-learning. With Foundation doctors and GP trainees undertaking four-month rotations, this meant that their e-learning could not be undertaken in a timely fashion, potentially affecting the quality of their work; by the time they had caught up with their e-learning requirements for their current rotation, they were often due to undertake their next one (T3-21).

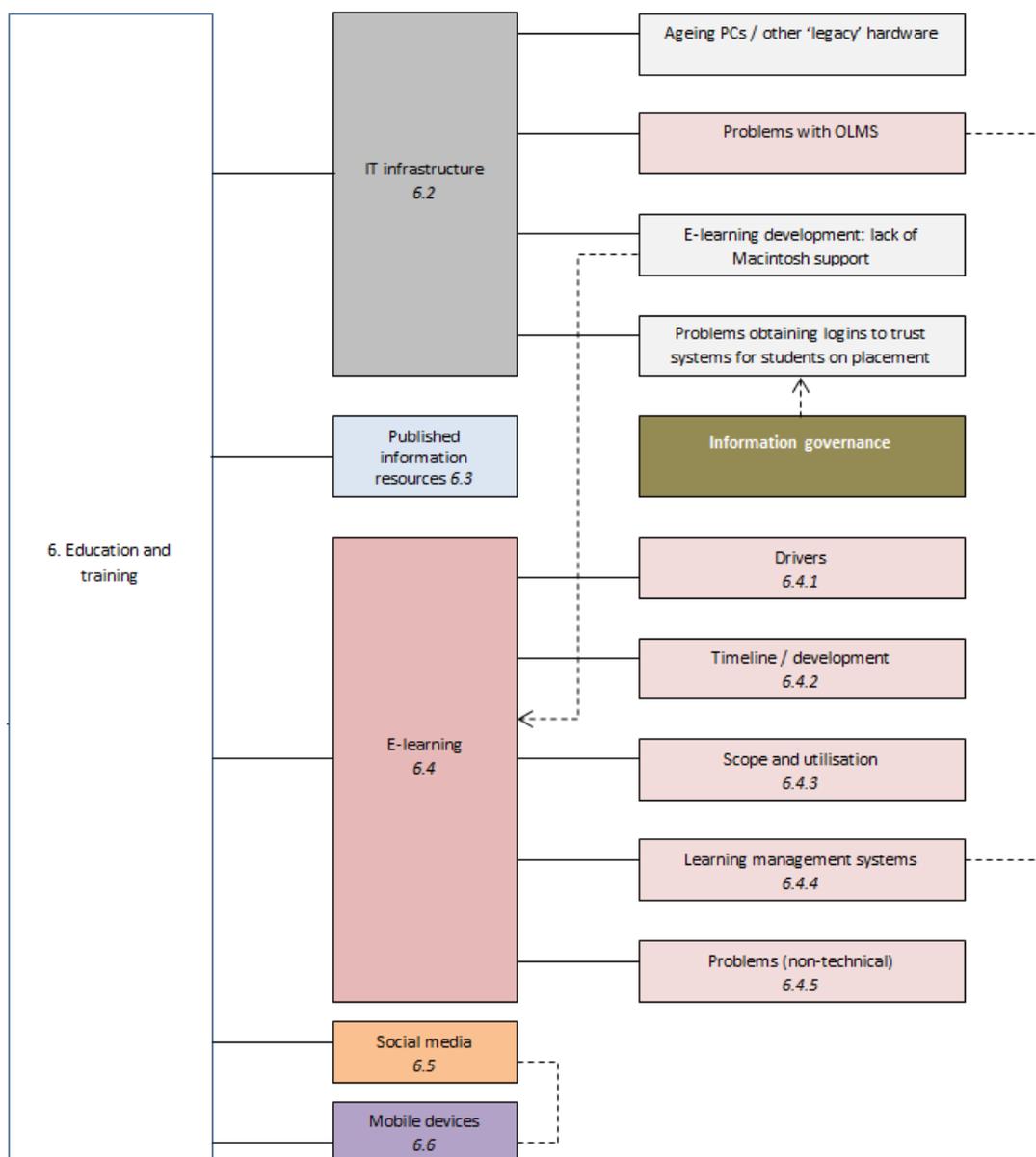


Figure 6.1: Education and training arrangements

T3-10 reported on a specific problem that had arisen two years previously with access to e-learning by community health staff on the outsourced S3 network. They had found that they were unable to run the statutory and mandatory training modules on the NLMS. Support calls had been logged with the S3 helpdesk but not acted upon. They were also finding that their learning activity was not being accurately recorded on the NLMS, and that in addition there were issues associated with the smartcards they were using to log on to the application. These persistent problems had led to a breakdown of trust with S3 and disengagement from e-learning on the part of these staff. The training department at T3 had then launched an investigation: a small working party consisting of a

representative from HR (on account of the smartcards issue), a training officer (T3-10 herself) and the senior analyst from the IT department (T3-17) visited each of the members of staff who had reported the problems. It was found that the main problem related to incorrect versions of Java on their PCs. Staff at S3 had apparently lacked understanding of their role as to the technical requirements of supporting e-learning, and were not acting on the calls they had received; they had instead disclaimed responsibility entirely, assuming that the issue lay with McKesson, the NLMS vendor.⁷⁵ McKesson for its part had insisted on there being only two nominated contacts from each Trust, an arrangement which was deemed unsatisfactory by T3-17. The lack of response from S3 had led to issues “festering” (T3-10); staff in T3-WPH had not been reporting to the training department the problems they were experiencing. Another technical problem was that the online system checker provided by McKesson to check the specification of users’ PCs, including the Java version they were currently running, was not working correctly under Windows 7; in particular, it was not correctly detecting the Java installation.⁷⁶ T3-17 was subsequently able to liaise with S3 to ensure that the Java version on these PCs was updated. To avoid the need for individual *ad hoc* updates, T3-17 was hoping to manage Java updates centrally on the main T3 network via Configuration Manager. According to the e-learning officer T3-05, any changes to system requirements would normally have been notified by McKesson to their contact in the Trust, who would then have passed the information on to the IT department for the changes to be rolled out remotely on Trust PCs. This at least was the process for the main network at T3. However T3-10 reported that sometimes this information was not sent in time by McKesson, and training and IT staff were alerted to the required changes only by users reporting the inability to run a particular e-learning module. In December 2014 a new contract for the Electronic Staff Record and OLMS was awarded not to McKesson but to IBM, to take effect from November 2015 (Meek, 2015c).

An issue relating specifically to e-learning development was reported by T4-22 at interview and in subsequent correspondence. Microsoft Windows operating systems (Windows XP, Windows 7, and Windows 8) were generally used within the NHS for PCs and laptops. NHS IT departments, therefore, did not support Apple Macintosh computers, which constituted a severe limitation for e-learning development, for which the Macintosh platform was widely used.

⁷⁵ McKesson: <http://www.mckesson.co.uk/>

⁷⁶ ESR online system checker: <http://www.esrsupport.co.uk/nlms/pccheck.html>

Specific issues encountered by T4-22 included the following:

- Many e-learning developers were setting up Macintosh-based systems covertly, but then could not register equipment or update software
- One manikin that T4-22's own centre had used was solely Macintosh-compatible until recently
- A considerable number of centres had invested in a specific software video performance analysis product that required an entire Macintosh system (multiple computers, servers, local area network (LAN) with Wi-Fi interconnection)

More generally, T4-22 had encountered the following problems with supporting Mac OS or iOS-based devices:

- Difficulty in accessing sites such as iTunes and the App Store via NHS IT; access was required regularly for software upgrades
- Inability to download and install programs or applications without extensive discussion or negotiations with IT
- Difficulty in arranging access to systems for users external to the Trust
- General lack of knowledge about or interest in Macintosh-based systems

This lack of support for the Macintosh platform has evident implications for e-learning development in NHS contexts; it was likely to be acting as a severe constraint, resulting probably in a need for outsourcing arrangements and their attendant costs.

Unusually, given the standard restrictions on end-users' downloading and installing software themselves, T4-22 had been able to download and install Dropbox⁷⁷ on to a laptop supplied to him by the IT department, on which he had found he had administrator rights. He was convinced that this was due to an oversight, but was not intending to advertise the fact!

The issues discussed in 5.2.2 with regard to generic logins also bore upon professional education. Where students were unable to obtain appropriate logins to Trust systems during their placements,

⁷⁷ Dropbox: <https://www.dropbox.com/>

their learning could be hindered. In T1, medical students on placement, who were issued by their university (U3) with iPads, connected not to the Trust network but to the postgraduate centre's own Wi-Fi network (T1-01). Wi-Fi connectivity within the students' residences was relatively poor, so many of them were coming into the library and using the computer suite there, which was otherwise little used (T1-06). According to T1-06, medical students' use of network facilities from within the students' residences for educational purposes had occasioned disputes with the IT department, which had claimed that they were downloading films.

A confusing situation appeared to prevail regarding the availability of Trust network logins to nursing students at T1. AHP students were reported as being able to obtain logins to the Trust network on the same basis as AHP staff (T2-01). Integrated governance had previously stated that nursing students were "temporary" staff and should not be given logins. This policy had now been reviewed; it had been agreed that nursing students should, after all, be given logins, but this decision did not seem to have been implemented.

T2-01 perceived the IT department's concerns as relating to "security of information and what you can access", rather than to training. Nursing staff were unwilling, in view of information governance prohibitions on sharing passwords, to share logins with students. In consequence, nursing students on placement in T1 were able to access the Trust intranet only within the library (where staff could log them on to the Trust network), not on the wards (T1-08).

The IT manager (T1-11) for his part indicated that he was not aware of specific training requirements for these students, although he stated that "they ought to have training before they are given access." In T4, generic logins could be issued by most of the wards, although the library service did not do this (T4-20). AHP students at T4 were able to use Trust PCs, but were driven to undertake much of their information seeking at home owing to the lack of available machines at work (T4-10). Students on placement within T4 were not able to log in to clinical systems; their tutors logged in for them to enable them to access specific content under supervision (T4-08). T4-08 spoke of the importance of students on placement at T4 having access to the EPR system once it had been implemented in order for them to learn to document care correctly. Medical students at T3 were reported to have read-only access to the Trust's EPR system (T3-21). Rather than their connecting to the Trust network, T3-06 would have liked to be able to provide access for students and teachers to

the academic wireless network, eduroam, but at the time of the study it had only been deployed within large single-site teaching hospital Trusts.⁷⁸

On account of T3's physical health services being outsourced and on a different network from the rest of the Trust, a portal had had to be set up enable staff within these services to access T3's e-learning (T3-09). However, T3 training staff were expecting e-learning to be available to staff much more readily than was then possible through the new Hadron intranet being implemented within the Trust (see Section 4.2.3).

T1 was hoping to be able to find the funding to set up a virtual learning environment using SharePoint through which to access e-learning; this was to replace the NLMS, the search facilities of which were perceived as decidedly lacking (T1-05, T1-10).

6.3 Published information resources

As with the other Trust library services, T3-LIS provided individual information literacy support to staff for their studies, as reported by the non-clinical teacher T3-04.

Within all three Trusts there were close links between education and training functions and library and information services. The library at T1 had been involved in supporting junior doctors' e-learning for some time before it had been decided to introduce e-learning widely across the Trust. It had facilitated online examinations in orthopaedics via its university computer suite, made its NHS computer suite available for trainer-led e-learning sessions for groups of staff with information literacy difficulties, and provided access to an e-learning authoring software package for trainers to use in creating their own e-learning material. Formerly, members of library staff had themselves facilitated e-learning sessions, but they had not needed to do so recently; they preferred subject experts to facilitate (T1-01). The library's computer facilities were also regularly used by medical students to access e-learning (T1-06). Library staff had a close working relationship with the postgraduate centre, with which it was co-located; each service was represented at the other's business meetings, and the library worked with the centre manager to produce lists of e-learning resources pertaining to the topics of educational sessions held at the centre (T1-06). Similarly the library at T4 provided computer facilities for students when none was available within the clinical area, and assisted students with accessing e-resources, ran training sessions on literature searching,

⁷⁸ A list of all eduroam participants was given at <https://www.ja.net/products-services/janet-connect/eduroam/eduroam-participating>

and provided staff and students with one-to-one information literacy training and support, which staff undertaking post-registration courses at universities found particularly helpful (T4-08).

T3-LIS appeared to work more closely with the Trust's training department than was the case elsewhere. The library frequently shared a stall with training at internal events, jointly promoting education and learning opportunities (T3-07). Sometimes the library manager was able to give a brief presentation to remind staff of the role of the library in supporting not only professional learning within the context of formal study, but also patient care. Promotional material about T3-LIS's resources and facilities was available in the Trust's computer centres.

6.4 E-learning

6.4.1 Drivers for the growth of e-learning

Local drivers for the growth of e-learning were observable mostly in T1, as the Trust's Learning and Development Department was about to roll out e-learning there. They included poor take-up of day release for training (T1), a need for more flexibility in the provision of training, coupled with the perceived poor quality of face-to-face training (T4), and lack of motivation on the part of staff to undertake training (T1) (T1-10; T4-01). As against this, T1-04 had felt that updating of mandatory and statutory e-learning in line with frequently-changing Trust policies was perceived as involving a heavy burden for the training department, and that this had led its introduction to be delayed. T1-10 and T1-05 reported that time was indeed an issue, and moreover that the introduction of e-learning had required a re-negotiation of the subject matter experts' role:

"Initially when we first proposed this a few years ago ... I think there was quite a lot of hostility from the subject matter experts, although ... they are nearly all on board with it now, because they can see that actually it will release their time, whereas I think before it was perceived as taking [over their role], and that's been a big step change." (T1-10)

6.4.2 Timeline and development of e-learning within each Trust

In T3 and T4, the use of e-learning for the delivery of training was reported to be well-established, and was referred to within T3's mandatory training policy. E-learning in T4 had started in 2009 (T4-01). T3 was described as having a "really strong culture of e-learning" (T3-09). (Nationally, mental health Trusts had frequently been early adopters of e-learning; with their typically wide geographical spread and large numbers of sites, it offered obvious advantages.) E-learning was only just starting in T1, beginning with statutory and mandatory training (T1-10).

The issue was raised by participants of “bought-in” versus “home-made”. T3-07 had been involved in an e-learning authoring project, and felt as a result that producing e-learning within the Trust was too time-consuming; purchasing it externally was a better alternative. The e-learning team at T4 reported that they did not have the capacity to work with clinicians to develop clinical e-learning packages. As a result, clinical e-learning in T4 was generally produced by external developers (e.g. T4-10, T4-05; cf. T4-22’s observations in 6.2 above about lack of technical support for e-learning development).

All the Trusts employed an in-house developer using e-learning authoring software to produce customised e-learning content to meet some mandatory and statutory training requirements in consultation with subject matter experts. Many professional bodies had produced extensive e-learning content available to their members; it was possible for Trusts to use this for mandatory clinical training. Other e-learning content was produced by universities (e.g. U3-Pharm for pharmacists). Otherwise, clinical e-learning could be commissioned from external providers for particular purposes (e.g. T4-05).

The sharing of e-learning between NHS organisations was viewed as being very desirable in avoiding duplication of effort (T4-12). Some degree of customisation was thought to be required, however, for each Trust, to reflect particular localities and Trust policies. However, T4-08 also felt that Trusts needed to have e-learning branded as “theirs”:

6.4.3 Scope and utilisation of e-learning

E-learning was being used extensively within two of the Trusts in the study (T3 and T4) for clinical and non-clinical mandatory and statutory training, particularly at induction. T4-19 indeed complained of “e-learning overwhelm” for doctors. T1 was just about to roll out the use of e-learning for this purpose. E-learning was also used within all the Trusts to support other professional learning, although this varied in extent by profession. Nursing (T4-05, T3-07, T3-20), and pharmacy (T4-04) participants reported past or expected involvement as subject matter experts in the creation of e-learning packages. Blended learning was preferred in T4 for physiotherapy training, as providing better coverage of practical issues and the benefits of face-to-face discussion (T4-08), and was reported as being used successfully for radiography training (T4-12). Dieticians in T2 were making very little use of e-learning (T2-02). The Chartered Society of Physiotherapy had not produced any e-learning, but had created an online portfolio for members to log their auditable professional development activities (T2-03).

6.4.4 Learning management systems

T3 made use of the National Learning Management System (NLMS) which was part of the Electronic Staff Record (ESR) system.⁷⁹ Mention has already been made of the T1 trial of a possible alternative hosting platform and LMS (6.2). For reasons likely to be related to the known usability problems of the NLMS interface (Clarke, 2006), a decision had been taken at T4 at the time e-learning was introduced there to implement a Moodle-based LMS instead. (Moodle is an extensively customisable open-source learning management system widely used across the world to support e-learning.)⁸⁰ The training department retained the services of a Moodle developer and system administrator. This offered a significant advantage in managing induction training, in that it allowed e-learning modules required as part of induction to be undertaken by new starters, in particular junior doctors, before their official start date; in Trusts where the NLMS was used, a new starter could not have an account, because, on the ESR system, they still had “applicant” status until they officially began work. At T3, this meant that junior doctors’ induction training still needed to be delivered face-to-face for two days rather than online (T3-21).

6.4.5 Non-technical problems with e-learning

E-learning “overwhelm” has already been mentioned (6.4.3), as has the difficulty of updating e-learning in a timely fashion to reflect changes in Trust policies (6.4.1). Other organisational (as distinct from technical) problems with e-learning were reported by participants.

T1-04 mentored students taking e-learning courses provided by three different universities, two of whom used the Blackboard LMS. One university gave her access to their Blackboard, but the other did not, meaning that she could not see what her students were supposed to be studying.

T4-22 mentioned the poor computer literacy levels that he had repeatedly encountered within the NHS in the course of his career. He suggested that this, and associated negative attitudes and low expectations, were part of an overall picture, which affected e-learning, of under-resourcing and under-development of information technology infrastructure and service provision within the NHS relative to other sectors. This issue is discussed further in Section 11.3.

⁷⁹ NLMS: <http://www.esrsupport.co.uk/nlms/index.html>

⁸⁰ Moodle: <https://moodle.org/>. The name is an acronym for *Modular Object-Oriented Dynamic Learning Environment*

6.5 Web 2.0 and social media

Use of Web 2.0 and social media applications and resources for education and training purposes was seldom discussed by any of the participants. The e-learning specialist T4-22 reported using Twitter as a main communication tool with other e-learning and simulation specialists. Educationalists were not aware of social media use by students for educational purposes, such as Facebook study groups. The only possible exception to this was the Facebook group referred to by the clinical teacher T1-08, who mentioned the use of one by a group of her students to disseminate information about changes to the teaching timetable. This was not, of course, something to which she as a lecturer had access, so she was not placed to comment on its content or about how the group was being used by the students concerned. Podcasts were available in principle to download at T3, but low bandwidth limited this in practice (T3-12). Use of podcasts for medical education, to be accessible via the new Trust intranet, was planned at T3 (T3-21).

Mandatory and statutory e-learning provided by Trusts did not make any use of social media, or of Web 2.0 platforms such as wikis. Also, in addition, participants had not encountered them in any other e-learning contexts. The only exception was that of accessing and using YouTube videos (e.g. the clinical teacher T3-19). This participant encountered jerkiness and buffering delays in viewing YouTube, suggestive of insufficient bandwidth. The researcher discovered subsequently that, in some instances, this could actually have resulted from explicit network management policies: the Trust IT manager (T3-06) spoke of a bandwidth limitation statement in place on the main Trust network, which introduced ten-second pauses into the viewing of video clips. (It is possible, however, that T3-19 was referring in some instances to availability of YouTube on the outsourced network supported by S3.) T3-19 had also encountered problems obtaining permissions to access YouTube content when presenting at training sites, and felt frustrated and demeaned by the need to do so:

“Yes. If you are doing a presentation or something within ... L&D you actually have to get special permissions to, say you wanted to use a ... YouTube clip ... or whatever, and some of them are very good, or even something simple like NHS -- ... like the other day I was doing something on immunisations and there is some quite good very simple little animated films ... so it’s not easy; it is putting another barrier and a step that ... increases your frustration really ... So what sometimes you do is -- you do it at home, so you put presentations, you put the links on and then when you come into like the L&D department you get, you will be OK to ... use that and then they have to do it, they have to ring up and get the access and whatever and you are allowed to, but again, let’s face it, we are professionals, you know, we are not going to be, you know, doing any illicit sort of, well ...” (Clinical teacher, T3, 19)

The library and the education department at T4 maintained Twitter feeds; however, some of the education department content consisted of re-tweets of material from other Trust services. T4-22 reported using Twitter in addition to email as a primary means of communication with e-learning specialists within the region and with his wider professional network.

Several indications were expressed of a need for advice and guidance on the professional use of social media. These all came from AHP clinical leads: T4-10’s suggestion of partnering with the Trust library regarding social media use; T2-02’s reporting that junior dietetics staff had expressed an interest in receiving training on professional use of social media; and T4-08’s uncertainty about how to use professional and personal Twitter accounts simultaneously.

6.6 Mobile devices

All Trusts in the study had U3-Med students on placement. U3-Med at the time was one of several medical schools in England where students were given iPads and expected to use them as fully as possible to support their clinical learning throughout their studies, requiring that Wi-Fi networks be available at the sites where they were based. The academic lead for e-learning at U3-Med (U3-Med-1) had reported no particular technical problems with students’ network access on any teaching sites, including T1, where they connected to the postgraduate centre’s wireless network. The project manager had apparently worked closely with Trust IT managers to ensure that Wi-Fi was in place at the relevant hospital sites and was accessible to students. T1-01 and T1-06 were, however, aware of problems with Wi-Fi connectivity in the residences at T1-LH (see also T1-06’s comment on this, reported in Section 6.2). The eduroam installation at T4 was referred to above (Section 4.4.3). According to T4-11, Wi-Fi was only then in the process of being installed in the education centre; he

was unclear, however, which network this was, *i.e.*, the main Trust Wi-Fi, the BYOD Wi-Fi or eduroam.

To support mandatory and statutory e-learning in T1, the training department had successfully submitted a bid to a Local Education and Training Board (LETB) learning infrastructure fund, and had procured six “rugged” Android tablets. Once e-learning had properly started, these were planned to be taken on the wards to allow staff to access e-learning within clinical areas via the Trust Wi-Fi network. These were supplied by the company Motion⁸¹ and were designed to minimise infection control risks; they had a completely flat-topped surface that could be readily disinfected. The intention of staff in the department was to use them as part of a mobile classroom that could be conducted within a day room on a ward. T1’s content used Adobe Flash, hence could not be accessed via Apple devices (Bristol, 2013; Brusco, 2011; Shankland, 2010). In addition to these devices, T1-07 indicated that some educational use was expected in the future of tablets provided for purposes of clinical record keeping; the Trust had submitted a bid in the second round of the Nursing Technology Fund⁸² for tablets on which to record clinical observations. A similar bid had been submitted by T2, for the use of 7” rugged iPads (T2-01).

In pre-registration nursing and midwifery education at T1, T1-08 reported that tablets were used by some the faculty members at U2 who were involved in supporting students working in private sector (*i.e.* non-NHS) academic placement areas, although none had yet been seen at T1-LH. In postgraduate medical education, T1-06 reported that many doctors were accessing learning resources via their own tablets. The difficulty they were having, she said, was not in getting access to e-resources as such, but in finding time to use them. The issue of insufficient time was raised also by T1-07 in respect of nurses. T1-04 reported that mobile devices were not routinely used in post-registration pharmacy education, although one student had needed to participate in a videoconference while sitting in her car using her iPhone on account of the lack of suitable PC facilities, including lack of webcams, within the department. Webinars were apparently being more commonly used by their education provider U3-2, where the staff conducting them were aware of the problems that students were likely to encounter with NHS IT, and were accordingly scheduling them in the evenings for students to access from home.

⁸¹ Motion: <https://www.motioncomputing.com/uk/products>

⁸² Nursing Technology Fund: <https://www.england.nhs.uk/digitaltechnology/info-revolution/nursing-technology-fund/>

T3-06 aspired to roll out eduroam (the national academic wireless network) across the Trust to support student placements of all kinds. However, he had found that no precedents existed for multi-site Trusts; existing NHS implementations of eduroam were on acute hospital sites.⁸³ T3-05 was aware of a project conducted by an e-learning specialist in another Trust (E15) to identify which tablets could be used to access content via the NLMS. Apparently in T3 very few staff had tablets; mostly they accessed e-learning via a Trust laptop or via a personal laptop using the trust virtual private network (VPN) connection and a remote access authentication token; such tokens were readily available to staff (T3-10, T3-06).

T4-01 reported that staff were accessing Trust e-learning content via their personal Android devices. However, the resources were not accessible on iPads or iPhones on account of the Adobe Flash issue with Apple devices (mentioned above, this section). The training department was investigating the possibility of a move to using HTML5 in future as the platform for their own e-learning content to obviate this problem. Use of mobile devices seemed to be well-embedded in pharmacy teaching; T4-04 taught medical students and other students who had their own mobile devices, using the NearPod⁸⁴ system to synchronise her own device with the students' devices rather than presenting on a screen. Students were able to interact with the content, e.g. type things on screen and submit them to the lecturer. In the context of physiotherapy education, however, T4-08 was not aware of any educational use of mobile devices.

Accessibility of e-learning content via mobile devices and platforms, including full learning management system functionality, had been identified as an essential system enhancement to the NLMS to be provided under the new ESR contract planned to take effect in November 2015 (NHS Electronic Staff Record Programme, 2014).

6.7 Summary

This chapter relates how e-learning was firmly established at T3 and T4, but only just starting at T1, affording the opportunity to investigate the early stages of implementation. T3 and T4 had adopted different approaches to circumventing the technical limitations of the then-current version of the National Learning Management System (NLMS). The account of technical problems with access to e-learning within T3's community health services illustrates the difficulties of supporting NHS e-

⁸³ eduroam: <https://www.ja.net/products-services/janet-connect/eduroam/eduroam-participating>

⁸⁴ NearPod: <https://nearpod.com/>

learning within an outsourced environment. Across all three Trusts, e-learning software compatibility issues with “legacy” PC hardware presented problems, despite extensive virtualisation across network environments (*cf.* Section 6.2 above). Lack of support for the Macintosh platform, as well as lack of staff capacity within training departments, served to inhibit the in-house development of e-learning; much of the more specialist work was being outsourced, with evident cost implications. Little evidence emerged of specific organisational factors underlying these problems.

Much e-learning content available to NHS staff, and all of the mandatory and statutory training material, was accessible via the National Learning Management System (NLMS) within each Trust, and was well supported. However, a number of issues were identified with the functionality of the NLMS, in particular the inability to provide access to it for new starters, thereby preventing e-learning being delivered to them in a timely fashion, i.e. before starting in post. A slowly increasing trend towards usage of podcasting and YouTube videos for educational purposes was apparent, despite technical and policy barriers. Other e-learning material of potential professional relevance was little mentioned by interview participants.

A steady growth in usage of mobile devices for educational purposes was apparent across all three Trusts, secondary in some instances to their use within clinical systems. In T1, tablet computers had been purchased specifically for e-learning purposes. However, lack of adequate Wi-Fi network coverage could present an obstacle to this. The general issue of Wi-Fi provision on NHS sites is discussed further in Sections 1.4.3 and 12.8.

The following chapter (Chapter 7) goes on to look at issues for information access presented by organisational dynamics and aspects of professional culture.

Chapter 7. Findings: organisational dynamics and professional cultures

7.1 Introduction

Following on from Chapter 5, which focused on the specifics of barriers to information seeking and use in general, and Chapter 6, which focused on barriers to education and training, this chapter focuses on national policy priorities and their implementation, and on regulatory concerns, as a means of identifying organisational dynamics within each individual Trust and the influences of professional cultures. References to some of these issues were made by participants, but were not described in detail. It also discusses the inter-relationships and mutual perceptions of the various services, including patterns of communication and collaborative working. In particular it highlights instances of apparent misinformation or misunderstanding, and long-standing unresolved issues. In addition it identifies staff attitudes, professional norms and wider cultural issues relating to the overall focus of the inquiry. It is concerned principally with IT infrastructure and how it managed, and with cultures, behaviours and attitudes relating to information technology use in general and to e-learning in particular. The content coverage is illustrated in Figure 7.1.

7.2 IT infrastructure

7.2.1 IT strategies Interview participants within IT, library and information services and training and development were asked about inputs to information technology strategy within their respective Trusts. T1-01 informed the researcher that the Director of Nursing had successfully lobbied “at the last minute” for her to be represented on the intranet planning group; this was the only input of which she was aware. The IT manager at T3 received input into IT strategic planning via the locality management teams; he or a colleague would represent the IT department at their periodic meetings. For the Trust’s two clinical systems there were user groups which were a key channel of communication with the IT department. For training and development the IT trainer, who was based within the IT department, provided feedback on IT issues arising with training (T3-06), although there was no explicit training and development or library input into the IT agenda. T3-06 was not apparently aware that the training department employed an in-house e-learning developer. T3’s implementation of a new Hadron intranet has been discussed previously (4.3.2). According to T3-19, a “Dragon’s Den” process existed within T3 for vetting, approving and funding proposed e-resources projects relating to patient information.

At T4, Department Information Groups had been established for each of the major hospital sites and for community services. A business analyst from the IT department was attached to each of these groups. At the group meetings, the business analysts had an opportunity to meet clinicians and to discuss new projects, issues with existing projects, issues with existing clinical systems, etc. (T4-20). No mention was made, however, of library or education input.

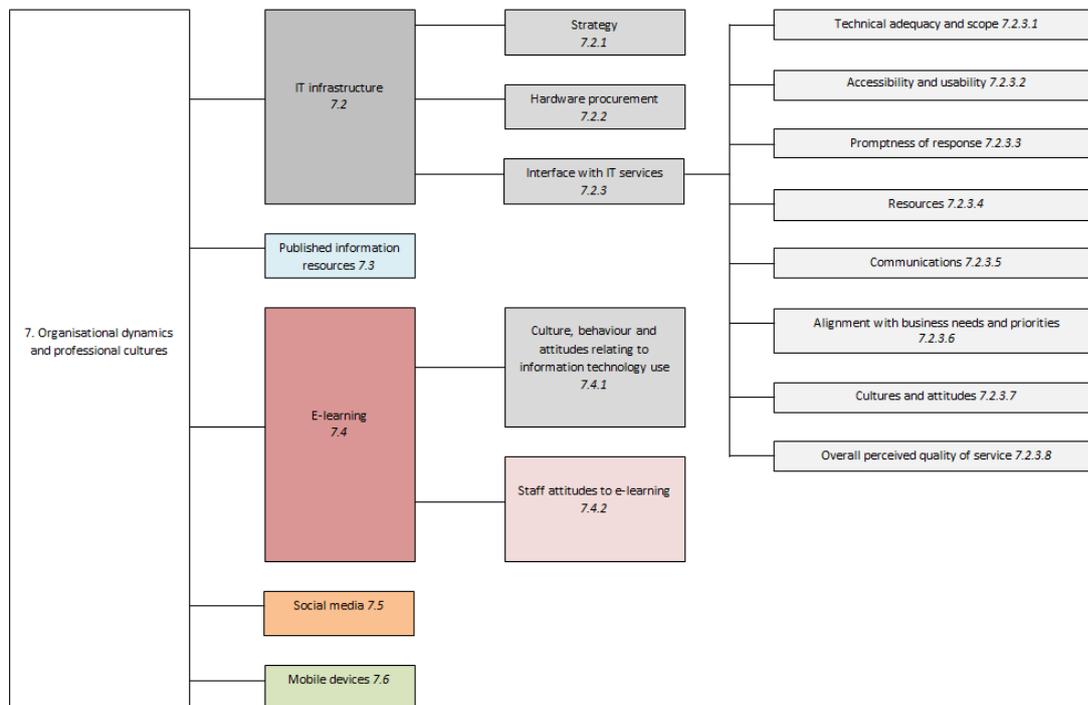


Figure 7.1 Organisational dynamics and professional cultures

7.2.2 Procurement of hardware

Participants in all three Trusts complained of the age of the computer hardware they were expected to use. T2-01, who was based on a T1 site, reported a recent conversation with a colleague as follows:

“... We ... have IT systems that we expect to last for ... ever and a day, you know; I was talking yesterday and someone was saying, ‘Oh, all the computers that we have got are at least 10 years old, you would think someone must be winding them up at the back nearly’”. (AHP clinical lead, T2, 1)

A medical education administrator (T3-21) described the PCs in her department as “ancient”. In 2013, the IT department at T3 had engaged a contractor to carry out an audit of PC specifications,

reporting back on which machines needed upgrading and which could not be upgraded and needed to be replaced (T3-10); what the upshot of this exercise had been, she was not sure.

Within all three Trusts, there was no ring-fenced funding for procurement of IT hardware and peripherals; central funding for upgrading or replacing PCs was associated only with specific projects, such as migration from Windows XP (T4); otherwise, local budget holders were responsible for meeting these costs in line with IT service standards and recommendations (T1-11). At T1, T1-04 reported difficulty in procuring and installing a new PC, particularly in relation to identifying funding. T4-10 reported a similar experience at T4, which had required her to continue using a “condemned” (i.e. officially obsolete) PC for some months. The IT manager in T3 reported that he could only recommend, not insist, that a service replaced an obsolete machine (T3-06). In T2, PC upgrades and replacements were provided by the outsourced provider S3 as part of their contract with the Trust, and were not controlled by the individual services: PCs were replaced when deemed irreparable or obsolete (T2-02). T4-10 reported an acute shortage of PCs in her department following a move; only two were available, whereas, in her opinion, five were needed, requiring her and her colleagues to share access to PCs and to hot-desk. The most recent CQC inspection at T4, published while the study was being written up, had identified a number of problems with the EPR and human resources systems and with patient records in some services.

In these situations the importance of providing staff with sufficient PCs of adequate specification and performance appeared to be insufficiently recognised by budget holders among other service priorities. Elsewhere within therapy services, the situation appeared to be better: another AHP clinical lead had concurred with the researcher’s suggestion that desktop hardware was “reasonably current” (T4-08). A radiographer in T4 reported that, within her service, the business manager readily agreed to the upgrading or replacement of PCs when necessary, to support the requirements of the PACS and CRIS systems (Picture Archiving and Communications System; Computer Radiology Information System) which were central to its clinical work.

7.2.3 Organisational interface with IT services

7.2.3.1 Introduction

It is intuitively evident that good IT support is required to facilitate online information seeking and use of all types. This section discusses how IT services related to and were perceived by end-users and to other departments within their respective Trusts. The focus here was on seven related but distinct aspects of their perceived quality and character that could affect access to information

services and resources: technical adequacy and scope of the service, accessibility and usability; promptness of response to support calls, character of communications, adequacy of resourcing, alignment with business needs and priorities, and general attitudes towards end-users, both of managers and staff.

7.2.3.2 Perceived technical adequacy and scope

The IT helpdesk at T4 had failed to resolve a persistent problem with the installation of an updated version of Adobe Flash Player, which IT had failed to resolve, resulting in considerable frustration. T1-01 reported that the T1 IT department was good with “quick fixes”. T4-22’s account of the T4 IT department’s unwillingness or inability to support a Macintosh e-learning development environment was noted above (6.2).

7.2.3.3 Perceived accessibility and usability

All the IT services were able to access user PCs remotely from the helpdesk, which was much appreciated by users. Incidentally, within T3 the library service was also able to use the same remote access facility DameWare (SolarWinds),⁸⁵ as the T3 IT department, as a means to provide user support. T3 IT staff were also able to use an online chat facility for resolving support issues (T3-20). None of the helpdesks had a web interface, i.e. for users to enter and monitor the progress of support calls; contact with helpdesks was via telephone or email in all cases.

T1-04 complained that communications with the IT helpdesk at T1 were cumbersome, i.e. that it was difficult to get to speak to anyone and an excessive number of emails were generated in relation to individual support calls. T2-03 complained of the slowness and impracticality of the process in logging support calls with S3, which involved a telephone queueing system, compared with the ease of contacting T1’s IT service.

These problems and other negative experiences of the interface with IT support would have contributed to time pressures and stresses in the working environment, and were likely to have engendered a reluctance to initiate support calls. In terms of the job demands–resources model of Demerouti *et al.* (2.5.5.3) they could be categorised as a “hindrance demand”. They are similar in

⁸⁵ DameWare: <http://www.dameware.com/>

nature to the “overhead” created by website blocking, as discussed in Section 11.3.2 and represented in Figure 11.2.

7.2.3.4 Timeliness of response

No explicit references were made by participants to IT department standards for responding to support calls. T4’s IT department was reported as being very prompt at remote updating of software (T4-08). Other than this, the only comments made by participants relating to timeliness of response related to clinical systems. T3-19 herself had found S3, the outsourced IT service provider for T3’s community health division, “really helpful” in her contacts with them. However, she mentioned that some of her colleagues felt that S3 had been tardy in resolving problems with the C2 clinical system, even minor issues related to user logins, thereby creating delays in data input and hence a clinical risk. A group of C2 “champions” had been established as a channel through which to resolve support issues. Another potential clinical risk relating to perceived slow response on the part of the same outsourced IT service to a problem with supporting supplies for tube feeding was described by T2-02. That such delays were occurring even with clinical system support, which was perceived to be a higher priority (see Section 7.2.3.5 below), seemed to indicate the existence of serious resource constraints, which would have been likely also to affect support for information seeking and use.

7.2.3.5 IT department resources

T1-08 expressed the view that, although the IT service at T1 was good, and indeed had improved over the last few years, it was under-resourced and struggling with inadequate infrastructure:

“Yes, I think they are dealing within restricted ... resources in terms of staff, in terms of ... the quality of the technological equipment they are using and perhaps the systems that they are working with. The software that they are working with as well – sometimes ... I think they do their best with what they have got to manage with.” (Clinical teacher, T1, 8)

T1-02 expressed a similar view, noting the lack of resources available for IT outside clinical departments. Similarly, the IT department at T4 was felt to be significantly under-resourced in relation to demand:

“And again, you know, it’s- it is not a department that is awash with staff ... We are a huge institute, [number of staff] people, goodness knows how many PCs and how many miles of cabling ... I think ... it is probably too much for them.” (Consultant surgeon, T4, 19)

7.2.3.6 Perceived quality of communications

Good communications and working relationships are an essential aspect of effective IT support. However, perceived communication inadequacies on the part of IT services featured strongly as a theme within T1 and T4. The librarian at T1 (T1-01) reported that the Head of IT Services in T1 habitually failed to respond to communications, although other members of IT staff were felt to be more positive towards the library and its service objectives. T1-02 also indicated that the Head of IT Services could be unresponsive. T1-11 was seemingly unaware that the library had computers that were on the Trust network. T4-22 stated that his only available contact with the IT department had been via a call handler at the helpdesk; he had never succeeded in speaking to an IT manager about the specific needs of his service. T4-09 reported that contact with the IT department regarding information governance-related matters was minimal, despite their physical contiguity.

7.2.3.7 Perceived alignment with service business needs and priorities

To provide an effective service, an IT department needs to be well aligned with the business needs and priorities of its internal customers; to support access to published information, the alignment needs to be with LIS and with education and training services (Beagle, 1999). T1-01 spoke of a situation where a perceived lack of alignment of priorities had thwarted the provision of a long-desired and much-needed service, namely the provision of printing facilities out of hours. The administration of printing and photocopying in the Trust was centralised, and IT had refused the library permission to make use of a possible sub-control option afforded by the software. T1-01 had subsequently identified another possible option, which had been approved by IT; unfortunately she was then threatened with loss of the funding from U2 which was required for this, and was unable to go ahead with placing an order for the system. The issue of out of hours printing within the library had apparently remained unresolved for 10 years, restricting use of library facilities for staff working shifts.

7.2.3.8 Perceived cultures and attitudes

The formation of effective working relationships has a strong attitudinal component; it is hindered by prejudices and negative attitudes, whether on the part of service providers or of customers.

T4-22 was of the opinion that clinical services generally were a much higher priority for T4's IT department than education services, a view in which T4-11 strongly concurred. In T3, in contrast, the main education and training services were thought to be well supported. In particular, according to

T3-04, IT staff had been willing to come out to provide training and support for the upgrade to Microsoft Office 2010.

A clinical tutor at T1 hinted that, in her experience, IT management culture within the NHS was liable to engender restrictive or negative attitudes to end-users as compared with other sectors:

“It very much depends on who happens to be [pause] in charge and ... also where they have come from ((laughs)). Sometimes it is ... where they have come from ... Ones that have been in the NHS the whole way up can be quite... ((laughs))” (Clinical tutor, T1, 6)

T4-10 had encountered an intractable problem with three iPads which had been paid for by a charity to use within a clinical service:

“Do you know, it has taken probably 18 months to even get them remotely functioning. To actually ... it’s been, I felt like giving them back; the challenge IT wise to get anything functional with those iPads ... has been most horrendous ... just ... actually getting them [set up] on ... any service ... We don’t have a relationship with Apple, we had -- people had given us vouchers to download apps but we couldn’t use them, we can’t access ... the Internet, we can’t go on-line and ... we couldn’t get them set up, and then using them has been a tremendous hurdle, an obstacle to -- I think we are finally there, but it has taken...”
(AHP clinical lead, T4, 10)

T4-22 reported also that the IT department could be inflexible (as reported in 7.2.3.6 above).

T1-4 perceived a cultural divide with T1’s IT department:

“But I think culturally, I suppose as an organisational basis, I think there is, I think -- quite right, you know, there is a big divide between the IT department and the rest of us.”
(Pharmacist, T1, 4)

The following further illustrates the apparent ambivalence of the IT department overall towards the T1 library service:

“That’s been ... one of the – the complications that – that we’ve got ... Originally we weren’t really recognised as part of the Trust, for example when we get CDs which are licensed, we’ll make them available in the IT suite. I’ve now got – I can call, and someone from IT will come down and actually install the CDs for me.”

“ ... They’ve – they’ve given me all the suggestions, so uncertain relations in the past were kind of forgotten about, I think ... We’re not really considered -- we’re slowly coming on the radar -- they haven’t quite worked out what we can do. I think at first we were seen as a bit of a threat, and – it’s – it’s beginning to change – where they can see that we might be able to work together, but that’s with a lot of the IT staff, but not the senior manager.”

(Librarian, T1, 1)

T1-06 described the T1 IT department’s attitude and level of alignment to business needs in the following terms:

“ ... They are not completely amenable, we do sometimes have to, you know, rattle cages and get the big guns in the Trust to sort it out, but generally we have managed to get what we need.” (Clinical tutor, T1, 6)

According to T1-04, some IT staff were patronising in their attitudes:

“They are patronising sometimes, it depends who you get to speak to ... some of them are very nice, very willing to help. You get the odd one that is very patronising.”

(Pharmacist, T1, 4)

Issues of ownership of processes and professional jurisdiction, as well as of attitude, were apparent in T1-01’s account of her “unofficial” involvement in implementation of the new Trust intranet:

“They haven’t rolled it out across the Trust, and we’re currently trying to – to support the IT department when they do it, that we’ll actually help add content to it and manage it on behalf of the departments, and ... I’ve done some work on metadata for leaflets before, as well. We’re not exactly embedded in the process, but we’re not off the radar, either ...”

(Librarian, T1, 1)

Similar issues were apparent in the way in which T4-09 spoke of the way in which he experienced the information governance function being excluded from major informatics projects:

“I think that is an endemic reflection of the older organisation and the culture that is here, there [are] clearly new people who have come into various departments. We have got a person who is responsible for project management now; he is from outside and he is more focussed on doing things in structured, PRINCE2 methodology using PID and all that, and we have had meetings with him and incorporated IG into that process, so it is more embedded for very smaller projects. He gets in touch with us frequently about smaller things, and we

will be involved in those projects and on the groups, but [for] the bigger ones there seems to be still this bureaucratic -- they want to control it at the top of the organisation, we don't want everyone else really involved in it ... Our message to them is that we need to be engaged because we want to be helping, pointing out issues from the outset; we don't want you to come along when it's done, want us to ... see it and then[us to] say, 'This is a fundamental flaw'" (Records and governance manager, T4, 9).

Evidence was presented within the literature review of negative attitudes to end-users as a common aspect of IT staff subcultures (2.5.2). The failures of cooperation and communication on the part of T4's IT services described above by T4-09 had the potential for serious adverse impacts not just upon information services, but upon the Trust's planned EPR implementation, a major strategic initiative (4.4.1, 4.5.1). Issues of professional jurisdiction are discussed in 11.5 below.

7.2.3.9 Overall perceived quality of service

Many users within T1 (e.g. T1-08, T2-02) were generally positive about the quality of service provided by the Trust's IT service helpdesk, finding the staff helpful, polite and prompt to respond to support requests. Users in T2 were generally dissatisfied with the outsourced IT service provided by S3, and stated their preference for an in-house IT support service. However one of the nurses in T3-WPH (T3-20) had contact with both the Trust IT services and with S3, and commented that, "They are all brilliant; they are both really, really good". T3-01 reported a steady improvement in T3's in-house IT services during her time in post.

T4-10 felt that IT services in T4 had improved considerably during her time at the Trust:

"They are significantly improved to how things were historically in terms of their action and resolving IT issues. I have to say, they have got their act together, but it has been a challenge." (AHP clinical lead, T4, 10)

T4-06 also gave positive reports of T4's IT services (*cf.* above, Section 7.2.3.4).

Overall, a variety of problems in the interface of users with IT services were described by participants, which had affected or could potentially affect access to information sources. These included understaffing and general lack of resources, a tendency to prioritise clinical systems at the expense of information and other services, poor communications, cumbersome and bureaucratic reporting procedures and processes, a lack of alignment with LIS and other business priorities, and negative or patronising attitudes on the part of IT support staff. A marked trend towards

improvement in overall quality of IT services was also noted, however, by participants in all three Trusts.

7.3 Published information resources

Some collaborative activities relating to published information resources have been noted previously: T3 library's work with the Trust's training department (6.3), and T4 library's effective working with the IT department on IP address checking and troubleshooting problems with e-resources (5.2). A notable failure of communication has been highlighted as well: the T1 Head of IT's habitual non-response to communications reported by the librarian T1-01 and others (7.2.3.6 above).

All of the Trusts' library and information services were well regarded by clinicians; all spoke highly of their library's help with searches and document supply, although T3-19 and T1-07 both felt that better domain knowledge would have improved the quality of some of the searches carried out. T3-02 regretted the T3 library's lack of a physical presence within the Trust:

"[The] library service is generally very, very good ... but I ... I think you do lose something when a library service loses a physical base, and it is just as if it disappears out of your consciousness really and, so I mean there have been places when I have had an hour or so, when I worked in [name of hospital], it would be nice just to walk over to the library just to flick through the journals and flick through the books and see if there is any new additions there that might be interesting, whether it's mental health or whether it was anything else. They just become more invisible, I think." (Clinical tutor, T3, 2)

T1-06 reported that the T1 library was always highly rated by the Deanery following their visits and by junior doctors in General Medical Council (GMC) training surveys. She mentioned also that, following an intervention by medical educators, the Trust management had resolved to make up a shortfall in library funding threatened by the proposed move of the U2 school of nursing from the T1-LH site.

T4-08 described the electronic resources available via the T4 library as very good. T4-10 was fulsome in her praise:

“I can’t rave about our librarians enough, so they have been my godsend ((laughs)) and I just ring them and I will go down, I know them, I have a relationship with them and they have helped me through and accessed things ... that I need and are brilliant ... they are clearly way ahead of the game” (AHP clinical lead, T4, 10)

T3-01 was described as an “excellent librarian” by T3-18.

T2-01 mentioned T1 library’s support for students:

“... They are very helpful in terms of supporting students and using that facility. It is the same with if they are out here and they want to come and use it ... it is not a problem.

(AHP clinical lead, T2, 1)

Library services were involved in specific service initiatives in support of evidence-based practice. T1’s library was involved in the provision of a specialised current awareness service focused on areas of board-level concern in relation to quality of patient care and patient safety, namely pressure sores, safer medicines and falls, which were reported as being effective (T1-07). T3-01 also provided a customised current awareness service to senior nursing staff in T3-WPH.

Another clinical teacher within the same service made some important observations about evidence-based practice in relation to the general culture of T3:

“I feel like the overall culture within our Trust really does ... value and prioritise ... evidence based practice and accessing resources.”

“That is like our mantra, the 6 Cs, and as part of that it is about ... evidence based practice, developing the individual, valuing them, culturing and whatever, and I do think that ... we are really supportive in that, supportive in accessing [resources] ... (Clinical teacher, T3, 19)

In May 2013 T3 had adopted the 6 Cs (care, compassion, commitment, courage, communication and competence) as its core values. The 6 Cs had originally been put forward as a statement of nursing values in the document *Compassion in practice* (Department of Health, 2012a).⁸⁶ At T3, the operational meanings of the 6 Cs for individual staff members by way of behaviours were elaborated within what was termed a “collective responsibility agreement”. Under “competence”, the

⁸⁶ 6 C’s: <http://www.6cs.england.nhs.uk/pg/dashboard>

document referred to a general duty for all staff members of acquiring knowledge and skills to support one's role, addressing any identified gaps.

T3-19 also reported encouragement from the Trust's management to become involved in guideline development. She felt that one reason why this might be being encouraged is that it could be directly advantageous to the reputation and prestige of the Trust.

According to T3-01, the emphasis on evidence-based practice was starting to be extended to business planning and service redesign:

"People are starting to realise that their business cases and their arguments they need to make --actually they are being asked for evidence, so me going to these meetings and standing up and saying, 'That's why we are here', a light bulb comes on for them and they think, 'I know who to ask now'. So you know it is an opportunity for making sure that things are evidence based, and we are needing to make more business cases, aren't we? ... It is one of the major things, and redesign being ... underpinned by evidence and best practice really, so it is not a bad time ... for being able to demonstrate why it is important to be around ..."
(Librarian, T3, 1)

T1-02, by contrast, felt that within management practice at T1 there was insufficient reference to published sources of evidence:

"... I think that spreads right across some NHS staff groups ... including ... middle managers in ... accounts, HR, some of the corporate functions. It's – there's a culture in some organisations, and I'd say it about here, that you should be busy, busy, busy, because that's the perception of efficiency and effectiveness, rather than OK, let's take in some information, let's digest it, let's talk about it, let's plan." (Human resources manager, T1, 2)

This quotation invites comparison with Thompson *et al.*'s (2008) concept of the "culture of busyness" in nursing (Section 2.4.5 above). T1's values statement, while referring to "high quality care" and "learning and leading", did not specifically mention acquisition of knowledge and skills; T4's also made only a passing mention of sharing knowledge and promoting best practice.

NICE-01, whose background was in commissioning of clinical services, felt that commissioning in general within the NHS made insufficient reference to published evidence, leading her to wonder to what extent evidence sources were used (see Section 1.4.1, above). he also felt that there was

insufficient training given to commissioners, and insufficient capacity within NHS library and information services to support commissioning effectively:

“... Often library services are quite small in their capacity and then if you have got a commissioning organisation which holds 40 commissioners in there and each of them require support for evidence based resources ...” (Senior manager, NICE, 1)

In terms of individual professional cultures, there were two important observations. First, T4-12 outlined the way in which the use of published evidence was embedded within one of the main regulations governing the work of radiographers, the Ionising Radiation (Medical Exposure) Regulations 2000:⁸⁷

“We have to, and this is part of our IRMER regulations, and IRMER is [the] Ionising Radiation (Medical Exposure) Regulations 2000 ... and as part of these what we have to do is justify each and every single request.”

Web searches formed a major part of the process of justification:

“... If it is something that you don't know, you want to look it up, so you will go on the Internet, you will put it in and then you will call up a site and it says 'access denied' ((laughs)) and then you will go and find another one, ... there is usually something that you can find that isn't 'access denied', but ... know sometimes you are looking up because you want to know what it ... because it's like when you are doing an X-ray ... you have got the clinical information about that patient, you know what they are potentially looking for, we know what that looks like if they have it, so we need to know that information when we are looking at our images, to say, 'Do we need extra projections, or is this enough for that examination?' You know, is there anything else, or do I need to take it urgently because we have spotted something that perhaps is ... potentially a life-threatening thing? ...” (Radiographer, T4, 12)

The short time frame available for conducting searches implied that online information needed to be instantly available. Sources consulted, according to T4-12, could include Google, Google Scholar, the Society of Radiographers' e-journals, or one of the standard bibliographic databases, such as CINAHL or Medline.

⁸⁷ IRMER Regulations 2000: <http://www.cqc.org.uk/content/ionising-radiation>

Second, as regards use of published information by nurses to support their practice and the modelling of professional behaviour by preceptors and mentors, the researcher had raised with T1-07, the matter of Bertulis' findings from a literature review (2008b) of non-use of published information resources by nurses: that nurses tended to base the selection of information resources on convenience and accessibility, rather than quality, and preferred informal sources (usually colleagues) to printed or online ones. T1-07 expressed her conviction that the modelling of professional information-seeking activity by mentors as an aspect of the enculturation of students and newly qualified nurses would improve in quality as more nurses became academically qualified; indeed, that the whole culture of nursing would change.

Bertulis, in her earlier report (Bertulis & Cheeseborough, 2008) of the Royal College of Nursing survey of nursing professions' information behaviour, had reported that nursing staff whose employers had positive attitudes to evidence to change their practice appeared to have better access to a whole range of resources, including the Internet and the local health library. Availability of published information resources, and organisational support of LIS, has been shown by other authors also to correlate positively with attitudes to evidence-based practice and information seeking (literature review, Section 2.4.5). Evidence was presented by participants in all three Trusts of positive perceptions of LIS. Within T3 there was clear evidence also of a well-developed culture of evidence-based practice across the Trust. While this was less obvious within T1, the library service was closely involved in support for particular patient safety initiatives. All the Trust LIS were highly regarded by clinical and training staff at "grassroots" level.

7.4 E-learning

The impact of regulatory drivers on e-learning in dementia care in T1 has been noted already (Section 4.3.1). Other relevant issues relating to organisational dynamics and professional cultures in e-learning, in particular drivers for the growth of e-learning, and scope and utilisation of e-learning in different professions, were discussed in Section 6.3.

7.4.1 Culture, behaviour and attitudes relating to use of IT

Aspects of culture, behaviour and attitudes relating to information technology use obviously have bearings on a number of areas, including clinical systems implementation, communications and information behaviour (Ward et al., 2008). They have a bearing particularly on e-learning, however, and, for that reason, are discussed here. According to T1-01, paper-based communication still

predominated within the Trust, while T1-04 indicated that a significant proportion of clinical staff were markedly averse to using computers:

“I don't like to use the word technophobic, but certainly on an individual basis I think there are still ... a number of clinical staff that don't like to use the computers or use them as little as possible. There are an awful lot of people that don't have their own e-mail address, even though everyone is issued with a Trust e-mail account; they use it so infrequently that their passwords expired ...” (Pharmacist, T1, 4)

According to T1-02, nurses and junior doctors in T1 were very difficult to reach via email. Problems with communicating via email in T1 were mentioned also by T1-04.

In a similar vein, T3-19 indicated that, while IT training and support were readily available within the Trust, there were nursing staff within T3's community services who tended to avoid using computers, and who also did not avail themselves of the IT training opportunities that were offered them. She had even known staff whose decision to take early retirement had been partly precipitated by “technostress”.

T3-19's comments here may be compared with those of T4-22 regarding poor computer literacy (6.4). As discussed in Section 2.8.5 above, habitual non-use of computers or aversion to computer use within the NHS is thought to be a relevant factor in the persistence of poorly-developed infrastructures and in low levels of information technology investment and innovation. Poor-quality IT infrastructure and negative experiences of IT support services may themselves be contributory factors in aversion to computer use, so that a vicious cycle may exist. As we have seen, many of the technical problems affecting access to published information resources related to inadequacies in infrastructure (5.2). It is also self-evident that, in an environment in which much, if not all, professional information in the health sciences is published, and expected to be accessed, online, aversion to computer use is likely to be associated with or result in poor levels of access to and use of information to support evidence-based health care.

7.4.2 Staff attitudes to e-learning

Observations of “e-learning overwhelm” for doctors at T4 have already been mentioned. The risk of “overwhelm” caused by inappropriate expectations of e-learning was highlighted by T1-01:

“... People think that e-learning is something quick and easy, and they forget to add up the time that it takes; it’s getting difficult for people to do it in their own time at home, particularly if they want work-life balance.” (Librarian, T1, 1)

Participants reported a range of attitudes to e-learning among the groups of learners of which they were aware:

“I think you will always find people who like it and people who dislike it – [it] is a bit like Marmite, isn’t it? You either love it or you hate it ...” (Non-clinical teacher, T3, 4)

Reasons given for disliking e-learning included the lack of interaction with other students and the opportunity to ask questions to check understanding (T2-01). When undertaking anatomy and physiology e-learning they did not learn how to pronounce the Greek and Latin words, leading to feelings of insecurity with the subject matter. Discussion boards related to e-learning modules could be intimidating or pretentious, and usability could be a problem; the authors too readily assumed that the content was readily navigable without signposting or guidance (T1-08).

T1-08 observed that it was vital for students’ understanding that feedback was provided with marks for test questions, so that reasons for incorrect marks could be understood and pinpointed; also that usability problems or system errors with e-learning could have a very aversive effect on learners, undermining their confidence in undertaking it.

In the view of one clinical teacher at T3, usability in e-learning was of paramount importance:

“... I think things have got to be made to a point where it’s like shopping on-line, it is easy [to] do ... it’s intuitive, it is simple ... that is what we have got to get to.” (Clinical teacher, T3, 7)

In recognition of the importance of usability, the e-learning developer at T3 was reported as spending a large amount of time on improving the user-friendliness and usability of the Trust’s e-learning content:

“... Over the last year, our e-learning developer has spent a huge amount of time working with the subject matter experts for the mandatory e-learning packages we have got that they are much more user friendly now, you can go back and to through them, we have got pre-course assessments so that if you do the assessment and pass you don't need to go through the whole thing, and ... there is lots of things being put in place to make the package much more user friendly and it has got ... it is more, before it was very grey, it is very coloured, there is lots of hints and tips ...” (Clinical teacher, T3, 4)

The training administrators at T1, T1-05 and T1-10, also spoke of the critical importance of usability and “debugging” from a change management point of view when e-learning was introduced within T1. T1-10 stated that she had learned this from unsuccessful initiatives she had seen elsewhere to introduce e-learning.

It is intuitively apparent that usability of information resources can affect access to and use of published information. The findings reported above suggest 1) that this may be particularly true of e-learning, and that 2) usability issues may be more likely to affect novice users of e-learning than those who are experienced. T1-05's comments suggested that poor initial experiences of e-learning could have enduring aversive effects. The findings here may be compared with the report of usability issues affecting HDAS, the NHS common interface to online bibliographic databases in the health sciences, which are discussed in Section 5.3 above.

7.5 Web 2.0 and social media

Several participants spoke of ways in which explicit professional norms relating to social media were transmitted or enforced. T4-08 mentioned a university lecturer's being “friends” with her students on Facebook as means of communication with them that she had found to be more effective than telephone or email, but then also monitoring the content of their posts and reprimanding them if they posted any content that she deemed unprofessional.

The clinical teacher T1-08 spoke of the peer monitoring of social media content among student nurses:

“... We have had students ... screenshot other students'... comments and bring them in and say, 'We think this is inappropriate', and ... raise their concerns with the university staff about other students behaving inappropriately, because they are worried as ... being friends with them; they think 'Well, I don't want to ...' and I think, 'Well, I am this person's friend on here',

and ... they ... tend to try and monitor each other and ... keep each other in line in terms of what is appropriate and not.” (Clinical teacher, T1, 8)

Participants mentioned specific teaching that students and junior doctors received about professionalism in the use of social media:

“... We warn all our students when they come to be careful about what they do or don't post in terms of -- obviously they need to think about what they are saying, if they are saying anything that links to the Trust as to whether it's ... libellous or not.”

(AHP clinical lead, T2, 2)

T1-06 highlighted the importance of maintaining appropriate privacy settings:

“We do talk to all the trainee doctors that start, about social media sites, but it is more to warn them to be careful about the sort of information... and ... warn them that ... if they allow open access then people looking to employ them can look at them, so it's about really, how to use, how to maintain your privacy settings, it's more that sort of thing.” (Clinical tutor, T1, 6)

Participants tended to perceive the level of risk of using social media in professional contexts as unacceptably high:

“I think generally, your more senior practitioners will tend not to use Facebook and social media, ... because of the potential risks inherent with that ... I know a lot of our staff do, but I think a lot of, I think perhaps if you speak to a few of the more senior staff they might say, ‘No, I just don't do that’”. (Clinical teacher, T1, 8)

The clinical teacher T1-08 felt that social networking could potentially involve her in potentially complex problems relating to her professional role and identity, in particular the need to establish proper boundaries with students and patients:

“I think ... for me there is a fear within my role and my connection with students and the practice that ... I am not on any social networking site, because I just think it opens the door to potential problems that I don't want to get involved with ... if I am not on it at all, that is not ever going to happen.” (Clinical teacher, T1, 8)

The AHP clinical lead T4-10 felt that NHS culture acted as a powerful disincentive to the use of Twitter in particular. Her primary concern appeared to be the possible risk to the reputation of the Trust:

“I would even have this niggle, now maybe it’s just because of what you get instilled into you when you are in the NHS a long time, is to -- what am I allowed to Tweet, and what am I not? You know in terms of... all that breach of ... reputation and that wider aspect, and I feel actually the reality is, we need to probably have some very open discussions about this, and a little bit of -- ... to be given authority to say you can, you can Tweet.”

(AHP clinical lead, T4, 10)

The clinical teacher T3-19 would have liked to use social media in connection with patient engagement with community health services; however, she felt that this was potentially a high-risk undertaking, in which support and training within the Trust would be required:

“Yes, but I also understand that sometimes within our groups there is a bit of a risk there, that would maybe ... you feel like you want to pull the reins back a little bit because, if I think of something like perinatal mental health or whatever, there is just a risk that you would want support to manage that risk really.” (Clinical teacher, T3, 19)

The issue of using social media for patient engagement had also come up as a possible service development within pharmacy services, but the pharmacist T3-18 felt that the existing lack of access to social media applications precluded him and his colleagues from doing so. Here it appears that the Trust’s restrictions on social media use had dissuaded him from pursuing a social media initiative. (Neither of these participants appeared to be aware of the help and support with social media initiatives available from T3’s communications department, as outlined by the communications officer T3-12 : see above, Table 5.2).

The findings here are comparable with those of Scragg, Shaikh, Shires, et al. (2017) in respect of staff concerns. General attitudes of staff to social media and social media policies are discussed in section 9.2.3 below.

7.6 Mobile devices

Professional norms and culture in relation to information technology of any sort are affected by, and are necessarily closely related to, current usage, policy and practice. Policy aspects were discussed in Sections 1.4.4 and 4.5.3, and earlier allusions have been made to existing usage, although not all

work-related usage of mobile devices was explored with participants, particularly when it related to clinical systems.

In T4, Trust mobile phones had formerly only been given to senior clinicians and managers, but were now available to anyone (according to T4-19). This participant, a consultant surgeon, reported using his own iPad for work via the Trust BYOD network, and his own iPhone for work-related calls, an apparently common practice.

There was a strong sense expressed within T1 and T3, and within some professional groups in T4 that, as T3-18 succinctly expressed it, “Personal smartphones and tablets aren’t really acceptable for use in a patient environment”. This, he said, reflected Trust policy, which precluded the use of personal smartphones in clinical areas. He explained that he was unclear on the full thinking behind the prohibition, but referred to possible breaches of confidentiality via the built-in camera and access to Facebook, or via loss of the device.

T1-08 spoke of expectations of student nurses regarding the use of mobile devices:

“In terms of using [their mobile devices] in practice I think there are issues around the opportunity that they might get to do that because of the work that they are doing ... so there are time constraints there. I think also, my gut feeling is that the ... nursing staff, their mentors, their ward managers probably wouldn’t reflect very positively on the students being on their mobile phones whilst actually on the ward ... [even for work-related or study purposes] ... they would probably ask them to do that in their break or ... sometimes they will facilitate them to go to the library if they need to do some research, and they probably would prefer them not to use mobile phones whilst actually within the ward area.”

“... There is perhaps the idea that maybe it is not appropriate ... being on your mobile phone in front of patients or in the clinical area ... because I think there is always the concern that ... they are not using it for research and education purposes, they might be ... texting their friends ...” (Clinical teacher, T1, 8)

According to T1-04:

“... There is an internal rumour within pharmacy that you cannot take smartphones on to the wards, and certainly you can’t use them on the wards, they are supposed to be left within the department.” (Pharmacist, T1, 4)

This seems at first sight to be an odd way of referring to a departmental policy. It was one of a number of instances in which restrictions on mobile phone use were cited as being official policy, but could not be found in Trust policy documents; see T4-04's comments, below.

T4-08 reported that AHPs in T4 were discouraged from carrying mobile devices with them when they were on the wards:

"Loads of them have bleeps or a pager, so if they need to be contacted for a professional reason then they are accessible ... it is linked to infection control and professionalism and things, so if they needed to access any educational things I would ... support them in accessing the Trust's ... equipment rather than having to use their own."

(AHP clinical lead, T4, 8)

"Quite a lot of our staff are still working in areas where there is a lot of equipment, and yes, it is never, for me as a professional it is never a great look to see a therapist walking down the hospital corridor taking a personal call on a mobile." (AHP clinical lead, T4, 8)

The radiographer T4-12 reported that, while there were no official restrictions within the Trust on the use of mobile phones in particular areas, it was a matter of "professionalism" that mobile phones were not used in patient areas. T4-04, however, reported that she used her own mobile regularly on the wards:

"Yes, a lot of people within the Trust have apps on their phone for various, various bits and bobs, so I have a BNF app, I have ... a NICE app, I have -- what else do I use? Oh, dose calculating apps, body surface area calculating apps, so kind of the things that I would do every day on a ward, I have an app for, and whereas five years ago I would never even have ... dreamed of taking my mobile phone down to the ward, I now have my mobile phone on me pretty much all the time."

When asked about possible restrictions on using mobile phones on the wards, her response was:

"Oh gosh, don't open this can of worms! I don't know. Certainly the medics have their phones on them, we have our phones on us and we use them quite freely and openly."

(Pharmacist, T4, 4)

Her response here may have indicated awareness of a common practice that was at variance with official policy. It should be noted, however, that at T4, tablets were used clinically in a variety of contexts, such as the major trauma team, where the so-called “rehabilitation prescription” was completed using a tablet. The stroke team members were also using tablets in a similar fashion. Both of these examples of clinical tablet usage were aspects of national programmes (T4-08). The community health services of T3 were also piloting the use of rugged tablets by nurses undertaking domiciliary visits (T3-19). Medical students from U3-Med using university-issued iPads to support their clinical learning were present in all three Trusts, although to a limited extent in T3 (psychiatry rotations only). The planned use of tablets at T1 has already been described (Section 6.5). T4’s BYOD policy and wireless network may have contributed to a wider acceptance of the use of personal smartphones in work contexts.

As described above (Section 5.2.6), board members in all three Trusts were issued with iPads. T4 had approximately 200 iPads altogether, which, according to T4-20, were used mainly for document management and for accessing email. Considerable numbers of staff also used their own iPads for work via the Trust’s BYOD network. At T3, laptops and Windows 8 tablets were the preferred mobile devices; only limited numbers of iPads (20-25) were in use.

Under existing university guidelines, medical students were strongly discouraged from taking their iPads on to the wards. However T1-07, a senior nurse manager, foresaw a time when policies and attitudes might change, particularly if iPads were able to connect to the Trust planned EPR system:

“If you are looking after patients you can’t be carrying an iPad with you ... and if you need to look anything up all the wards have got computers, so you can look things up. I can’t see the need for that at the moment ... but as we get more ... progressive, then I think we will have a stance on that that will ... yes, all have iPads which aren’t linked up to one system and they need to be. This electronic patient record has got to link through to every piece of kit, and currently it doesn’t.” (Senior nurse manager, T1, 7)

The clinical tutor T3-02 stated his view that, away from clinical areas, staff were using their personal mobile phones far too much for non-work purposes while at work. He complained in particular of staff using their mobile phones during morning handover meetings:

“... When we discuss every case, this is the home treatment team, so it is quite an ill group of patients that we are talking about you will see people not listening and ...” (Clinical tutor, T3, 2)

A gradual overall shift was apparent towards greater acceptance of the use of mobile devices in the context of professional work. In general it appeared probable, however, that professional culture regarding the use of mobile devices was lagging somewhat behind trends in mobile learning and use of point of care information (Lumsden, Byrne-Davis, Mooney, & Sandars, 2015).

7.7 Summary

This chapter has focused on the interface of clinical services, training and LIS with IT services, on the use of information resources and perceptions of LIS, and on culture, behaviour and attitudes relating to the use of IT and to e-learning in particular. Participants in all three Trusts reported that procurement of PC hardware was the responsibility to individual services (IT departments had limited control over hardware procurement) and was not accorded a high priority by service managers unless directly required for clinical systems. In consequence they were obliged to use old, sometimes obsolete, PCs. No central or ring-fenced funding was available to cover the cost of replacements. IT services in all three Trusts were reported as being accessible via telephone and email, and (in the case of T3) via online chat. Participants described the communication processes with T1's IT helpdesk and with the outsourced service for T3's community services, S3, as cumbersome and time-consuming. While responses to IT support calls were generally described as timely, the quality of communications in general with IT departments, and their responsiveness to business needs, were stated to be unsatisfactory both in T1 and in T4, where negative attitudes towards end-users (and in the case of T4, to the information governance managers) on the part of IT staff were also described. End-users also reported that the IT departments of T1 and T4 tended to focus on clinical systems as their main priority, at the expense of other problems; at T3, however, education and training were felt to be well supported. Although all the Trusts' IT services were reported as having improved steadily over the previous few years, those at T1 and T4 were described as significantly under-resourced in relation to demand.

All the library and information services appeared to be highly regarded, and their activities well aligned with the business processes of their respective Trusts. The importance of evidence-based practice (EBP) as an aspect of the overall culture of each of the Trusts appeared to vary. At T3, it appeared prominent; at T1, an emphasis on EBP was described by participants in relation to particular quality and patient safety initiatives, but as insufficiently emphasised in overall

management culture; in T4, it was not referred to at all. It is possible that, being a research institution, EBP at T4 was taken for granted. Some indications were given of the importance of EBP within individual professional cultures: a detailed account of its application within the practice of radiographers (T4), and an opinion about trends in recently qualified nurses' enculturation into habits of information use at T1.

Participants spoke of a cultural aversion among clinical staff to the use of computers, and widespread lack of use of electronic communications in particular. Information literacy problems were cited as one possible barrier to e-learning implementation; others included usability issues (particularly important for less experienced users), e-learning "overwhelm" in terms of the time required, and the lack of opportunity to interact with other learners.

Means of transmission of professional norms regarding social media use could include a presence on and monitoring of particular social media platforms, as well as formal face-to-face teaching on e-professionalism. Concern was expressed by clinicians about the perceived risks of professional use of popular social media platforms: these were perceived as presenting risks to reputation of the Trust, confidentiality, and the maintenance of appropriate professional boundaries. Interest was expressed by clinicians within T3 in the possible use of social media for patient and public engagement, but the participants concerned felt that existing restrictions within the Trust on social media use acted as a strong disincentive to pursuing any practical initiatives.

Professional norms relating to the use of mobile devices, as reported by participants, stressed the unacceptability of using these in general, and mobile phones in particular, within clinical areas. However, there appeared to be an increasing acceptance of the use of mobile devices in non-clinical contexts. The use of tablet computers for recording patient observations, for record keeping and for e-learning, as well as T4's BYOD arrangements, may have been a contributory factor.

The following chapter (Chapter 8) discusses more formal policy aspects of the regulation of IT services' use.

Chapter 8. Findings: information governance and security

8.1 Introduction

General aspects of information governance and security within the three Trusts, including the use of secure web gateways, have been discussed extensively in the “background” chapter (4.2). This chapter covers a number of specific issues: acceptable use policies, monitoring of staff web use, mobile device security, general endpoint security issues, and the effects of these on access to published information resources and on education. Under the heading of access to published information resources, the chapter looks in detail at the frequency and extent of website blocking, the nature of content that was blocked, responses to encountering blocked sites, the effects of website blocking, and awareness of national whitelist and browser requirements. The content coverage is illustrated in Figure 8.1.

8.2 Acceptable use policies

T1 and T3 had incorporated all aspects of IT use, including the Internet, into single policies. T4 had separate policies governing Internet and email use and computer and network security. The policies varied somewhat in scope and content, however, as outlined below.

All the policies included the key constituent items of an acceptable use policy (AUP) as identified by Gallagher, McMenemy, and Poulter (2015). In AU1 a substantial section was devoted to acceptable use of the Internet, social media and instant messaging. It was notable in the positive attitude it expressed towards the Internet at the beginning of the document:

“Use of the Internet is a key information resource for [T1]. Our ability to exploit and gain advantage from information will enable us to maintain and improve our reputation and ensure that we meet our strategic business and professional goals.”

It sought to encourage the following activities: communicating with fellow employees, business partners of the Trust and suppliers within the context of employees’ specific job roles; acquiring or sharing information necessary or related to employees’ job roles; and personal educational, research and recreational use of Internet services in accordance with the policy which did not interfere with the employee’s own or other work duties. It stated, however, that personal or recreational use of email and the Internet was “a privilege, not a right” and could be withdrawn, also that non-work

activities resulting in heavy network traffic were not acceptable. Individuals were asked to limit their personal use of the Internet; according to the policy, the Trust allowed “limited personal use, for communication with family and friends, independent learning, and public service”. It offered lists of examples of acceptable and unacceptable use of Trust IT facilities; the latter included the standard range of illegal activities as proscribed in computer misuse legislation (see Section 2.7.3, and Appendix G). In addition to these, online shopping, whether for Trust-related or personal purposes, without prior approval was specifically banned, as was the sending of “unreasonably large electronic mail attachments or video files not needed for business purposes”, this latter in the interests of maintaining network performance. Pornography was treated at some length: the deliberate viewing and/or printing of pornographic images were banned. An exception was made, however, for “legitimate study and research into pornography and associated issues” as the “only reason for deliberately accessing such material”.

Within AU3, personal use of the web and email was allowed on a similar basis to AU1, although staff were required to put “PERSONAL” in the subject line of personal email messages, and not to store them for more than two weeks. The specified categories of unacceptable IT system use in AU3 were similar to AU1’s, and included gambling and pornography (T3-06). Personal use of the web during breaks was subject to the approval of a member of staff’s line manager. Unintentional access to sites of an offensive nature was to be logged as an incident.

AU4Int specified the use of Microsoft Explorer and Microsoft Outlook as the standard web browser and email client; however, version numbers were not given. Installation of additional software or plug-ins required the permission of the IT department. Personal usage of email and the Internet was normally allowed during break times, subject to line management approval. In contrast to AU1’s “legitimate study and research” exception for accessing pornography, AU4Int stated that “ALL forms of pornography transmitted or received via any medium will ALWAYS be deemed as offensive.” A long list of categories of unacceptable material was provided, which appeared to derive in its entirety from the SWG4 documentation. In similar fashion to AU3, unintentional access to offensive or proscribed material was to be reported to line management.

A specific warning was issued about downloadable files:

“Access to downloadable files, the downloading of files and transmission of files may be restricted by [the secure web gateway] and / or NHS and Trust network settings. These restrictions may [apply to] files of [certain types] (e.g. .zip files) and / or files that exceed specific size thresholds, and may change in line with security advice”.

The tone of AU4Int was notably minatory: the threat of disciplinary sanctions for internet misuse appeared twice, within a text box and highlighted in bold. The use of peer-to-peer (P2P) applications was specifically banned in AU1 and AU4Int, as constituting a risk to the security of the Trust network. Generally, file downloads were required to accord with legislation such as the Copyright Designs and Patents Act 1988.

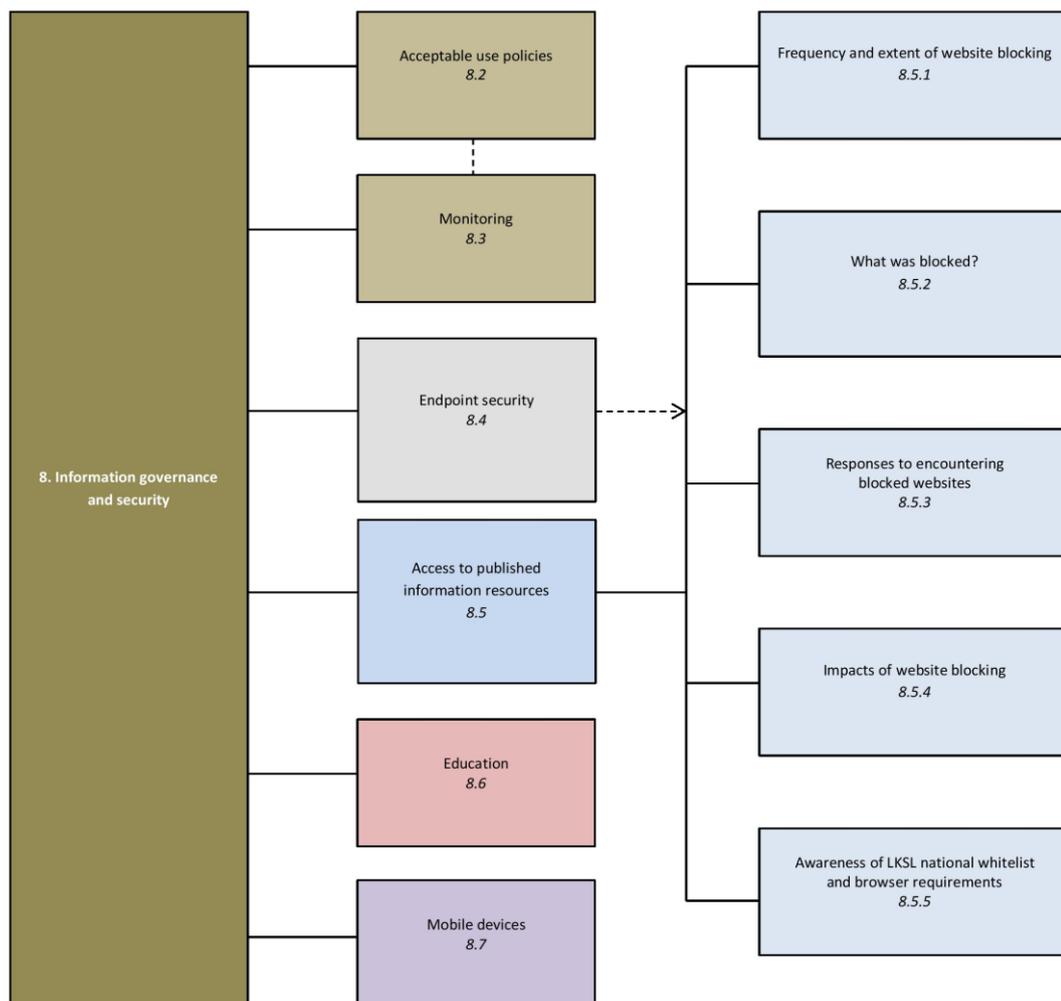


Figure 8.1 Information governance and security

Other than T1's exception for pornography already mentioned, no qualification was made in any of the Trusts' AUPs regarding intention or purpose of access to categories of material generally considered as unacceptable. This contrasts markedly with the provisions of the "model" AUP published by HSCIC (literature review, Section 2.7.3.2). No instances of requests to access such material for research or clinical purposes were discussed by participants.

The originator of AU4Int was given as the director of informatics. Approval of the policy had been given by "Trust information governance" in lieu of the IM&T steering group, which at that time was in abeyance and due to be re-launched. The policy had apparently been ratified by staff side representatives of the Trust's consultative committee, presumably on account of its messages regarding disciplinary measures; however, no other consultations with staff groups were mentioned. The date of issue of the version publicly available via the Trust website was given as March 2011, with a review scheduled for March 2012, which was thus overdue. AU4Sec listed a manager responsible for IT infrastructure and business continuity as its originator. It had been issued in March 2014, with a scheduled review date of October 2016. No details of consultations with or ratifications by other staff groups were given.

AU3 gave the director of operations as the lead executive, with the head of IT as the author. The approving body was the Trust records and clinical systems group. A link was provided to a copy of the equality impact assessment, also to a list of the staff consulted during the document's preparation. The implementation date was given as March 2014, with a scheduled review date of March 2019.

AU1 gave the head of ICT as the author of the policy, with the medical director as the lead director. The approving body was the information governance committee. An equality impact statement was provided, also a list of the managers and staff group consulted during the policy's preparation. The implementation date was given as March 2013, with a review scheduled for March 2016.

Review arrangements were noted very briefly in each document. No mention was made in any of the policies of any arrangements for monitoring of the impact or effectiveness of the AUP and of its enforcement.

8.3 Monitoring

AU1 described in detail the monitoring of web use that was undertaken in relation to the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA). According to the policy wording:

“The [IT Department] keeps records in order to monitor traffic flow and system usage. These indicate the dates, times and sites accessed. The [IT Department] staff do not inspect any of this information to check on personal use, nor do they routinely inspect the contents of any internet log file.”

Circumstances cited as warranting monitoring included a threat to the Trust’s systems or data resulting from malware, suspicion on the part of the Head of IT that IT facilities were being misused, or a request from the police in furtherance of a criminal investigation. The T1 secure web gateway did, however, send automatic notifications to IT managers of attempts to reach blocked websites (T1-12). Managers were also notified by IT of excessive non-work-related usage by members of their staff. As reported in 4.5.4, T1-02 reported, however, that while penalties for misuse were stated in policies, in practice not a great deal of monitoring took place of compliance with information security policies, e.g. regarding the proper use of smartcards. The pharmacist T1-04, however, expressed concern about the consequences of attempting to access blocked websites in the course of her work, and was keen to avoid doing so:

“You won't use search terms that you want, or you just think, ‘I can't do this at work’, because you know it is going to throw up blocked content, or there will be questions asked.”
(Pharmacist, T1, 4)

However, the automatic notifications of attempts to reach blocked websites did not appear to be acted upon.

AU3 did not mention the requirements of RIPA. It stated simply that:

“Should a line manager have a concern about an individual’s use of the internet, [the IT Department] can provide a log file which will contain details of the site accessed by the user, the time of day the sites were accessed and for how long.”

“If a member of staff has been accessing or trying to access an inappropriate website, it is the responsibility of the [IT Department] staff to notify the [IT helpdesk] manager or deputy, who in turn will contact the user’s line manager and ask them to take appropriate disciplinary action.”

T3-06 reported receiving requests from managers for records of the web use of individual members of staff approximately every two months. He would have liked to put in place some system of automatic reporting to line managers at regular intervals of websites visited by staff across the Trust; however, he said he did not have the resources to do so, and that he had other priorities to address within his limited budget. He did, however, generate a report for each meeting of the records and clinical systems group of the “top ten” websites visited. Log files covering up to three months’ worth of data were potentially available to be scrutinised. A contract IT staff member had been dismissed within the relatively recent past for excessive Internet use during working time (T3-06, T3-03). T3-06 reported receiving requests periodically from managers to block certain sites that were deemed inappropriate, but which were not blocked by SWG3, indicating that some degree of under-blocking was occurring. He did not give further details of these, nor did he state whether or not he actually added them to a blacklist. No routine monitoring was undertaken of content filtering accuracy.

According to AU4Int, reports of email and Internet use were generated by the IT department for monitoring purposes and could be made available for managers “where cause for concern may indicate this is appropriate”, i.e., in accordance with the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA). The need to “investigate alleged or suspected non-permissible use” was the only justification referred to for accessing these reports. It also stated that alert messages identifying the user were sent to IT managers when attempts were made to access websites in “certain blocked categories”; these were monitored and “appropriate action ... taken, if necessary”. The user was also alerted to the fact that their attempt to visit a blocked site had been recorded. Two participants (T4-10 and T4-05) reported being concerned, after seeing these, about the possible repercussions, and a speech and language therapist, T4-08, mentioned general concern about this: “What staff wouldn’t want either would be for IT to think that people were trying to access [inappropriate material] ...”. In practice, however, IT managers at T4 did not scrutinise log files of blocked websites to assess filtering accuracy; T4-20 reported that he had no time to do so.

Use of Skype was specifically banned in the policy under the category of peer-to-peer (P2P) networking applications, these presenting a recognised security risk (2.6.3).

8.4 Endpoint security

T4-09 commented on what he perceived as laxity about basic information security measures in T4:

“... The basic stuff that went on in terms of... tighter and greater awareness around security measures, printing e-mails, port control for memory sticks, things like that, that are enforceable through organisations, aren't always enforced here, and it is a big cultural shock for them. People have said to us, 'This place is five or six years behind other Trusts' ... Just because it's a big Trust ... doesn't mean it's at the top of its game in everything, I don't think.” (Records and governance manager, T4, 9)

Indeed, the Trusts in the study did not follow basic security best practices in several respects: the use of older versions of web browsers, which presented a security risk in itself (P1), occurred in all of them (2.6); all the Trusts had at least some PCs still running the obsolete Windows XP; screen locking of PCs was not implemented in T1, thereby increasing the risk of unauthorised access to confidential data; and USB port blocking was not implemented in T4 (T4-09, confirmed by T4-20), thereby potentially allowing data breaches via the use of unauthorised unencrypted USB memory sticks. Of these, the lack of port blocking at T4 was potentially far the most serious. The confusion regarding the use of encrypted memory sticks in T4 has already been noted (5.2.1). It seems paradoxical and inconsistent that, although levels of website blocking were relatively high in T4, other areas of IT security, as just outlined, were lax.

8.5 Access to published resources

This section is concerned with the blocking of websites and responses thereto.

8.5.1. Frequency / extent of website blocking experienced

The senior manager at NICE, NICE-01, stated that “[Blocking of websites] is what we hear from our library community, they do tell us this quite a lot”. Reports of the frequency of encountering blocked websites varied across the three Trusts and by professional group. Most of the participants in T1 (T1-01, T2-02, T1-06) reported encountering blocked sites and content very infrequently; the comment from the clinical tutor T1-06 was typical:

“As a post grad clinical tutor, no-one is coming to me and saying 'I cannot get access ...’”
(Clinical tutor, T1, 6)

T1-04, however, reported that she encountered them more often:

“... Sometimes you just think, ‘I will go and do it at home’; it is an awful lot easier. Even if you know it is not social media or anything -- it is just, because obviously we do get queries about things ...” (Pharmacist, T1, 4)

The IT manager T1-11 reported that only five requests to unblock websites had been received by the helpdesk within the last 18 months. T1-05 and T1-10 reported encountering blocked websites in the course of their work, but did not provide details, or any indication of frequency. T2-03, who worked across both T1’s and T2’s systems, reported that more blocking of websites occurred within T2 than within T1.

The reported incidence of blocked sites, as reported by the librarian T3-01 and clinical teacher T3-07, was similarly low in T3’s main network. The pharmacist T3-18 had experienced only four instances in five years. T3-19, a clinical teacher working within T3’s community health services, reported, however, that she was encountering blocked sites when carrying out Google searches. This was presumably occurring on the outsourced network (see above, Section 4.5.3).

Levels of reported blocking of websites were generally much higher in T4, however. In relation to the support of teaching activity within medical education, T4-11 reported having encountered a blocked website only once in the previous four years. The librarian T4-06, who was new in post within the last six months, cited a figure of one a month, which he said had been quickly unblocked by the IT department once reported. T4-03 suggested that, dependent on the type of work she was undertaking, she might encounter a blocked site every two months. T4-12 reported encountering blocked sites “sometimes, not often”. T4-04 and T4-10 both reported frequently encountering blocked sites: “daily, probably” (T4-04); “it might occur every week” (T4-10). T4-05, a clinical teacher, while not giving an estimate of frequency, was evidently encountering blocked sites regularly, as also was T4-22, who reported the frequency as “fairly often”. T4-10 commented “I am just constantly hit with denials, blocks and ...” T4-05 was under the impression that there were fewer restrictions on web searches within the library: “certainly in the library you can access things more readily.” T4-03 observed that blocking of websites “does happen a lot”.

The number of blocked websites encountered by library staff would have depended on the type of searches they were undertaking for readers and the resources they were using, It is unclear in this situation, however, why the number of blocked websites should have been lower for the library staff

than for clinicians within the Trust, or why T4-05 should have formed the view that there were fewer restrictions on web access within the library compared to other parts of the Trust; this was subsequently denied by the IT manager T4-20.

*8.5.2 What was blocked?*⁸⁸

The retired IT manager, P1, recounted an amusing episode in which the implementation of a skin tone detection feature within the web filter at his former Trust had aroused the ire of the dermatologists, who had thereby been blocked from accessing online dermatology resources containing images of skin conditions. The feature had therefore been disabled forthwith; compare the attempts by pornography seekers to access an online dermatology atlas: Section 2.7.3.4.2 above. Apart from individual site restrictions, he reported that the only thing that had been blocked “as a matter of course” was streaming radio, on account of its high bandwidth usage. P2 mentioned iTunesU,⁸⁹ specifically, as being an educational resource that was blocked within his Trust. Much of the provision of IT infrastructure in his organisation was outsourced, and he did not himself have direct control of the secure web gateway, although he suggested that the rationale for the site being blocked might relate to potential bandwidth consumption and impact on network performance, rather than to malware concerns. He indicated that these were likely to be deciding factors for other Trusts in their blocking of access to resources of an apparently legitimate character.

The very few specific instances of individual work- or study-related websites, as distinct from web applications, reported as having been blocked at T1 included the British Medical Association⁹⁰ website (T1-01) and a BBC adult literacy website (T1-10). As reported in 5.5 above, the AHP clinical lead T2-02 reported that an online professional forum was not accessible from computers at T1. (Professional forums can be classified as web applications managing user-generated content, although their technology predates that of Web 2.0 technologies and social media.)

At T3, T3-18 reported being blocked from accessing sites that he had needed to refer to in relation to the medication management of a patient who was self-harming:

⁸⁸ Blocking of Web 2.0 and social media applications is discussed in Section 8.5.3 below.

⁸⁹ iTunesU: <http://www.itunesu.co.uk/>

⁹⁰ British Medical Association: <http://www.bma.org.uk>

“... So of course when you put in queries about self-harm the question then is ‘Why is somebody looking at self-harm?’ Another one in relation to anorexia for example, or bulimia, because of course you get your ‘pro-ana’ sites which are ... there. Good reason they are being blocked, but the reason you are trying to, you are looking for particular searches underneath that title --not a ‘pro-ana’ site but because that title, that name in itself raises issues you have to, I tend to narrow down my searches and then go to IT and ask, ‘I want a particular paper relating to this search’.”

Other instances of blocking that he had encountered appeared to relate to “objectionable” terms:

“Unfortunately some of the queries you do get have words that the computer system or the IT system recognises as being out of the ordinary ((laughs)) and so therefore can block.”

(Pharmacist, T3, 18)

He reported in particular that results of a search engine query “hyper-sexuality” had been blocked. Another instance of blocked content at T3 was described in Section 5.5 above, which appeared to relate to an intellectual property issue with podcast teaching material.

The relatively small extent of T3’s forensic services was noted above (4.1.1), the relevance of this being that information needs in forensic services frequently concerned subject matter (relating, e.g., to sexual offences, violence or arson) that is commonly blocked by web filters.

Within T4, as reported by the AHP leads T4-08 and T4-10, the consultant surgeon T4-19 and the medical education administrator T4-11, there was a consensus among clinical participants that the Trust web filter tended to block material containing images or advertisements. This could as much affect information intended to be provided to patients as professional-level information for clinicians:

“Yesterday on the neonatal unit I needed to show a parent at the bedside what ... disposable teat ... to purchase in a chemist and I wanted to show her a picture of just what it looked like ... But went on every -- by every cot side there is a computer, ideally so you can bring anything up, went on and I just wanted to show a picture on the Boots website: denied, blocked ... just typed in the product, [trade name] teats and ... it was denied ... it’s basic stuff like that even, that never mind trying to actually look at articles.” (AHP clinical lead, T4, 10)

T4-08 reported a similar experience in attempting to access patient information containing images.

The blocking of advertisements was subsequently confirmed by T4-20:

“That is correct, well advertising certainly, because there are malicious adverts out there that get ... that pop-up all the time, so adverts as a category is blocked.” (IT manager, T4, 20)

He maintained that, with advertising-supported legitimate websites, this was not a problem, because the main content was still available to be viewed:

“Yes, what we do find is because they are in frames, ... and iFrames, then the main site gets through, but then sometimes adverts on each site get blocked.”

He denied, however, that images in general were currently being blocked; however, he seemed uncertain of the exact situation:

“Image sites aren’t blocked; there are, they used to block image sites, and I need to check that actually because ... as far as I know image sites aren’t blocked, but they were some image sites that did contain pornography so we did block image sites. Image sites are not currently blocked.” (IT manager, T4, 20)

In subsequent email correspondence, he suggested that some of the sites which users had been attempting to access were from Google Ad Services, which invariably appeared at the top of search results lists. Being advertisements, these were, of course, blocked. This accorded with T4-12’s observation that, in particular, sponsored Google listings appearing at the top of search results were blocked, whereas the same site appearing further down in the “free” search results might not be.

T4-08’s and T4-10’s experiences with patient information sites suggested that the configuration of SWG4 to block images may not have been working as intended. T4-20 did not initially offer any explanation as to why the entire content of the sites, rather than just the advertisements, were blocked in these cases. He was evidently not aware of the problem; indeed, as indicated in the quotation above, he seemed to be somewhat uncertain as to what the current configuration of the device was regarding images. Subsequent contact with the SWG4 helpdesk confirmed that, using the then current version of the SWG4 software, legitimate websites should normally have been available with advertising suppressed. However, it was stated that occasionally (owing to problems with how that site had been written), if the advertisement failed to load, it prevented the site as a whole from loading. However, this was not common. It was possible that sites identified by clinicians as carrying

advertising were being blocked for other reasons. The situation appeared to be complex and somewhat confusing.

Other than the blocking of advertising, T4-12 felt that what was blocked was “quite arbitrary”. The communications officer T4-03 observed also that the web filter blocked “objectionable” words out of context. The pharmacist T4-04 had encountered blocking of access to an article in the *British Journal of Psychiatry*; she thought this had happened for the same reason, “something in relation to drugs and alcohol”.

8.5.3 Responses to encountering blocked websites

Responses that were referred to by participants included doing without the blocked material and looking for alternative sites, reporting the site to IT, circumventing restrictions using a mobile device on a different network, and carrying out the search at home.

T4-03 reported regarding her response to encountering blocked websites that “It depends how essential it is; for me to actually -- if I can find information that will do elsewhere, I make do, but if it is something that I think I am going to use frequently I just e-mail IT.” T4-04 hardly ever bothered to report them; her comment was, “I just shrug”. She had contacted IT only “on a handful of occasions where I have needed access to something, and I have had to ring them and say, ‘I need access to this website because of x, y, z’.”

T4-09 commented, “Personally I don’t try because I have given in trying to get the other things fixed” (this is in keeping with his report in 4.2.1.4 of poor service from the IT helpdesk). He contrasted this situation with how matters had been managed in his former Trust:

“So, if I needed, a classic one we got is when I was there we got a lot of Fol requests from journalists, we used to copy all our Fol requests to the communications department and they would have access to this website journalistlisted.com⁹¹ or something, they had access to that, being Comms., but we didn’t in Fol, and they used to say to me, ‘Oh, they are on this website, they are a journalist’, and I could never check it, and then I would speak to IT one day and they set me up straight away, they wouldn’t have a problem, they would see that there is a business need for it, and they would grant that ... but I don’t know here whether the process would work.” (Records and governance manager, T4, 9)

T4-12 was fairly sure that students used their mobile phones to circumvent blocked websites as far as signal strength, custom and policy allowed. However, she did not make clear whether the students were using 3G or 4G networks to do this, or one of the Trust’s networks (i.e., BYOD or eduroam).

Several participants (T1-04, T4-05) reported postponing their searches and conducting them at home. T3-06 was sure that users did this in T3, rather than contacting the IT helpdesk, and did not give up their search attempts:

“I think a lot of staff just ... maybe don’t raise it as an issue; if they can’t get on to it they wait until they get home ... They will do it when they get home, I am sure.” (IT manager, T3, 6)

All the Trust IT departments reported that they had established procedures for handling requests to unblock websites and web applications, which might involve consulting information governance:

“Yes, they go to the helpdesk in IT, and then it can be looked at, and usually they come then to IG if ... if they are not sure about the website ... and they will ask if we are happy with it.” (Records and governance manager, T1, 9)

⁹¹ Journalisted: <http://www.journalisted.com>.

Similar processes were reported to be in place at T3 (T3-03) and T4 (T4-20).

T3-01 described her experiences with her occasional requests to unblock websites:

“When I have experienced blocking I have just been able to flag it with the IT department and because it’s been up, because it’s never been an iffy site they will unblock it. Obviously they will ask you what site it is, ... but largely they will be things like charities or large organisations, that they can tell when you tell them what it is, and it’s fine to unblock it and the words that you are typing in ... you know they could be quite sensitive words from the fact of what we do as a Trust, so -- but like I say the response has always been quick when it has happened, and it’s been occasional.” (Librarian, T3, 1)

According to T3-06, the librarian T3-01 had never, to his knowledge, raised a request to unblock a website. He observed however that her requests may not have come to his attention because her judgement as an information professional was most likely to have been trusted by the IT staff member responsible for the secure web gateway, so that the normal requirement for line management authorisation of unblocking requests had been waived in her case:

“... There is always a chance that if [T3-01] has raised it as an issue then the chap who manages that element of the infrastructure would have just taken it on board that [T3-01] has asked for it so she is doing it in a... this is a bona fide site and it shouldn’t be blocked, so he may have just actioned it.” (IT manager, T3, 6)

T3-18 also reported that his requests to unblock websites were also trusted by IT staff: “people are aware that I ... do medicines information queries for the Trust”.

T3-06 described in more detail the process within T3 for getting a site unblocked:

“... The process [for getting a site unblocked] is to log a request with the service desk, and then ... the chap who manages that would then, would then come to me and say what shall we do in relation to this [site] ... there is having that justification from an audit perspective to say the reasons why ... so then it would be a question of doing that level of investigation to find out why it was blocked in the first place, ... and to determine what those risks were, and if I felt there was some risk involved I would probably run that past our information governance ...” (IT manager, T3, 6)

T3-06 did not explicitly admit the possibility of false positives.

In parallel fashion, T3-03 described how T3-06 would consult with her if they were in doubt as to whether or not access to a particular website or web application was allowable:

"... If they are not sure they will ring me and say, 'What do you think?' but quite often it will be [that]they will have a look at it, and ... if you say ... 'This is [x]', it is usually quite obvious what you want access to and why."

Decisions on business need in web access were made, she said, according to "... Who is asking, what the reason is, and what they want access to." T1-06 reported that blocked websites at T1 were unblocked promptly by IT:

"... Occasionally, I mean occasionally I find when I have tried to go on to -- things were blocked, but if we e-mail IT [and] ... say why we need access to the resources they usually ..."
(Clinical tutor, T1, 6)

T3-12 reported that she had needed to make the case to IT for the unblocking of some social media applications; the "default" security posture had been to block them:

"... We do have to make the case for why we think something should work in the way it does ... but I guess in terms of social media ... our IT department ... will set up blocks to certain types of social media and then we need to make the case as to why something is unblocked ((laughs)). So that is the way it tends to happen." (Communications officer, T3, 12)

In T4, T4-20 claimed that a second-line support engineer could "allow the site within minutes" once the job was in the queue. T4-12 had found that the IT helpdesk staff were prompt in responding to emailed requests to unblock sites: "I just usually send an e-mail to the IT helpdesk and say, 'This is blocked; please unblock'." However, T4-04 had found that:

"... On the handful of occasions I have asked, I think on two occasions they said they would unblock the website, and I think that took about 48 hours, a couple of days, 2 or 3 days maybe to get that sorted. And on the other occasions they said that the website was still not permitted." (Pharmacist, T4, 4)

Unfortunately, she was unable to recall what sites they were and what reasons had been given for the refusals.

The librarian T4-06 reported that unblocking of websites was “fairly quick”. The clinical teacher T4-05 had successfully placed requests with IT to unblock websites. She reported, however, that the site in question (which she could not recall) had been unblocked for her only, not across the Trust. This limited unblocking for an individual user was flatly denied, however, by T4-20, who informed the researcher that previously blocked websites, when unblocked, were made available to all users on the network.

T4-05 reported having encountering blocked websites so often that she had given up searching from her office computer and was regularly taking work home:

“Well, to be honest I’ve actually stopped accessing – trying to access now because I tend to know that it will be blocked. I did go on the library website yesterday to have a look, and ... I didn’t have a problem going via the library through to the resources – and that helped me to get through ... I think I’ve just got used to taking it home now and doing it at home, to be honest.” (Clinical teacher, T4, 05)

Promptness of IT helpdesk response in unblocking websites was not discussed by users in T3. In all three Trusts, as we have seen (8.2 above), the IT managers did not scrutinise log files of blocked websites, and appeared to depend upon user reports as their main approach to addressing over-blocking or false positives. In T4 it is likely that a great many blocked sites were going unreported.

8.5.4 Effects of website blocking

For T4-12, encountering blocked websites had not had a great impact, since she had in each instance been able to find alternative sources of information: “I have not had the occasion where I have not been able to find what I want.” However, several participants described feelings of frustration and annoyance:

“It is quite frustrating because I think ... you are, you know, I understand why it happens, you know that you are doing it with the best of intentions because you need that information, the system is not supple enough ...” (Pharmacist, T4, 4)

“I would say blocked websites are incredibly infuriating.” (Pharmacist, T4, 4)

“... It’s quite frustrating, it’s quite annoying ...” (Clinical teacher, T4, 5)

T4-04 felt that it was difficult, when working with colleagues in other Trusts, not knowing what other Trusts had access to; consistency would have been desirable:

“I think a standard approach would make such a difference; I think if you know your colleagues working at other Trusts know that you have the same access that they do and you know you can all, you know where you stand, whereas at the moment I think nobody really knows where, what sort of situation anybody else is in.” (Pharmacist, T4, 4)

The “workaround” of conducting searches at home, or working at home, has already been noted: cf. the discussion of “avoidance” strategies in Section 11.3.2. The negative effects on staff members’ work-life balance through needing to work at home were readily evident, as were the effects on productivity and on personal and organisational effectiveness caused by delays in unblocking websites and resulting from needing to take time to report blocked sites.⁹² These are clearly illustrated in T4-05’s comments below:

“... As I’ve said, it did ... impinge on my personal time [indistinct] at home where I can access the sites quite easily at home ... just generally frustrated, and it – certainly if you - with me I do quite a lot of teaching, and obviously teaching’s got to be research-based, and you’ve got to be able to access the latest information to keep everything up to date ... it just causes a delay ... you put it to one side and take that home, but then when you’re doing it regularly you’re taking it all home, and if you’ve got three or four curriculums, or ... you’ve got to update your ... teaching packages ...” (Clinical teacher, T4, 5)

The shortage of time for information-seeking reported by clinicians of all disciplines across a wide range of studies (see 2.4.4, 2.4.5 above) would have served to magnify these negative effects: if an information need at a particular time could not be met on account of a blocked website, it was unlikely to be revisited, and was likely to remain unmet unless a suitable alternative source of information could be found in a timely fashion. The effect of blocking of websites is discussed further in Section 11.3.2 below.

The researcher asked T4-20 about the possible extent to which he believed that false positives (sites incorrectly blacklisted, as described by other participants) might create problems for users. His response was as follows:

“Yes it does, yes. There is no doubt about it, with the amount of websites that are out there, you do get false positives, there are... I mean I have some particularly ... the e-mails, I can understand the frustration from users sometimes when they -- because the e-mails ... yes, ‘Why is this blocked?’ and it’s blocked because if the site isn’t categorised then [SWG4’s categorisation engine] unblocks, scans the website looking for any particular words, keywords whatever, images and then categorises based on what it can scan on the page, and if for any reason that is blocked as pornography, then that is when the users get particularly irate when they see that a site has been blocked.” (IT manager, T4, 20)

He mentioned pornography here specifically; however, there are numerous other reasons that he could have cited why websites could be blocked as inappropriate (Section 2.7.3.1). It is clear that T4-04 and T4-05, who in their roles as clinical educators undertook a great deal of web searching in the course of preparing educational material, were experiencing continuous negative effects on their working lives from blocked websites. Other participants, such as T4-10 and T4-21, frequently experienced negative effects on clinically-related information seeking from blocking of websites. Although T4-20 here acknowledged briefly that false positives occurred, and had previously mentioned processes for getting websites unblocked (see above), he conspicuously failed to give any indication that the negative effects of false positives on users’ working lives might in any way be considered a possible issue of concern within IT services. Both he and his counterpart T3-06 in T3 appeared to be focused far more on suspected or actual computer misuse by members of staff and the security risks that might thereby be presented to their Trusts. As already discussed (in the literature review, 2.6) the findings of research relating to the subject distribution of malicious websites suggest that this focus may be misplaced other than in relation to “adult” content.

8.5.5 Awareness of national measures

One of the agreed follow-up actions from the TDAG survey (described above in Sections 1.4.5 and 2.7.3.4.2) (TDAG, 2009b), was the setting-up of a national whitelist of “domains not to be blocked” within the NHS. It will be recalled that library managers were intended to send the updated versions of the whitelist to their Trust IT departments as soon as they received them from their local TDAG representative, for the necessary configuration changes to be made to the Trust SWG. However, none of the IT managers in any of the Trusts appeared to be aware of the list. Among the librarians, T3-01 and T1-01 were both aware of the list, but said that it was not implemented within their respective Trust IT departments. T3-01 indicated that this was because in T3 there was so little trouble with the blocking of content. Neither librarian had been asked by end-users to intervene in

instances where web content was blocked. The records and governance manager T3-09 was unaware of the list, as were the library staff at T4 (T4-06, T4-07). It was evident that within the Trusts in the study the processes for maintaining, publicising and implementing the national whitelist were not working as originally intended.

T3-06 reported that he had not seen the letter from NICE regarding browser requirements for the administration of OpenAthens and the link resolver (see below, Appendix J). T1-12 did not indicate whether or not he had seen it; he did indicate, however, that T1 was no longer tied into any NPfIT contracts for systems requiring the use of older browsers. Owing to shortage of time in the interview, the researcher was unable to ask T4-20 whether he was aware of the letter. The letter had not been addressed to named individuals; it is possible therefore in T1 and T4 that it had been received by the Head of IT (T1) and the Director of Informatics (T4) but not forwarded to other staff.

8.6 Information governance and education

Issues relating to information governance and education were very little discussed by participants. They arose in only two contexts: making available conference presentations, and making audio-visual recordings for teaching purposes.

T4-11 advised the researcher that, when presentations were sent out to the participants of paediatric conferences, particularly paediatric nephrology conferences, images of children were removed from the presentations. He was unclear, however, as to whether this was a matter of formal policy, either within Trust information governance or from the university medical school, or what the precise rationale might have been.

The other issue arose in connection with a project to video record clinical scenarios for teaching purposes proposed by T4-22:

“... The idea was we were going to put some cameras in an A&E department and we were going to have almost a button on the wall which ... you hit to video what was going on. And the idea was that it was a way of ... actually analysing ... a variety of different things, but getting some feedback about real clinical events ... We had huge equipment issues because we found a really nice piece of equipment that would do all that, we could put it in a secure cabinet above the false ceiling and do all the rest of it, but and it would record to a memory stick or a hard drive incorporated but it wouldn't ... do any of that on an encrypted memory stick ...” (E-learning specialist, T4, 22)

One of the restrictions that had been imposed was that the memory stick needed to be encrypted in case a video showing real patients was inadvertently lost, thereby resulting in an information governance incident. He had therefore been unable to proceed with the project.

8.7 Use of mobile devices

National and local policies significantly shaped the Trusts' information governance and security policy and practice in respect of mobile devices. National policies were discussed in Section 1.4.4 above. Reference has been made above to Trust policies and requirements relating to mobile devices: T1 pharmacy department's prohibition of the use of mobile phones on the wards (7.6), T3's prohibition of the use of smartphones in clinical areas (5.6, 7.6), T4's BYOD policies (4.5.3), and perceived departures from policies (5.6, 7.6).

8.8 Summary

In summary, this chapter provided an account of the implementation of specific security systems and policies in terms of their effects upon information seeking and use. These included acceptable use policies, monitoring of staff web use, the use of secure web gateways, use of mobile devices, and endpoint security.

Acceptable use policies, while they varied in tone (with that of T4 being notably minatory) were broadly similar in content in relation to allowable personal web and email use and to categories of unacceptable web use. Although review dates were specified, no mention was made in any of the documents of processes for monitoring the effects of the policy. All the Trusts had processes in place for individual monitoring of web use in cases of concern, i.e. in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA) and its associated code of practice, whether the Act was actually referred to or not. Although attempts to access websites that were blocked were not followed up in any of the Trusts, several clinical staff reported concerns about the possible repercussions of these, and one (T1-04) reported that it inhibited her search activities. The T3 IT manager was concerned about overall levels of recreational web use, on which he reported regularly to an information governance committee. None of the Trust IT departments scrutinised log files of blocked websites to assess filtering accuracy, citing lack of time to do so; they appeared to depend solely upon user reports as their approach to addressing over-blocking or false positives. However, users frequently did not report blocked websites, preferring to look for alternative material to meet their information needs, or to carry out searches at home.

Promotional material for the three SWGs appeared to reflect different corporate attitudes on the part of the vendors to the possible over-blocking of legitimate websites. That for SWG3 acknowledged the possibility of over-blocking of legitimate websites as a likely issue for NHS services; those for SWG1 and SWG4, however, focused solely on prevention of inappropriate web use. SWG1 and SWG3 offered fully granular control of Web 2.0 and social media websites, whereas SWG4 did not, with potential implications for social media management at T4. IT departments had implemented default configurations for web filtering, and, other than “rationing” access to Web 2.0 and social media sites at T1, had not made use of other configuration options.

The reported deficiencies in endpoint security, i.e., the ongoing use of Windows XP and older browsers, lack of screen locking (T1) and lack of USB port blocking (T4), represented potentially serious information security risk factors for their respective Trusts.

Perhaps surprisingly for a teaching and research institution, evidence of frequent blocking of websites, affecting the work of clinical educators in particular, was found at T4, but not at T1 or T3. In general, sites appeared to be blocked either arbitrarily, on account of their containing content relating to sexual behaviour, drugs, or self-harm (T3), or of their inclusion of images, particularly advertising images (T4). Users frequently did not report blocked websites, preferring to look for alternative material to meet their information needs, or to carry out searches at home. While all the Trusts had procedures in place for getting legitimate websites unblocked, times taken for this could vary within a Trust, the longest reported being 48 hours at T4. Delays in unblocking sites, and the need to work at home, were reported by one clinical educator as adversely affecting her productivity and work-life balance (T4-06).

Neither IT managers nor librarians appeared to be aware of the national whitelist of “domains not to be blocked” within the NHS, suggesting that its management and dissemination needed to be reviewed. Similarly, IT managers did not appear to be aware of the letter issued by NICE relating to libraries’ browser requirements for link resolver and OpenAthens administration, indicating again possibly that the dissemination strategy had not been fully effective, although in practice the required browsers were available to library staff in all Trusts under the terms of general policies. The lack of awareness of these initiatives may have reflected the general “bureaucratic and administrative fatigue” characterised in relation to NHS IT by Solomon, Beale and Lennox-Chugani (2016).

The following chapter goes on to consider policy issues that relate particularly to corporate and individual staff communications, mainly as they relate to social media.

Chapter 9. Findings: communications policies and practices

9.1 Introduction

This final results chapter sets out the findings relating to the remaining main theme, communications policies and practices, as these relate both to Trust and to individual professionals. The only relevant 'column themes' under this heading are social media and mobile devices; the chapter therefore begins with a consideration of social media. The content coverage is illustrated in Figure 9.1.

9.2. Web 2.0 and social media

9.2.1. Web 2.0 and social media policy in relation to media strategies

Policy and guidance for all Trusts were intended to cover both work-related and personal uses of social media from wherever they were accessed.

T1 had produced a specific policy regarding social media (SoMe1) and had treated the use of social media also in its IT acceptable use policy (AU1). SoMe1 had been published only within the last few months (T1-09). T4 briefly mentioned social media in AU4Int, and had produced a separate social media guide (SoMe4) for staff. T3 briefly referred to social media within AU3, and had incorporated brief coverage of social media within its overall media relations policy (SoMe3). The research directorate of T4 had produced its own social media guide for staff (SoMe4-Res), incorporating information about ethics requirements relating to the use of social media for purposes such as recruitment of research participants (T4-03).

The departmental responsibilities within each Trust for social media policy and guidance were varied. In T1, SoMe1 was the responsibility of the information governance manager. In T3, SoMe3 was held by the communications department. Within T4, AU4Int was held by the informatics department, and SoMe4 was held by the communications department in association with human resources and union representatives. Responsibility for departmental social media guides lay with the individual departments.

SoMe1 and SoMe4 both incorporated general positive statements about the advantages of health professionals' using social media. SoMe4 referred to the benefits of sharing knowledge and skills outside the organisation, acknowledging the existing uses of social media by staff members, and the Trust's wish to encourage and support these. SoMe1 cited opportunities for research, raising awareness of topical health issues, public engagement and the chance to establish a wider and more diverse professional network. However, it also indicated that blocking access to social media for most staff within the Trust was a matter of policy, while acknowledging that many staff were accessing social media via personal mobile devices.

All policies referred to the need to ensure the operational effectiveness of the Trust and to avoid bringing the Trust (in T1, also the NHS) into disrepute. Also they all referred to the need for professionalism in the use of social media, and incorporated standard warnings not to breach confidentiality directly or indirectly through the posting of PII or photographs online, or through sharing information about the Trust that was otherwise sensitive or, as in T1, subject to non-disclosure agreements. SoMe1 provided some brief scenarios to illustrate the confidentiality issue with respect to PII. The policies also specifically prohibited the posting of material likely to contravene diversity or bullying and harassment policies, or that was in any other way illegal. All stressed that disciplinary action could be taken for inappropriate use of social media, including possible dismissal, and that civil proceedings or criminal prosecution could also result.

SoMe1's instructions were the most detailed and prescriptive. They stressed the need for factual accuracy on social media and for inaccuracies to be corrected in a transparent way. Staff were enjoined not to post any photos on personal social media sites of themselves or colleagues in uniform, or in an identifiable work setting, and to work on the basis that anything they wrote or posted could be shared more widely without their knowledge or permission. They were enjoined to use their real names if they were associating themselves in any way with the Trust. They were also warned that posts under a pseudonym could become admissible in a disciplinary investigation or hearing if, at a later stage, these posts became associated with the staff member's real name. Procedures were established for what actions a staff member should take should he or she feel harassed, bullied or victimised as a result of another member of staff's post via a social media site.

SoMe3 was brief in nature. It prohibited posting of PII and of illegal content. It stated that SoMe content should represent T3 and not offer personal opinions or views. Staff were strongly advised to consider the implications of any material published online. Staff wishing to utilise SoMe tools

extensively for the purpose of sharing information in a professional capacity were enjoined to seek advice from the communications team.

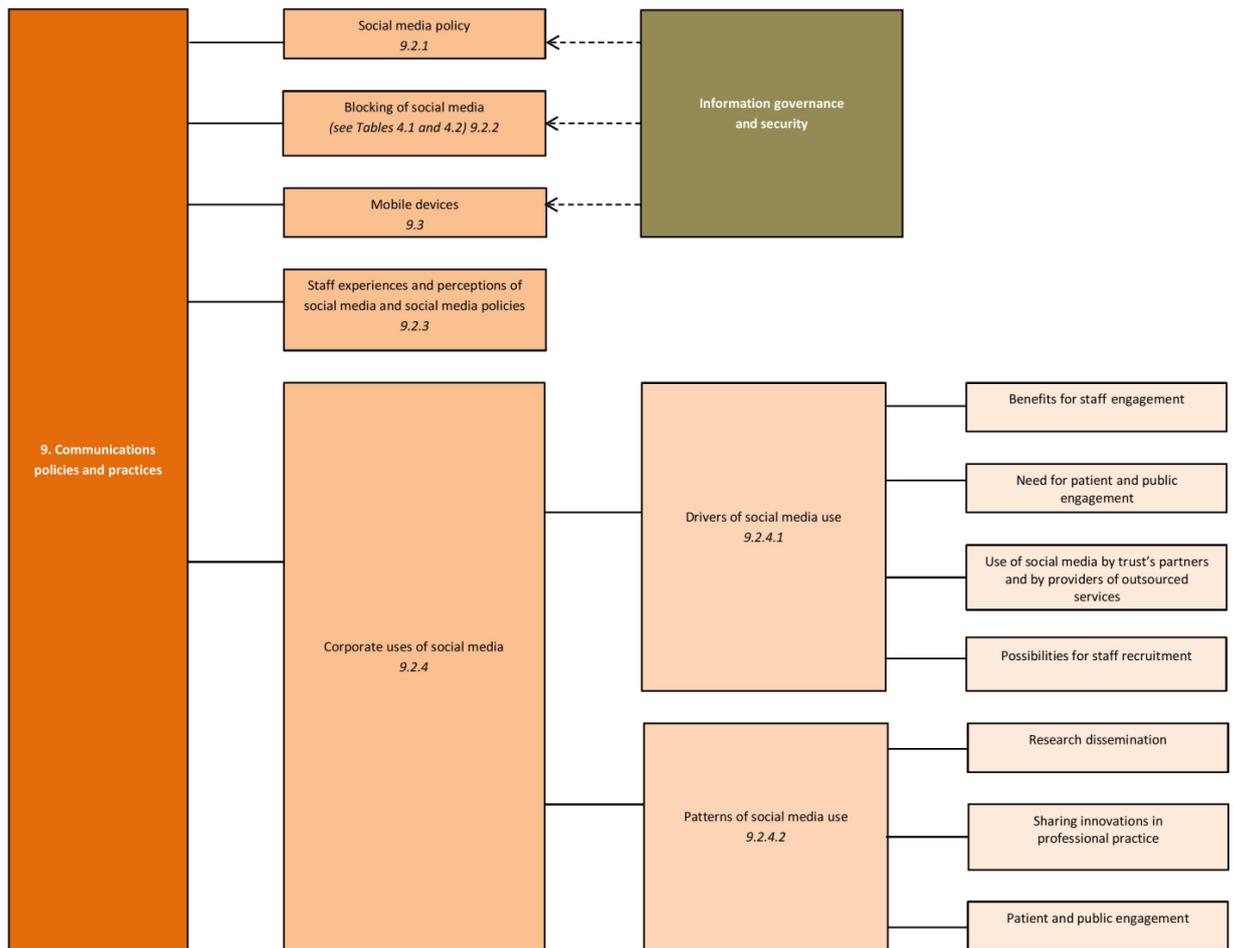


Figure 9.1 Communications policies and practices

SoMe4 included recommendations regarding privacy settings and general safe behaviour online. It stated that the posting of photographs on sites such as Facebook required specific permission from the subjects. It stressed that staff were responsible not only for content that they posted themselves on social media sites, but also for the content of comments that they permitted to be displayed. Staff were enjoined to refrain from identifying Trust colleagues by name, as well as patients, and to refer to social media guidance produced by their own professional body or regulator, as applicable.

SoMe4's position on access to social media within the Trust network was not stated formally; however, essentially, staff who could not demonstrate a specific business need for access to popular social media applications such as Twitter and Facebook were blocked from accessing them. Requests

for access required to be authorised by a line manager (T4-06). However, staff members who were unable to access social media from their desktop computers frequently did so from their own mobile devices via the BYOD network, on which the security settings were intended to be less restrictive. According to T4-22, however, in some instances, the settings on the BYOD network were more restrictive than those of the Trust network. Similarly in T3, access to “professional” sites, such as LinkedIn and Academia.edu, was routinely allowed, but not access to Facebook, Twitter etc. Not all participants were aware of their Trust’s policies or guidance on social media; for example, T4-08 and T3-07 stated that they were not.

The implementation of Web 2.0 and social media policy in T1 appeared to be the subject of considerable confusion. Contradictory accounts of T1’s policy were given by different participants, as can readily be seen in the accounts below of policy and practice regarding the availability of specific applications. It was seen earlier (in Section 4.4.4) how the practice of setting quotas for the usage of particular web applications had not been publicised.

Policy, experiences of misuse, and attitudes appeared to be closely inter-related. The senior nurse manager T1-07 commented on the orientation of SoMe1 regarding social media, suggesting that incidents involving their misuse, and in particular a breach of confidentiality, had given rise to the Trust’s initial negative stance, which was now softening to some extent:

“So I think we have taken a very, very firm stance around social media, and actually I have to say I think, I think at the time it was right because it has really raised the profile of the importance of ... confidentiality in the organisation, so I think it has got-- a very strong message went out to all staff that Facebook, ... social media, can have, cause some real problems if we are not careful with it. People have got that message, so now -- that is great and we can start to backtrack a little bit, relent, and so we have got a social media policy.”

(Senior nurse manager, T1, 7)

The breach of confidentiality on Facebook had been the act of a clinical staff member, leading to her dismissal (T1-02, T1-09). T1-12 reported similarly that there had been serious incidents at T1 involving social media, which had led to the policy decision to impose a complete block on access to popular social media applications within the Trust network:

“Social media sites are blocked on Trust PCs, so you can’t access Facebook, I couldn’t access Facebook or Twitter from ... my PC ... and the Trust very much took that view ... because ... there were a number of incidents related to staff ... inappropriately using those sites during work time. So, that was the view ... because it was misuse ...”

“... In a previous role I held in the organisation as a lead nurse ... I had to discipline two senior members of my nursing team where it was reported to me that they weren’t doing their jobs on nights, where they were not responding ... (Senior nurse manager, T1, 12)

T1-12 had asked IT to investigate. The report indicated that they had not moved from the computer for 3½ hours and had been accessing Facebook and a variety of other non-work-related websites:

“Well, they are not employed to be on Facebook for 3½ hours, so ... there were decisions made then at an organisational level, that actually we can’t have ... staff, the decision was we can’t ... trust staff to use it sensibly, we can’t ... trust staff to ... use it sensibly in their break, ... so ... the decision was to block it from all Trust PCs.”

(Senior governance and risk manager, T1, 12)

This represents a restrictive response to what was reported to have been a single (albeit flagrant and extremely serious) instance of misuse. However, according to the clinical tutor T1-06, there was not in fact a complete ban at all: access to social media websites was allowed during breaks. T1-06 reported that she was able to access professional Twitter feeds and blogs from her desktop computer, suggesting that these were not blocked.

T1-12 outlined how SWG1’s settings were configured in relation to social media websites:

“So we used to block Facebook, MySpace, BeBo, Twitter. Websense now allows you to take a granular approach to it, so we can now allow access to Facebook, but we don’t allow access to Facebook chat, we don’t allow access to ‘add new friends’ and ‘accept friends’ and that sort of thing, so if somebody has got a ... work reason, professional reason to access Facebook they can do, ... same with Twitter; ... we have got granular ... security through [SWG1] that is set up on that.” (IT manager, T1, 12)

When asked whether access to social media websites was allowed only to particular categories of staff, he responded as follows:

“No ... we don’t block websites based on the staff member, we base it on the website and the category of website. So [SWG1] has ... snap-ins built in for Facebook and Twitter and all the popular sites, so you can say, ‘Yes, I will allow access to that, yes I will allow access to that’. The same thing, what we generally do is we will add a quota on each and say, ‘Right ... in your day you will have 30 minutes of quota for sites that we don’t just allow wholeheartedly’, so ... like games websites, social media. I think YouTube is on that, without looking I am not 100% sure, but we ... “ (IT manager, T1, 12)

As described in 8.3 above, the quota system was flexible in that a user could ask to have a usage quota for a web application increased for specified business purposes, with subsequent usage being audited. This facility had particular application to the use of personal cloud storage applications and also online presentation applications such as Prezi, both of which were categorised by SWG1 as “personal online storage”.

T1’s practice accorded with current industry trends:

“Granular controls for social media are becoming one of the most requested features in Web security solutions as businesses and organizations are increasingly realizing the benefits of granting employee access to social media. In the past, social media controls were often binary and businesses would either completely block access or allow totally unregulated use. Many Web security vendors now offer granular controls that allow businesses to provide a safe and controlled social media experience for users based on different needs and policy criteria.” (Radicati Group, 2012, p. 6)

As we have seen, however (Section 8.3 above) similar granular controls do not seem to have been implemented at T3 and T4, despite the fact that the respective SWGs offered this facility. By contrast with the serious incidents of misuse at T1, the HR manager T3-09 reported that no serious breaches of confidentiality via Facebook or other social media site had occurred at T3, only instances where some “inappropriate” content had been posted, details of which were not given. No information governance incidents specifically involving social media were reported either at T4. Details of other types of incident currently under investigation at T4 (there were reportedly several) were not disclosed.

9.2.2 Blocking of Web 2.0 and social media applications

The availability and status of individual social media applications was described above in Tables 5.1 and 5.2. The restrictions in T1 and T4 on access to blogging and microblogging applications (WordPress, Twitter) and in T3 and T4 to content communities (SlideShare, YouTube, Prezi) were noteworthy in particular, since anecdotal evidence indicated considerable usage of these applications by health professionals in relation to information behaviour.

9.2.3 Staff experiences and perceptions of Web 2.0 / social media use and related policies

Aspects of usage of social media in relation to information seeking and sharing are described also in section 5.5. Social media and professional norms are discussed in 7.5.

Several participants provided indications of a pronounced generational divide in attitudes to, and use of, social media, with senior staff avoiding using them entirely, or using them only in non-work contexts:

“I think most of, I can happily say that most of the more senior staff in the department don’t use social media in either their personal or work life ... the younger ones do use it. I know the ones who are sort of in the middle band have used it and then have realised that it wastes half their life and have stopped using a lot of them. I am only saying what they are saying to me; I don’t use them.”

(AHP clinical lead, T2, 2)

Several other clinical staff (T4-19, T3-20) similarly expressed views of social media in general which were negative or indifferent.

T1-01 suggested that attitudes to social media would change markedly over time as the younger generation of staff were appointed to management roles:

“...The higher up you are in the organisation, the older you are likely to be and the less technically aware you are ... 5 years, 10 years, the people who will be in charge of the organisation will be the ones who have grown up with all this stuff and are comfortable and familiar with it, so I think it is a changeover, it is this X and Y Generation thing, isn’t it? I think we are on the cusp of the power shift ...” (Librarian, T1, 1)

In discussing social media policy, the senior nurse manager T1-07 emphasised the serious consequences of breaches of confidentiality, both for patients and their families and for the organisation as a whole:

“We need to get the balance right between recognising the benefits of social media and the risks of using social media; ... if we ... breach patient confidentiality, then the implications of that for us as an organisation [are] absolutely huge. So that does tend to make us a wee bit ... risk-averse, ... just because we will have -- it damages the reputation of the Trust, it puts patients in fear of sharing information with us, because then they wonder where is it going to go, who is going to have access to it, and so we ... have to get that balance right ... to think that there is the opportunity that that could actually be out in the public arena is just ... devastating for all the patients and families.” (Senior nurse manager, T1, 7)

It was striking here that she used the term “risk-averse” in relation to the Trust’s policies, and offered a justification for this approach; compare here T1-02’s comments in Section 4.5.4 above, the account of NHS organisational culture in Section 2.5.5 of the literature review, and the general discussion in 11.4.1.

T1-02 characterised the Trust’s policy as follows:

“Here we have an IT ... led approach to computer misuse, so things are very tightly controlled, often blocked, and – and that’s the approach that this trust takes, which in terms of ... cultural progress down those sorts of like ... thinking about social media and the uses of social media ... it’s really restrictive ... we ... can’t access any social media here ...”

T1-02 candidly expressed her personal disagreement with it:

“I don’t necessarily agree with that, because I think it lies in both camps, really, there’s a responsibility on both sides for ... control of misuse, but ... I tend to feel, or think, that ... people are adults at work, and as such ... these are resources, and it feels a bit archaic, really, to block usage completely ... where it could be really useful.”

In her view, use of social media by NHS Trusts was a very important tool for public and staff engagement, and T1 through its current policy was missing a major opportunity:

“In my ... profession, which is ... resourcing, really, you see huge benefits where companies have embraced social media and are putting – they’ve got a presence ... and they use it – and you see it in the NHS, you see other trusts doing it. [H13] down in ... London – absolutely fabulous – using their Twitter feed, and things like that, and ... it has a huge effect on the staff who work there, because they feel like [H13] people, that ... ‘Look how fantastic your trust is – isn’t this a great place to work?’ And ... we miss out on that, and part of it is because of the massively restrictive and quite old-fashioned, I think, approach to IT security, which is just to block it and not to discuss it, and that’s it.” (HR manager, T1, 2)

The records and governance manager T1-09, by contrast, was personally in favour of a total ban on access to social media websites:

“Yes. I mean to be honest I would rather them all blocked, Facebook included.”

She mentioned a report she had recently read in which the top ten websites accessed by public sector staff had been listed:

“The majority were ... personal e-mails, Facebook, things like that, not for work purposes, and I just wonder if that is going on here.”⁹³

Here it is evident that she was concerned about the possible adverse effect that access to social media websites could have on productivity:

“... it kind of blurs the boundaries of what is acceptable and what not.”

(Records and governance manager, T1, 9)

The librarian T1-01 and her colleagues had found recently that the online presentation application Prezi⁹⁴ and cloud storage applications had suddenly been blocked without warning. This had had a particular impact upon the library, because her induction presentation was in Prezi and could not

⁹³ The researcher was unable subsequently to locate the report concerned. It is possible that T1-09 was referring to the report of the TaxPayers Alliance publicising the extent of personal web use at the Department of Work and Pensions (TaxPayers Alliance, 2010) or an article in the *Daily Telegraph* on social media and personal web use at the Department of Communities and Local Government (Hope, 2012).

⁹⁴ Prezi: <http://prezi.com>

readily be migrated to another platform. SlideShare,⁹⁵ an application for hosting and sharing presentations, was also apparently blocked.

When asked about the status of Prezi within T1, the senior risk and governance manager T1-12 responded as follows:

"I honestly don't know, and I wasn't aware that it was blocked. In fact it was ... the postgrad medical centre who told me, because it was ... I can't think, it came to light at a meeting I was at, that said that Prezi, someone had wanted to use Prezi and they couldn't, and I said, 'Well, I can't see why we couldn't use it', so I am actually raising it with IT to say, 'Why can't we?'" (Senior risk and governance manager, T1, 12)

According to T1-09, IT had referred an unblocking request for Prezi to her:

"... We weren't sure, it was questioned basically -- it wasn't necessarily that we saw that it was Prezi and thought right, absolutely not ... it, the way that it was on the web was questioned by IT and that just to see if IG was happy with it, and because it is cloud-based ... you have to be ... careful because if they are presenting patient information on [the] cloud then it can be open for all on the intranet, Internet, sorry ... so it was just basically ... to look at exactly what they wanted and see if it was acceptable or not; it wasn't blocked in the end." (Records and governance manager, T1, 9)

It is unclear from this account what the nature of T1-09's concerns were about the application being "cloud-based": whether about possible non-compliance with the Data Protection Act requirement not to transfer personal information outside the European Economic Area without specific consent or entitlement to do so, or about possibly inadequate security within the application itself, or both. Her account suggested that Prezi was still normally blocked and had been unblocked for one user only, whereas that of the IT manager T1-11 indicated that it was available to all staff, with a quota set for usage. The most obvious explanation could have been that a new quota-based system of social media controls had been implemented by IT department, perhaps on an experimental basis, without prior consultation with the information governance managers; however, this seems at first sight unlikely.

⁹⁵ SlideShare: <http://www.slideshare.net>

T1-01 stated that she “had been campaigning about social media for some time”, attempting unsuccessfully to implement a number of services based on social media applications. She felt that the blocking of web applications was essentially a matter of lack of understanding, and related to attitudes which were generationally-based. She felt that this applied to Prezi in particular:

“ ... What you do in Prezi you can also do in PowerPoint or Word – you know, click of one button and it’s uploaded to the Internet ... (Librarian, T1, 1)

T1-01 had also, in the past, been blocked from creating a library film club blog, despite receiving advice from the Trust’s legal services that this would be permissible, and suggestions from them as to the drafting of an appropriate policy. She had been told officially that no Trust-related social media activity would be allowed until the social media policy had been developed, which, in the event, had taken several years, and at the time the interview was conducted had apparently still not been officially launched.⁹⁶

According to T1-01, restrictions on access to blogs and blogging platforms were affecting the library’s distribution of the current awareness bulletins produced by local libraries, entailing extra work in producing PDF or Word documents:

She remarked on the transient nature of some social media applications: “sometimes you’re just getting up and running and the resource has gone”, “a lot of these things ... are fairly faddy”. She also noted the difficulty of evaluating the impact of a library presence on Facebook and Twitter. Her preference would have been to use blogs and wikis: blogs “basically as a tool to sit behind whatever I do” and wikis – “it’s an internal communication thing between the Trusts”. She appeared to think that internal, NHS-specific systems held more promise for professional networking than public platforms such as Twitter and Facebook. While she was well aware of CILIP’s exhortations to librarians to use social media within their services, she felt that staffing issues made it difficult, in practice, for NHS libraries to maintain an effective social media presence.

Regarding information governance incidents relating to social media, T1-01, although not referring to specific past incidents, took a pessimistic view of the likely future response: “I think if something should happen, that it would be a very reactive culture.” She felt that changes in the Trust’s culture

⁹⁶ By the time the researcher interviewed T1-07, it had just recently been published.

and policy relating to social media would come about in the near future through external pressures, notably moves by bodies such as the medical royal colleges to integrate social media within their ways of working.

The perception of the training staff at T1 was that the Trust's restrictive social media policy, and its web filtering practices in general, represented a desire on the part of the senior management to exercise organisational control for its own sake. T2-01 expressed the view that the corporate attitude to social media in T1 was generally negative. Her own Trust, T2, she thought, was "slightly more forward-thinking in terms of using social media".

9.2.4 Corporate uses of Web 2.0 and social media

9.2.4.1 Drivers

The decision to use social media corporately in T3 was described by T3-09 as driven fundamentally by the need for patient engagement, particularly in child and adolescent mental health services:

"... There was resistance for quite some time for things like Twitter accounts and ... but we have gone very much now, I think -- it's once you have breached the Rubicon [sic] ... you are in the social media, you make the decision that we are going to engage and we are going to use it, and I think because we have ... service users we are trying to engage in who are ... child and adolescent mental health, and if that is the most relevant way to engage with them we ... had to do it, we had to understand and provide for that ..."

She said that the use of social media platforms by the Trust's partners and providers of outsourced services had been a factor in the way that use of social media was gradually spreading:

"It is ... just in a ... non-anxious way, if that sounds right, because there has been a lot of anxiety, and I don't know if that's just me and where I sit in the organisation, because for years we talked about Twitter and forums and ... the pitfalls of both, and now it just seems to be gently washing in, and we have got this policy and everything seems much more enabled, so obviously the first test will be when there is something inappropriate."

(Human resources manager, T3, 9)

T3-09 felt also that the work on social media published by NHS Employers (NHS Employers, 2013a, 2013b, 2014), and its then chief executive's role in this, had been decisive in influencing her own view: *"He was the one that turned around social media."* She was not herself active on Twitter, but

followed his and several other Twitter feeds as a professional resource: *“I like to see and hear what is going on.”*

For T3-12, the rationale for using social media was about going to where people are:

“If you think of the use of social media from a communications point of view, it is being where people are at ... you go to there to have a conversation with them rather than expecting them to visit you on your corporate Trust website or in your corporate Trust magazine, and so ... it is just another media channel.”

She felt that there was a necessary balance of risk and reward in using social media:

“And I think that is probably where you have come across the term risk, because I think it is a balance of risk versus reward, and obviously there is a huge potential reward for engaging with communities via social media, but you do have to have the safeguards in place, so that has always been the sort of approach that this Trust has taken, is that if we are going to extend access to channels like this, there is some responsibility that individual staff members take on, around their responsible use of that media ... and we have evaluated the risks and deemed them to be acceptable.” (Communications officer, T3, 12)

In T1, use of social media corporately by the Trust was only just beginning to be discussed:

“We are only at the stage where it is currently being discussed - I’ve written up a proposal which has been approved by my exec. ... and it’s going to go here, there and everywhere for approval.” (Communications officer, T1, 3)

In T1, the local drivers for social media use were perceived to be its possibilities for recruitment of staff (T1-03), provider and partner organisations’ adoption of social media (T1-01), and perceived benefits for staff engagement and the health of organisational culture (T1-02). The T4 communications strategy contained no specific references to social media use.

T1-03 reported that he had personally been resisting the idea of venturing into use of social media for some time, on account of lack of resources. Unlike T3 and T4, which had well-staffed media and communications departments, T1 employed one communications officer, supported by a part-time assistant, to carry out a wide range of duties which included editing of staff newsletters and moderating the trust website and intranet. His time was therefore already very limited: he reported that he had “been fire-fighting for years”. T1-02 felt that, apart from the information governance

concerns about social media identified in 9.2 above, other organisational factors had contributed to a resistance to the use of social media:

“The culture in – in many Trusts, which is, like you said, not to engage in ... professional social we- networking at work, because it’s perceived to be perhaps ‘slacking off’ or people potentially not ... having the time, and ... not having the right environment or mind-set to do it ... So, and then you ... lose lots ...” (Human resources manager, T1, 2)

9.2.4.2 Patterns of Web 2.0 and social media use

The only presence that T1 had on social media was via some videos on YouTube promoting its newly-refurbished maternity unit. T1-03 had reserved a number of Twitter handles for future use.

The Trust charity had a Facebook page, but not T1 itself, other than an “unofficial” page on which some quite negative feedback had been left about the trust’s services. (This may have been something that T1-03 was alluding to in a comment he had made, “There are conversations going on out there about us that we can’t easily respond to”.) Apart from the additional workload, T1-03 was concerned about how to handle negative comments on social media:

“And what also was worrying me is if ... former patients ... what can I say - hijack – though that’s not the word I mean – if they ... if they bombard us using that ... it’s obviously very public ... and it is ... a case of – OK, well we would have to work out how will we respond to these ... professionally to try and nip it in the bud and ... – so as well as responding to them it is also - once – once you have a social media presence you can’t leave it. You have to have a cycle of things going on ...” (Communications officer, T1, 3)

T1-03’s expectations regarding feedback from patients were notably negative; he evidently perceived patient feedback on social media as needing to be “managed” or “controlled”, rather than presenting any kind of opportunity to improve service delivery. In T3 and T4, Twitter and Facebook were used extensively for patient and public engagement, for research dissemination, and for sharing innovation in professional practice. In each case, social media activities were closely regulated, mainly by the communications department of the Trust.

In T3, there was no corporate Facebook page as such, but use of Facebook had been successfully piloted within locality health promotion services. The T3 Twitter feed was active in retweeting general items about mental health which were thought to be of interest to followers. In T4 there existed an umbrella corporate presence on Facebook and many separate Twitter feeds for individual

departments and services. The Facebook page, however, appeared to feature mostly news items from the “media centre” of the main Trust website. According to T3-12, T3’s various forms of social media presence were clearly intended to form part of an overall media strategy:

“We approach our use of social media channels strategically, so if we are going to do something, we do it with an objective in mind”. (T3-12)

The creation by the library at T4 of a current awareness portal and Pinterest site has already been noted (Section 5.5).

9.3 Mobile devices

The general NHS policy requirements relating to portable media and devices, including mobile phones and tablet computers, were set out in Section 1.4.4.

T1 did not have a discrete mobile devices policy as such. However, a number of policy restrictions on the use of mobile devices appeared to be in operation, including a general prohibition on the use of smartphones in clinical areas. The rationale for this appeared to relate primarily to risk of breaches of confidentiality or privacy. T1-07 observed how such breaches could be entirely inadvertent. She noted how easy it was inadvertently to include a patient in a photograph when the focus of the photographer’s attention was elsewhere; this could result in problems of informed consent and breach of privacy, if the photograph were subsequently to be posted to a social media website. An incident of this type had occurred in the recent past. As discussed in 7.6, the pharmacy department prohibited the use of mobile phones in clinical areas by its staff (T1-04). According to T1-01, BYOD was specifically prohibited within T1.

T3 was the only one of the Trusts to have a specific mobile devices policy. According to T3-18, it expressly prohibited the use of mobile phones in clinical areas. However, such a prohibition was not found explicitly within the text of the policy, which enjoined users only to “be aware of, and respect, local policies regarding the use of mobile communications devices”. Users were warned that all calls made on Trust-provided mobile phones were logged by the network provider, and that “there should be no expectation of privacy in anything created, stored, sent or received” on one.

T4 incorporated its mobile devices policy within AU4Sec. All Trust-owned mobile devices were required to have MDM enabled on them, allowing monitoring of application deployment, location tracking and remote wiping of the device. Mobile apps that were installed on Trust-owned devices

were required to be licensed and purchased through authorised sources. As far as possible, users were enjoined to avoid storing Trust data on mobile devices.

9.4 Summary

Individual use of popular social media platforms and Web 2.0 resources was restricted in all of the Trusts to varying extents. In practice, T3 was the most restrictive. A distinction was commonly made between “professional” and “recreational” resources, with Twitter, despite its increasing professional use, generally perceived as “recreational” in nature. Social media were sometimes felt by research participants to be suitable only for personal or recreational use (*cf.* Ward et al., 2009). They were often perceived as high-risk, especially by nurses and AHPs, based on concerns about privacy and confidentiality and of maintaining appropriate professional boundaries with patients and with students. Professional online forums hosted by professional association websites (e.g. iCSP) were favoured by AHPs as a means of communication and networking, but were not always accessible within NHS network environments, with evident implications for this group of clinicians. Noticeable generational differences were observed in use and expectations of social media, with students and younger colleagues being perceived as heavy users, but colleagues within the same age group far less so, with implications for enculturation and informal guidance in e-professionalism. Corporate use of social media for external relations was well established at T3 and T4, but only just starting at T1. Individual services at T4 also used Twitter for internal communications. While the three Trusts were at different stages of implementation, a gradual process of acceptance was evident across all the Trusts in respect of corporate use of social media. External drivers of this that were mentioned by participants included NHS Employers and professional bodies. There was also an apparent increasing awareness of the possibilities afforded by social media as tools for patient, public and staff engagement.

Regarding personal use of social media, organisational and system policies facilitated this to some degree (the quota system in T1 and the BYOD network in T4), but also reflected a continuing organisational ambivalence. Policies and guidance produced by regulators (e.g. the Nursing and Midwifery Council (NMC), the General Medical Council (GMC), and the Health and Care Professions Council (HCPC), were increasingly known to be available, on which training in e-professionalism for students and trainees could be based. The educational usefulness of YouTube content appeared to have been recognised to some extent relatively recently by IT departments, although restrictions were still in place; compare the findings of Elcock (2016), which are presented in full in Appendix P.

A discussion of the adoption of social media for corporate communications in terms of models of diffusion of innovations will be presented in Chapter 11.

Chapter 10. Findings: synthesis of results by Trust

A synoptic overview of key findings for the three Trusts is set out in Table 10.1 for comparative purposes, drawn mainly from Chapters 5 to 9 but incorporating some material from elsewhere, notably Section 4.4.4. The main findings are considered below in terms of various aspects of the Trusts' organisational performance and dynamics as discussed in Sections 4.1 and following above: financial management, innovativeness, digital maturity, information governance, and working relationships with IT services. (Digital maturity is considered here in general terms rather than with reference to a specific framework.)

10.1 T1

T1's organisational performance overall as indicated by most key metrics (Table 4.2) appeared to be relatively good. However anecdotal reports indicated that it suffered from ongoing medical staffing shortages, and the annual reports indicated that it was in financial deficit, reported as >£1m in 2014-15, reduced from >£12m the previous year. Some of the non-clinical services with which the researcher had contact (information governance, research, communications, IT, training and development) appeared understaffed. This appeared to raise questions concerning T1's capacity to respond to environmental challenges, and to deliver improved effectiveness and financial savings, through innovation in its operations and services. Its strategic objective of reducing management costs, as indicated in its 2013-14 annual report, is likely to have related to deficit reduction measures and to these low staffing levels. In comparison with other NHS organisations, T1 could be considered a 'laggard' in terms of organisational innovations such as e-learning and use of Web 2.0 and social media applications.

In some respects, T1 did not appear to have a high level of digital maturity. The fact that development of its IT strategy had been outsourced, as reported by the IT manager T1-11, suggested a lack of in-house capacity for strategic planning in terms of IT. It was reported as not yet having a full EPR system, though one was planned. Its IT services were, according to participants' reports, not particularly "user-friendly": there were shortages of PCs in clinical areas, remote access to Trust systems did not always work well, and its current intranet (scheduled for replacement) was out of date and 'clunky' in terms of functionality. The high level of HDAS crashes cited by the librarian T1-01 is likely to have indicated inadequate network bandwidth. Participants' comments indicated that remote access to Trust email was generally available, but remote logins to the Trust network were

enabled only for senior staff. Encrypted USB memory sticks were reported as being difficult to obtain, and their use restricted off site. Enterprise-level cloud storage was reported to be available

		T1	T3	T4
Chapter 5. Findings: barriers to information seeking, use and sharing				
5.2.1	<i>Encrypted portable media and devices</i>	Encrypted USB sticks difficult to obtain – bureaucratic hurdles / expense? Specific permission required for use off-site	Encrypted USB sticks easy to obtain	Encrypted USB sticks expensive - no longer issued in practice – though still required in policy – confused situation
5.2.2.2	<i>Remote access</i>	Remote access restricted to senior staff	Remote access easy to obtain	Remote access available – not discussed by participants
4.2.3, 7.2.1, 7.2.3.8	<i>Intranets</i>	Existing intranet ‘clunky’ and out of date; new intranet in development –	New Hadron intranet planned Knowledge manager part of library team	Adequate intranet, readily accessible without login on Trust sites – but T4-LIS reported errors in administration
5.2.3	<i>“Legacy” software</i>	50% PCs upgraded from Windows XP to Windows 7 – aiming to complete by April 2015 Incompatibility of applications with Windows XP a hindrance to accessing e-resources	Process of upgrading to Windows 7 in hand – but would not be completed before end April 2015	PC upgrading to Windows 7 from XP – aiming to complete by April 2015 – but no funding identified – had not publicised plans to end-users
5.2.4	<i>System policies and permissions</i>	System policies: unable to install ActiveX controls or enable cookies	Effects of system policies not mentioned	System locking / encryption on laptops affected presentations
5.3	<i>Browsers</i>	Standard browser: IE7, but LIS staff had access to Google Chrome	Standard browser: IE8	Standard browser: IE7, but alternatives available as required
5.2.5, 5.3, 5.6	<i>Numbers of PCs in clinical areas</i>	Shortages of PCs on the wards, leading to inability to access BNF	Lack of access to BNF an issue BNF could not be accessed via the Trust’s BlackBerry devices. Some users downloaded BNF application for own iPhones	Shortages of PCs in clinicians’ offices (AHPs) BNF not mentioned specifically

		T1	T3	T4
5.2.6	<i>Access to approved storage</i>	<p>Board members and divisional general managers provided with Content Locker for iPads – a secure collaboration and document management application</p> <p>No cloud storage solution available to other staff</p> <p>Use of Dropbox, OneDrive etc. ‘rationed’ by SWG</p>	No cloud storage solution mentioned	<p>Board members and other senior managers provided with BoardPad for iPads – secure collaboration and document management application</p> <p>No cloud storage solution available to other staff</p> <p>Staff able to use Google Drive for storage – but disliked by IT as possible security risk</p> <p>Access to Dropbox blocked</p>
1.4.3	<i>Webmail</i>	Trusts (other than T2) used domain-based email rather than NHSmail		
5.2.7.1	<i>Webmail</i>	<p>Remote access to T1 email via MS Outlook Web App was available to all staff via a login on the intranet</p> <p>Allowed other webmail, but not for T1 business</p> <p>Attachments in webmail not to be opened, on account of malware risk</p>	<p>Remote access to T3 email available to all staff</p> <p>Allowed webmail applications, but not for T3 business; only to be used with line manager’s permission</p>	<p>Remote access to T4 email via MS Outlook Web App was available to all staff</p> <p>Access to Google Mail allowed within T4, though IT manager would have preferred to block it on security grounds</p> <p>Hotmail previously blocked, but access restored quickly after doctors complained (was typically used by junior doctors for work-related purposes as alternative to frequently changing Trust email)</p>
5.2.7.2	<i>Email attachments</i>	Email attachment size limit was 22MB – no problems reported	No problems reported	<p>Users encountered problems sending email attachments owing to size limit (10MB)</p> <p>Formerly not been possible to download and read attachments in Hotmail messages</p>

		T1	T3	T4
5.2.7.3	<i>Spam filter and DLP false positives</i>	Spam filter and DLP had sometimes blocked receipt and sending of email communications from key external organisations	No problems reported	DLP system blocked only sending of PII
5.3	<i>Use of information services by clinicians</i>	Clinicians used e-resources from NHS Evidence and Trust LIS, accessed via OpenAthens Also e-resources provided by professional bodies, Google Scholar – as alternative or in addition to NHS Evidence / Trust LIS		
5.3	<i>Problems with e-resources</i>		Librarians reported problems accessing some major publishers' content via OpenAthens – publishers had not properly implemented it	
		Librarian reported HDAS very prone to crashing		Had implemented alternative to HDAS LIS conducted regular IP checks on availability of e-journals – worked closely with IT department
5.5 <i>See also Tables 5.2, 5.3</i>	<i>Podcasts</i>	Planned to use internally-produced podcasts for information dissemination Availability of external podcasts unknown	Planned to use internally-produced podcasts for information dissemination – but external podcasts unavailable due to bandwidth problems	External podcasts available to download
5.5, 9.2.2	<i>LIS use of Web 2.0 and SoMe</i>	Library active in attempting to develop SoMe / Web 2.0-based services – felt that obstacles related to lack of understanding of cloud services and generational attitudes	No SoMe / Web 2.0 services mentioned by librarian	Library developed SoMe platforms (Pinterest for infographics, WordPress for library CAS) – accessible to staff via trust network (if approved) or BYOD network on personal mobile devices
5.5	<i>Online forums</i>	Online forums important to AHPs for professional discussion and information sharing – but blocked within T1 – use not encouraged at work	Online forums not mentioned by participants	Online forums not mentioned by participants

		T1	T3	T4
	<i>Other Web 2.0 applications</i>	Web 2.0 applications other than Skype (generally blocked as P2P) generally accessible		
	<i>Blogs and microblogs</i>	SoMe: blogs, microblogs blocked	SoMe: content communities blocked	SoMe: blogs, microblogs blocked
5.6	<i>LIS support for mobile devices</i>	LIS supporting iOS and Android personal mobile devices LIS maintained national list of clinical mobile applications	LIS supporting iOS and Android personal mobile devices	Support for mobile devices not mentioned as such by library staff
<i>Chapter 6. Findings: education and training</i>				
6.1, 6.2, 6.4.4	<i>IT infrastructure</i>	Delivery of educational content frequently hindered by IT infrastructure issues: network bandwidth, inadequate specification of PCs, lack of sound cards and peripherals (e.g. webcams); monitor resolutions too low		
		New starters unable to access induction e-learning before starting in post – NLMS did not allow access to people who were not already registered as staff		New starters problems circumvented at T4 via use of Moodle
		T1 hoped to circumvent via use of new e-learning portal – not yet tested	T3 had portal set up for community staff to enable them to access e-learning. T3 junior doctors' induction needed to be delivered face-to-face for two days	
6.1		NLMS system checker did not work correctly to verify Java versions – national issue		

		T1	T3	T4
6.1	<i>IT infrastructure</i>	Problems reported related to other PC infrastructure issues: lack of webcams and hence inability to support teleconferencing; near-obsolete PCs whose hardware specification that was inadequate to run particular e-learning modules (despite virtualisation)	Major problem with access to e-learning had been caused by outsourced T3 provider ignoring need to update Java version on users' PCs. Other problems reported with with sound and lack of network bandwidth hindering or precluding the download of podcasts or the viewing of video clips (T3-19).	Java version issue not applicable – used Moodle as alternative to NLMS Problem reported with low screen resolution rendering content difficult to view
6.2	<i>Network logins for students</i>	AHP students able to obtain network logins on same basis as staff Earlier ban by integrated governance on nursing students being given Trust network logins had been reviewed – but new policy not implemented – student nurses able to access Trust intranet only in library, where staff could log them on. (Medical students had access to PGMC Wi-Fi for iPads)	Issue of student logins to Trust network not specifically referred to by participants IT manager wished to implement eduroam for students, but no multi-site NHS precedents for this; students therefore needed to connect to Trust Wi-Fi	Wards able to be issued by wards – students could use these to access Trust network Library did not issue generic logins Students unable to log in to clinical systems
6.3	<i>LIS support for e-learning</i>	Library heavily involved in supporting e-learning: -- encouraged use of computer suite for e-learning and online examinations -- provided access to an e-learning authoring package for trainers to use -- worked closely with postgraduate medical centre	Library and training worked closely together to promote education and learning opportunities: -- promotional material about LIS available in T3 computer centres -- librarian invited to give presentations at training events on role of LIS	Library: -- provided computer facilities for students -- assisted them with accessing e-resources -- ran information literacy training sessions

		T1	T3	T4
6.3	<i>Scope and utilisation of e-learning</i>	T1 was just about to roll out the use of e-learning for clinical and non-clinical mandatory and statutory training	E-learning was being used extensively for clinical and non-clinical mandatory and statutory training, particularly at induction	
		E-learning used within all Trusts to support other professional learning, varied in extent by profession		
6.4	<i>Perceived disadvantages of e-learning</i>	Perceived disadvantages of e-learning: -- heavy workload involved in constantly updating mandatory and statutory e-learning in line with Trust policies -- diminution / devaluation of subject matter experts' role -- easy to underestimate time required / overall burden of e-learning requirements	No disadvantages mentioned by participants	Overall burden of e-learning requirements for junior doctors created "overwhelm"
6.4.1	<i>Drivers for adoption of e-learning</i>	Drivers for adoption of e-learning: -- poor take-up of day release for face-to-face training -- lack of motivation to attend training	Specific drivers not mentioned – though anecdotal evidence suggested that mental health Trusts were early adopters of e-learning – geographical spread, large number of sites an obvious driver – able to take study leave to attend IT suites or access at home	Drivers for adoption of e-learning: -- need for more flexibility in training provision -- perceived poor quality of face-to-face training -- lack of motivation to attend training
6.4.2	<i>Timeline and development of e-learning</i>	E-learning about to be rolled out	E-learning well established – "really strong culture of e-learning" – advantages evident for mental health Trusts – geographical spread and large numbers of sites	E-learning well established – started 2009
6.4.2	<i>Sources of e-learning content</i>	Professional e-learning content produced by professional bodies and universities – Trusts could use for mandatory training Use of e-learning, and involvement of professional bodies in producing e-learning, varied widely by profession		

		T1	T3	T4
		Not discussed by participants	Producing home-made e-learning too time-consuming – buying in a better alternative	E-learning team did not have time to work with clinical staff to produce e-learning – clinical e-learning therefore produced by external developers
6.5	<i>Web 2.0 and SoMe use for learning</i>	Nursing students used Facebook groups – but not known how – participant had no access	Use of podcasts for postgraduate medical education planned	Twitter used to communicate among e-learning and simulation specialists Education department maintained active Twitter feed
		YouTube widely used for teaching – but technical obstacles encountered (e.g. bandwidth limitation) and specific permissions sometimes required		
6.6	<i>Use of mobile devices for learning</i>	U3 medical students using iPads to support their learning while on clinical rotations		
		NLMS used Adobe Flash, therefore could not be accessed on Apple devices (iPads etc.). Could be accessed on some Android and Windows devices		
		Medical students connected to PGMC Wi-Fi	Medical students able to connect to T3 Wi-Fi	eduroam retro-fitted across much of site to support this – but not available everywhere
		‘Rugged’ Android tablets purchased to enhance access to e-learning via mobile classrooms on wards Expecting in future to use tablets purchased for clinical purposes also for e-learning	Most staff accessed Trust e-learning via a personal or Trust laptop using a VPN and remote authentication token	Staff accessing Trust e-learning content via personal Android devices Use of mobile devices well embedded within pharmacy teaching – tutor used NearPod for interaction with students via their tablet computers Otherwise no uses of mobile devices reported for educational purposes

		T1	T3	T4
<i>Chapter 7. Findings: organisational dynamics and professional cultures</i>				
7.2.1	<i>IT strategies</i>	<p>No library or training input into IT strategy</p> <p>Librarian on planning group for new trust intranet – but did not feel fully embedded in process</p>	<p>IT manager received strategic input via locality management teams – IT department represented on these.</p> <p>-- Clinical systems user groups for T3's two clinical systems provided important channel of communication with IT</p> <p>-- IT trainer provided feedback with IT issues related to training</p> <p>-- No explicit library or training input into IT strategic agenda</p> <p>-- 'Dragon's Den' process for vetting, approving and funding new patient e-information projects</p>	<p>Departmental information groups established for each major hospital site and for community services; business analyst from IT attached to each of these</p> <p>No library or education input</p>
7.2.2	<i>Hardware procurement</i>	In all areas except T3 community services, no ring-fenced funding for replacement of IT hardware and peripherals; central funding associated only with specific projects; local budget holders responsible for meeting costs		
		<p>Reported difficulties in getting new PCs and peripherals installed – administrative obstacles, lack of funding</p>	<p>IT department had engaged contractor to audit PC specifications, with a view to upgrading or replacement</p>	<p>CQC had identified needed improvements in hardware and infrastructure, especially in community services</p> <p>Some services reported inadequate or old PC hardware, also shortage of PCs. Other services well provided for, especially where clinical need readily apparent, e.g. radiology</p>
7.2.3.2, 7.2.3.4	<i>Experiences of IT support</i>	IT department good with 'quick fixes'		IT department had failed to resolve a problem with Adobe Flash over several months – but updated software promptly

		T1	T3	T4
		Provided email and telephone contact, remote logins to users' PCs – no web interface to helpdesk		
7.2.3.3, 7.2.3.6		Difficult to get to speak to anyone in IT support, and email communication cumbersome – excessive numbers of emails generated	Provided online chat facility Process of logging calls with outsourced IT support service S3 slow and impractical – telephone queuing system	
7.2.3.4		S3 slow to respond to calls relating to clinical systems		
7.2.3.5, 5.2	<i>Experiences of IT support</i>	IT department perceived as good but as under-resourced and struggling with outdated infrastructure – tended to focus purely on support of clinical systems	IT perceived as supporting education, training and LIS functions well	IT department perceived as under-resourced in relation to demand – helpdesk tending to prioritise clinical systems over educational issues IT worked closely with LIS to keep firewall settings up to date for e-journals
7.2.3.7		Out of hours printing issue in library unresolved for 10 years – perceived lack of alignment of IT business priorities – restricted library use for staff working shifts IT manager seemingly unaware that LIS had computers on the Trust network as well as the university network	No specific alignment issues mentioned by participants	No specific alignment issues mentioned by participants – but problem getting donated iPads configured to provide patient information
7.2.3.6		Head of IT Services habitually failed to respond to communications, but other staff better	No communications issues with in-house IT reported	T4-22 unable to speak to a senior member of staff to resolve specialist support issues Information governance contact with informatics was minimal despite physical proximity of offices – information governance function was excluded from major projects

		T1	T3	T4
7.2.3.8		<p>IT management culture in NHS perceived as engendering negative attitudes to end-users compared with other sectors – staff who came from a private sector environment thought to be more amenable</p> <p>Cultural divide perceived between IT and other staff</p> <p>T1 IT department perceived by librarian as highly ambivalent towards LIS</p> <p>Some IT staff perceived as patronising towards end-users</p>	IT staff attitudes not raised as an issue by participants	Negative / exclusive IT staff attitudes reported by records and governance manager
7.2.3.9	<i>Experiences of IT support</i>	Users generally positive about quality of IT support: staff helpful, polite and prompt to respond to support requests	<p>In-house IT perceived as very good – steadily improved over librarian’s 9 years in post</p> <p>Contrasting reports received of outsourced IT (S3): some good, some very poor</p>	Quality of IT support perceived as having improved over last few years
7.3	<i>Perceptions of LIS</i>	<p>Library well regarded by clinicians</p> <p>Reported that better domain knowledge would improve quality of mediated literature searches</p>	<p>Library well regarded by clinicians – though clinical tutor regretted the lack of a physical library presence – librarian described as “excellent”</p> <p>Reported that better domain knowledge would improve quality of mediated literature searches</p>	Library well regarded by clinicians – for quality of support to users and scope of e-resources
		LIS provided current awareness service focused on specific patient safety areas: safer medicines administration, falls, pressure sores	LIS provided customised current awareness service to nurses in community services	LIS maintained current awareness portal No other current awareness services mentioned

		T1	T3	T4
7.3	<i>Evidence-based practice</i>	<p>EPB initiatives focused on specific patient safety areas</p> <p>Management practice perceived as referring insufficiently to published sources of evidence</p> <p>AU1 expressed strongly positive view of the use of the Internet for information seeking</p>	Strong culture of EPB – reflected in 6 C's adopted as T3 values statement	<p>EBP initiatives not mentioned by participants</p> <p>Clinical teacher T4-05 mentioned need to keep teaching material fully up-to-date with results of most recent research</p> <p>Use of published evidence by radiographers embedded in the IRMER regulations governing requests for radiographic images</p>
7.4.1	<i>Cultural attitudes to IT</i>	<p>Significant proportion of staff averse to using computers</p> <p>Paper-based communication still predominated within Trust – use of email to communicate with staff was problematic – not everyone used the Trust email - allowed their accounts to expire</p>	<p>Some community staff tended to avoid using computers and would not avail themselves of training opportunities that were presented to them</p> <p>Techno-stress cited as a reason given for community nursing staff taking early retirement</p>	Computer aversion / non-use cited in general by T4-22 as an aspect of wider problems with NHS IT, but no specific instances offered
7.4.2	<i>Attitudes to e-learning</i>	<p>Nursing students' reasons for disliking e-learning: lack of interaction with other students; insecurity with subject matter (pronunciations of terms etc.); disliked discussion boards; poor usability</p> <p>E-learning staff emphasised importance of improving usability and debugging when e-learning introduced</p>	<p>T3 e-learning developer spent a great deal of effort on improving usability</p>	<p>Junior doctors suffering from e-learning overwhelm</p> <p>Usability not referred to by e-learning staff</p>
7.5	<i>Attitudes to Web 2.0 and SoMe</i>	<p>Peer monitoring of social media content by student nurses</p> <p>E-professionalism training provided: what and what not to post, privacy settings</p> <p>Level of risk of using social media in professional contexts generally perceived as unacceptably high</p>	Clinician participants keen to use social media to improve patient engagement with community health services – but perceived as high risk undertaking – unaware of guidance available from communications department	<p>Saw NHS culture as a powerful disincentive to use of Twitter</p> <p>Concerned with reputation of the Trust</p> <p>Need expressed for further training and guidance</p>

		T1	T3	T4
7.6, 5.6	<i>Mobile devices</i>	Strong sense among clinicians (T1, T3, some professional groups in T4) that “personal smartphones and tablets aren’t really acceptable for use in a patient environment”		
		Medical students strongly discouraged from taking iPads into clinical areas – written policy		
		Clinicians’ stated views about content of policies restricting use of mobile devices sometimes at variance with actual policies		
		Student nurses discouraged from using mobile phones in clinical areas Pharmacist cited departmental and Trust policies prohibiting use of mobile phones in clinical areas	Pharmacist cited Trust policy as precluding the use of personal smartphones in clinical areas Laptops and Windows 8 tablets the preferred mobile devices – only 20-25 iPads in use Trust BlackBerry mobile phones unable to access the web	Doctors and pharmacists at T4 commonly used own smartphones for work purposes – may have been facilitated by BYOD. No actual restrictions in T4 on use of mobile phones in particular areas – but perceived as a matter of “professionalism” that mobile phones should not be used in clinical areas Trust mobile phones available to all staff who needed them – but some very out of date

		T1	T3	T4
<i>Chapter 8. Findings: information governance and security</i> ⁹⁷				
8 <i>passim</i>	<i>Cybersecurity</i>	No cybersecurity incidents reported at any of the Trusts within previous few years		
8.2	<i>Acceptable use policies</i>	All AUPs included key constituents as identified by Gallagher, McMenemy and Poulter (2015) All banned illegal activities as described in computer misuse legislation		
		<p>AU1 sought to encourage both work-related and recreational information seeking in accordance with the policy which did not interfere with work Internet use at work “a privilege not a right” Allowed limited personal use Specifically banned were: -- online shopping without prior approval -- sending of unreasonably large email attachments not required for business purposes -- deliberate viewing of pornography other than for legitimate study and research -- use of P2P applications (e.g. Skype)</p>	<p>AU3: allowed personal use of email and web on similar terms to AU1 -- Included gambling among prohibited activities -- Personal email to be identified as such with ‘PERSONAL’ in the subject line and deleted after two weeks -- Unintentional access to ‘offensive’ sites to be logged as an incident</p>	<p>AU4Int: Personal use of the web and email during breaks required permission of line manager Installation of additional software or plugins required permission of IT department No viewing of pornography allowed for ANY reason Long lists of categories of unacceptable material – apparently derived <i>verbatim</i> from SWG4 documentation Specific warning about downloadable files Threats of disciplinary sanctions for Internet misuse General minatory tone Use of P2P applications (e.g. Skype) banned Downloads required to conform with copyright legislation</p>

⁹⁷ Material from Section 4.4.4, Secure web gateways, is also included in detail here on account of its close relationship with the content of Chapter 8.

		T1	T3	T4
		<p>AU1 authored by Head of ICT Lead director – Medical Director Approved by information governance committee Equality impact statement provided List provided of staff groups consulted Implemented March 2013 Review date March 2016</p>	<p>AU3 authored by Head of IT Lead director: Director of Operations Approved by records and clinical systems group Equality impact statement provided List provided of staff groups consulted Implemented March 2017 Review date March 2016</p>	<p>AU4Int authored by Head of Informatics Approved by “Trust information governance” in lieu of IM&T steering group, at that time in abeyance Ratified by staff side representatives of Trust Negotiating and Staff Side Committee – no other staff groups consulted No equality impact statement provided Implemented March 2011 Review date March 2012 – <i>past review date</i></p>
8.3	<i>Monitoring of staff web use</i>	In accordance with RIPA 2000, records were kept of web use, but individual usage was monitored only at the request of a line manager in cases of concern		
		Frequency of monitoring requests not referred to by IT manager	IT manager received monitoring requests about every two months	Frequency of monitoring requests not referred to by IT manager
8.3	<i>Monitoring of staff web use</i>	<p>SWG1 sent automatic notification to IT department of attempts to access blocked websites One participant expressed concern at consequences of this – inhibited her searching - but were not acted upon by IT IT department also notified managers of excessive non-work-related web use</p> <p>Little monitoring of compliance with information security policies in practice, though penalties for misuse stated in policies</p>	<p>According to AU3, line managers could in principle be contacted regarding attempts to access a blocked site – but actual occurrences not described by participants</p> <p>IT manager reported regularly to records and clinical systems group on “top ten websites visited”</p>	<p>SWG4 sent automatic notification to IT department of attempts to access blocked websites One participant expressed concern at consequences of this – but not acted upon by IT</p>
		No routine monitoring undertaken by any of the Trusts of content filtering accuracy		
4.4.4	<i>Secure web gateways</i>	No under-blocking reported	IT manager received requests from managers periodically to block sites deemed inappropriate that were not blocked by SWG3 – unclear what nature of sites was or whether added manually to blacklist – suggestive of under-blocking	No under-blocking reported

		T1	T3	T4
		Focus of SWG1 promotional material solely on preventing inappropriate web use	Case studies of SWG3 implementation in NHS referred to problems presented for clinicians by over-blocking "Over-blocking a huge problem for the NHS" P2 (IT manager whose Trust used SWG3) unaware of any problems of website blocking	Focus of SWG4 promotional material solely on preventing inappropriate web use
4.4.4	<i>Secure web gateways</i>	Quotas implemented for usage of many Web 2.0 applications – though apparently not publicised Offered facility to set up different access levels according to job role – again not implemented Offered a facility for analysing security threats posed by particular URLs or IP addresses and reporting incorrectly categorised websites; unlikely, however, that end-users within the Trust would have accessed it	Offered facility to set quotas for usage of many Web 2.0 applications – but not implemented Also offered: -- facility for delegated temporary unblocking of blocked content to select users and managers – not implemented -- facility to set up different access levels according to job role – not implemented	Offered facility to set up different access levels according to job role – not implemented
4.4.4	<i>Secure web gateways</i>	Offered 'granular' controls on functionality of social networking applications	Offered 'granular' controls on functionality of social networking applications	Did not offer fully granular social media controls
		Default categories of restricted web content implemented	Implementation of web access controls not discussed by IT manager	Default categories of restricted web content implemented – extensive

		T1	T3	T4
8.4	<i>Endpoint security</i>	Did not implement locking of PC screens	No endpoint security issues mentioned by participants	Endpoint security perceived as lax: printing emails, port control for USB memory sticks non-existent; situation confused re: availability of encrypted USB sticks
		All Trusts still using older versions of browsers – compatibility with legacy applications – potential security risk		
		All Trusts still using Windows XP – potential security risk		
8.5.1	<i>Blocking of websites</i>	Blocking of websites reported to NICE manager by librarians as a frequently-occurring problem		
8.5.1	<i>Frequency / extent of blocking</i>	Very little blocking of web content mentioned – though pharmacist reported carrying out searches at home on account of it	Very little blocking of web content on internal network – more occurring on outsourced network	Some clinical staff experienced very high levels of website blocking – “constant” or “daily” or “weekly” – but library encountered relatively few – one a month
8.5.2	<i>What was blocked?</i>	No specific content types mentioned by participants	Sites relating to eating disorders and sexual behaviour blocked	Web filter tended to block material containing images or advertisements, including sponsored Google listings Configuration to block advertising was a matter of policy, but sometimes the entire site was unintentionally blocked
8.5.3	<i>Responses to encountering blocked websites</i>	Low levels of reporting - IT manager reported that only five requests to unblock websites had been received by helpdesk within last 18 months	IT manager did not discuss reporting levels – but likely to have been low in line with low incidence of blocked websites	Despite high levels of blocking, participants described making very few reports to IT of blocked content: “I just shrug”, “I have given in trying”, “I’ve actually stopped trying to access now” Likely that many blocked sites unreported
		Participants in all three Trusts reported that staff postponed web searches and carried them out at home on account of website blocking		
		All Trusts had processes for getting websites unblocked – sometimes IT consulted information governance if in doubt		

		T1	T3	T4
		Blocked websites unblocked promptly by IT	Library and pharmacy staff reported that their unblocking requests were trusted without further checking Blocked websites unblocked promptly by IT	Time taken to unblock websites varied widely – required second-line support engineer to action – could be “fairly quick” but sometimes took several days
8.5.4	<i>Effects of website blocking</i>	Effects not described by participants	Effects not described by participants	Effects or impacts of website blocking: frustration, annoyance, ‘infuriating’ Work-life balance, productivity, personal and organisational effectiveness affected through continually encountering blocked sites and needing to work at home IT manager acknowledged issue but was not considered a matter of concern for IT services
		IT manager essentially pragmatic in overall approach: “my main ... role is making sure that things keep on working here ... people can come in, log on to the computer, and do their job”	IT managers seemed far more focused on suspected or actual computer misuse and the possible attendant security risks (insider threats) than on problems caused by lack of accuracy of web filtering	
8.5.5	<i>Awareness of national measures</i>	All IT managers unaware of national whitelist		
		Librarian aware of list but said it was not implemented within T1	Librarian aware of list but said it was not implemented within T3	Records and governance manager, librarian unaware of list
		IT manager did not indicate whether he had seen the letter from NICE, but stated that there were no NPfIT legacy applications in T1 requiring the use of older browsers	IT manager not seen letter re: browsers from NICE	Unable to ascertain whether IT manager had seen letter – could have gone to Head of Informatics

		T1	T3	T4
8.6	<i>Information governance and education</i>	Issues relating to information governance and education not mentioned by participants	Unable to record real-life clinical scenarios for teaching purposes on account of a recording issue: information governance insistent that the removable media within the recording device be encrypted, but the device could not write to encrypted media	Images of children removed from paediatric nephrology presentations sent out to delegates following conference – unsure of precise rationale for this practice or whether it related to a formal policy
<i>Chapter 9. Findings: communications policies and practices</i>				
9.2.1	<i>Corporate use of SoMe</i>	T1 just starting to experiment with SoMe for external communications New SoMe policy recently launched Apparent discrepancy between policy and SWG configuration	Use of SoMe for external communications with other organisations well established – piloting SoMe communications with patients and public Restrictive policies on internal use	Use of SoMe for external communications well established – delegated to individual departments Restrictive policies on internal use – but mitigated in practice by BYOD – network settings less restrictive
		Policies intended to cover both work-related and personal uses of social media from wherever they were accessed		
	<i>Web 2.0 and SoMe policy in relation to media strategies</i>	Information governance responsible for SoMe policy	Communications department responsible for SoMe policy	AUP for Internet and email use held by informatics department SoMe4 policy held by communications department in association with human resources and union representatives Departmental social media guides the responsibility of individual departments concerned

		T1	T3	T4
9.2.1	<i>Web 2.0 and SoMe policy in relation to media strategies</i>	<p>SoMe1 cited opportunities for research, raising awareness of topical health issues, public engagement and the chance to establish a wider and more diverse professional network</p> <p>Blocking access to social media for most staff within the Trust was a matter of policy</p> <p>Acknowledging that many staff were accessing social media via personal mobile devices</p>	<p>SoMe3 did not discuss possible advantages of SoMe use</p>	<p>SoMe4 referred to the benefits of sharing knowledge and skills outside the organisation</p> <p>Acknowledged existing uses of social media by staff members</p> <p>Expressed Trust's wish to encourage and support these</p>
9.2.1	<i>Web 2.0 and SoMe policy policy in relation to media strategies</i>	<p>SoMe1 referred to the need to ensure the operational effectiveness of the Trust and to avoid bringing T1 and the NHS generally into disrepute</p>	<p>SoMe3 and SoMe4 referred to the need to ensure the operational effectiveness of the Trust and to avoid bringing the Trust into disrepute</p>	
		<p>SoMe1 referred to the need for professionalism in the use of social media Incorporated standard warnings not to breach confidentiality directly or indirectly -- through the posting of PII or photographs online -- through sharing information about the Trust that was otherwise sensitive or subject to non-disclosure agreements</p>	<p>SoMe3 and SoMe4 referred to the need for professionalism in the use of social media Incorporated standard warnings not to breach confidentiality directly or indirectly -- through the posting of PII or photographs online -- through sharing information about the Trusts that was otherwise sensitive</p>	
		<p>All policies also specifically prohibited the posting of: -- material likely to contravene diversity or bullying and harassment policies -- that was in any other way illegal All stressed that: -- disciplinary action could be taken for inappropriate use of social media -- civil proceedings or criminal prosecution could also result</p>		

		T1	T3	T4
		<p>SoMe1:</p> <ul style="list-style-type: none"> -- Very detailed and prescriptive -- Precluded posting of photos on SoMe personal sites of staff in uniform on in an identifiable work setting -- Enjoined staff to use real names if associating themselves in any way with T1 -- Included procedures for dealing alleged bullying and harassment via social media -- Urged staff to be aware of possibility of information being shared without their permission or knowledge -- Stressed need for factual accuracy 	<p>SoMe3:</p> <ul style="list-style-type: none"> -- Brief in nature -- Prohibited posting of PII and illegal content -- SoMe content should represent T3 and not offer personal opinions or views -- Staff strongly advised to consider the implications of any material published online -- Staff wishing to utilise SoMe tools extensively for the purpose of sharing information in a professional capacity enjoined to seek advice from communications team 	<p>SoMe4:</p> <ul style="list-style-type: none"> Included recommendations regarding privacy settings and general safe behaviour online -- Stated that posting of photographs on sites such as Facebook required specific permission from the subjects -- Stressed that staff were responsible not only for content that they posted themselves on social media sites, but also for the content of comments that they permitted to be displayed -- Staff enjoined to refrain from identifying T4 colleagues by name, as well as patients -- Staff referred to social media guidance produced by their own professional body or regulator
9.2.1	<i>Web 2.0 and SoMe policy</i>	<p>Policy, experiences of misuse, and attitudes appeared closely inter-related</p> <p>Implementation of policy in T1 appeared confused</p> <p>Popular SoMe applications were 'supposed' to be blocked, but in fact were only subject to a quota system, although functionality was restricted</p>	<p>Access to "professional" sites, such as LinkedIn and Academia.edu, routinely allowed in T3, but not access to Facebook</p> <p>SWG3 allowed 'granular' controls on popular SoMe sites – but not implemented</p>	<p>Facebook, Twitter and other popular social media platforms blocked by default in T4</p> <p>Requests for access required:</p> <ul style="list-style-type: none"> -- demonstration of specific business need -- authorisation by a line manager <p>SWG4 allowed read-only access to popular SoMe sites - but not implemented</p> <p>Staff frequently accessed SoMe from own mobile devices via BYOD network</p>

		T1	T3	T4
9.2.3	<i>Staff experiences and perceptions of Web 2.0 / SoMe and related policies</i>	Indifference or negative attitudes towards SoMe widespread		
		Suggested by participants that a marked generational divide existed in attitudes to SoMe: younger staff comfortable and familiar, older staff negative		
		<p>T1's policy and practices described as 'risk-averse', as 'reactive', and as seeking to exercise control for its own sake</p> <p>One participant (HR) described them as 'IT-led' and expressing tight control – missing a major opportunity for public and staff engagement</p> <p>But records and governance manager in favour of a total ban on SoMe access – concerned about adverse effect on staff productivity</p>	<p>T3-19 said she felt frustrated and demeaned by the need to secure unblocking and permission from IT for use of YouTube for training</p>	<p>SoMe policies and practices not commented on as such by participants</p>
		T1 library had experienced problems getting use of Prezi approved – situation appeared confused		
		Librarian had been told that 'no Trust-related SoMe activity would be allowed until the social media policy was developed'		

		T1	T3	T4
9.2.4.1	<i>Drivers of corporate use of SoMe</i>	<p>Local drivers for SoMe use perceived to be:</p> <ul style="list-style-type: none"> -- possibilities for recruitment of staff (T1-03) -- provider and partner organisations' adoption of SoMe (T1-01) -- perceived benefits for staff engagement and health of organisational culture (T1-02). <p>Corporate use of SoMe only just beginning to be discussed</p> <p>Culture of Trust another negative factor; professional social networking at work perceived as 'slacking'</p>	<p>Decision to use SoMe corporately in T3 described by communications officer as driven fundamentally by the need for patient engagement, particularly in CAMHS</p> <p>Rationale for using SoMe: going to where people are</p> <p>A necessary balance of risk and reward in using SoMe</p> <p>Use of SoMe platforms by T3's partners and providers of outsourced services another factor in spread of SoMe use: now "gently washing in" (T3-09)</p> <p>Publications of NHS Employers cited as an important general influence on SoMe use by Trusts</p>	<p>No specific drivers for SoMe use discussed by participants</p>
9.2.4.2	<i>Patterns of SoMe use</i>	<p>Communications officer had resisted adoption of SoMe it on account of workload</p> <p>Was concerned about possible negative feedback from patients and how to manage or control it</p>	<p>SoMe used extensively for:</p> <ul style="list-style-type: none"> -- research dissemination -- patient and public engagement -- sharing innovation in professional practice <p>SoMe activities closely regulated by communications department</p>	

		T1	T3	T4
9.2.4.2	<i>Patterns of SoMe use</i>	Trust charity – but not T1 itself – had a Facebook page	No corporate T3 Facebook page Use of Facebook successfully piloted by locality health promotion services T3 Twitter feed retweeted items of general interest about mental health	Umbrella corporate T4 Facebook presence Facebook page seemed to feature mostly news items from “media centre” of T4 website Many individual Twitter feeds for T4’s individual departments and services T4 LIS had current awareness portal and Pinterest site for infographics
9.3	<i>Mobile devices and SoMe</i>	No discrete mobile devices policy as such General prohibition in force on use of smartphones in clinical areas – related to concern about breaches of confidentiality or privacy BYOD specifically prohibited	Had specific mobile devices policy No ban on using mobile phones in clinical areas – but users enjoined to ‘be aware of, and respect, local policies regarding the use of mobile communications devices’ Users warned that on T3 mobile phones: -- all calls logged by network provider -- ‘there should be no expectation of privacy in anything created, sent, stored or received’	All T4-owned mobile devices were to have MDM enabled Mobile apps that were installed on such devices required to be licensed and purchased through authorised sources As far as possible, users were enjoined to avoid storing T4 data on mobile devices Personal mobile devices on BYOD network required PIN protection via Trust-approved security application

Table 10.1 Summary and comparison of findings by Trust

only to senior managers in conjunction with the use of iPads for document management, and use of personal cloud storage solutions was reported to be restricted. The service provided by the IT department was perceived by participants as good in terms of technical capability, but as struggling with inadequate staffing levels and outdated infrastructure, and hence focused on maintaining clinical systems as its main operational priority. It is likely that the task of EPR implementation was placing a particular strain on its resources. There were also indications from participants' comments of poor communication on the part of IT managers and staff, and of insufficient alignment to business needs. Some aspects of IT services appeared to be good: Wi-Fi coverage was adequate across most of the main hospital site, plans for upgrading from Windows XP were well in hand, and it had implemented a market-leading secure web gateway; also, no legacy NPfIT applications remained in use. Very little blocking of legitimate websites was reported. Participants indicated that alternatives to the standard web browser (IE7) were available to staff according to business need.

While working relationships between information governance and IT management seemed to be harmonious and collaborative, marked differences of attitude and approach were apparent between the two groups in relation to policy development. The IT manager T1-11 described his overall approach to information security management as "pragmatic"; his focus was on "making sure that things keep on working here". He contrasted this with the tendencies of T1's information governance, which he perceived as "always [wanting] to tighten things down". For their part, information governance managers, as indicated by their comments, were apparently concerned about computer misuse, particularly in relation to social media, and tended to see IT staff as concerning themselves exclusively with technical matters at the expense of risk governance issues.

T1's approach to Web 2.0 and social media, as represented in its policies and in the attitudes of nursing, information governance and communication managers as apparent from their comments, seemed cautious to the point of negativity. Past occurrences of flagrant misuse, leading to heightened concern about breaches of confidentiality and privacy, as well as under-resourcing of the communications function, appeared to underlie this. This marked tendency was offset to some extent, however, by the approach of T1-11, who had implemented via the secure web gateway a flexible "rationing" approach to many social media and Web 2.0 applications. As indicated by apparently conflicting accounts from participants, confusion seemed to exist about the implementation of policy. Support from the university on site (U2) appeared to have assisted the library in maintaining a high-profile, innovative service to Trust staff and students, including the facilitation of e-learning initiatives and use of personal mobile devices for information purposes.

The relatively low level of research activity at T1, as indicated by national and Trust reports, may have been a factor in the researcher's difficulty in recruiting respondents at this site. It has a possible relationship also with the reported lack of emphasis on evidence-based practice other than in relation to specific patient safety initiatives.

10.2 T3

T3 gave the appearance of being a stable, cohesive, high-performing, and innovative organisation within the limits of its resources. Its organisational performance overall, as indicated by key metrics (Table 4.2) was good. It reported a small financial surplus. Its library service was described by the librarian T3-01 as largely electronic, and the librarian fulfilled a clinical librarian role (itself innovative within mental health) as well as a management one. E-learning was reported by participants as being well-established within the culture of the Trust, being delivered in close partnership with library services, and well-supported by the IT department. Other comments indicated that there was also a strong culture of evidence-based practice, reflected in the adoption of the '6 C's' as T3's statement of values, and likely to be related to its relatively high level of research activity.

T3 appeared to have a moderate level of digital maturity. Mental health and community services had both successfully implemented EPR systems some time previously. The provision of IT services was split between the community services, where it was outsourced, and the mental health services, where it was provided in-house. The in-house service was well-regarded by participants; however, evaluations of the outsourced service (S3) were mixed. It was planned to take the outsourced service in-house, as being more cost-effective. S3 had conspicuously failed to address a support issue related to the NLMS, leading to major problems of staff disengagement from e-learning within community services before it was eventually resolved. In-house IT services were reported by participants to be user-friendly in respect of contact and communication with the helpdesk, availability of remote access to the Trust network and email system, and availability of encrypted portable media. Wi-Fi coverage was available across the Trust estate, although its quality was described as variable; a process existed to report poor signals. According to the IT department strategy, laptops were the preferred mobile device; little use was made of tablets or smartphones. Trust mobile phones were reported to be of a dated type, and unable to access the web. Plans for upgrading PCs from Windows XP were reported to be not on schedule to meet the deadline for the end of Microsoft support. The IT manager reported difficulty in persuading service managers to upgrade or replace obsolete PC hardware.

Participants reported that, after a lengthy process of deliberation and discussion, T3 had adopted a social media strategy in respect of its external communications. Judging from reports of the availability or otherwise of particular applications, individual staff access to and use of social media and Web 2.0 applications appeared to be limited; in practice, T3 was the most restrictive of the three Trusts in this respect.

Information governance functions were delegated to a considerable extent across individual departments and services, with the records and governance manager T3-03 exercising a coordinating role, and also being responsible for the annual IGT returns. Working relationships between information governance and IT were reportedly collaborative in character. In respect of attitudes to computer misuse, T3-03 expressed a considerably higher level of trust in the good intentions of staff than those of the IT manager T3-06, who appeared from his comments to be very focused on measures to report and reduce personal web use (PWU), which he perceived as presenting a malware risk. T3-06 stated that under-blocking of inappropriate web content was sometimes reported to him. Other than monitoring of individual web use at the request of managers who had particular concerns about possible individual misuse (as with the other Trusts), actual policy and practice in respect of PWU did not extend to measures other than the regular reporting to the records and clinical systems group of the “top ten” websites visited by Trust staff as a whole. Also it did not appear to be reflected in a restrictive configuration of the SWG, since very little blocking of legitimate websites occurred within the in-house network. T3-06 stated, however, that he would have liked, had resources allowed, to undertake more extensive analysis and reporting of PWU. Two factors in particular may have influenced T3-03’s sanguine attitude to information security: the limited extent of T3’s forensic service provision (4.1.1), and the very small number of recent information governance incidents (4.1.2.2).

10.3 T4

T4 was a very large teaching hospital Trust, which was in financial surplus and planning for new capital projects and growth of its specialist services and research activities. It was also planning developments of its IT infrastructure. Its organisational performance overall as indicated by most key metrics (Table 4.2) was good. Trust documents indicated that the reconfiguration of services following the takeover of a neighbouring Trust was not complete at the time of the study.

T4’s library service was evidently well resourced in terms of premises, holdings and staff, and was reported by clinicians to provide an excellent service to Trust staff and students. To obviate the

deficiencies of HDAS, it had implemented an alternative interface to bibliographic databases, EBSCO Discovery Service. In many respects T4, as indicated in Trust documents and the comments of interview participants, demonstrated a high level of digital maturity: it was highly innovative with respect to its use both of clinical and of non-clinical IT, and further major investment in its infrastructure and systems was planned. The innovativeness of T4 in general as an organisation is likely to have related to its position as a major teaching and research centre. It had been successful in its NTF bid for mobile devices to support community staff; it had implemented an automated tracking system for clinical observations, and had developed a successful business intelligence system. It had introduced BYOD, and was working on developing a “home-grown” EPR system. Enterprise-level cloud storage was available to senior managers in conjunction with the use of iPads for document management; otherwise, staff were able to use Google Drive for cloud storage, though its use was deplored as potentially insecure (T4-20).

However, judging from participants’ comments, IT staff were very stretched to deliver good quality technical support. It is likely that EPR development and implementation, in particular, was placing a considerable burden on IT services. Failure of service managers to fund the replacement or upgrading of obsolete PC hardware and peripherals, as reported by some participants, would have added to this. The latter issue was reported in some instances to be hampering clinicians’ work. Information governance as a function appeared to be subordinated to IT, while communication between information governance managers and IT services was reported to be minimal. Information governance was reported as a low organisational priority in practice, and poor in respect of the implementation of basic security measures such as issue and use of encrypted USB memory sticks and USB port blocking (T4-09). Despite this, no serious information governance incidents (SIRI Level 2 or above) had occurred in the recent past. Compared with the other Trusts, it was evident from the texts that there had been little consultation between IT and other staff groups in developing IT security and acceptable use policies. For the latter, the scheduled review was well overdue. The IT department was not required to support e-learning, for which the training department retained the services of its own Moodle developer and system administrator. E-learning was reported to be well established. The use of Moodle as the host for T4’s e-learning meant that some of the logistical and technical difficulties presented for e-learning by the NLMS as reported by training staff in the other Trusts, in particular the “new starters” issue, were obviated.

A high level of blocking of websites was reported as occurring, which was likely to have related to several specific technical issues which are discussed in detail in Section 11.3.2 below. The adverse

effects on online information seeking appeared from participants' comments to be considerable, particularly for clinical educators and other clinical staff who needed to make extensive use of web search engines in the course of their work. Like his counterpart at T3, the IT manager responsible for SWG4 believed that PWU presented a malware risk *in se*. He acknowledged that, although he was aware of users' complaints about blocked websites, he was faced with numerous competing operational pressures, and chose not to act on them. The failure of IT services to engage with the information governance function could have excluded a possible organisational avenue through end-users could address the problem of over-blocking. He did not generate any form of report for managers on the extent of PWU.

While many Web 2.0 and social media applications were reported as blocked on the T4 network, the effects of this were apparently mitigated to a considerable extent by BYOD: a separate wireless network had been set up to support BYOD, on which the settings were in most cases less stringent, allowing staff to circumvent the restrictions. Responsibilities for corporate communications using social media were delegated to individual departments and services.

The following chapter builds upon the results chapters and draws together the findings to develop a possible model of the effects of deficiencies in IT infrastructure and of the blocking of legitimate websites. It provides a discussion of the adoption of social media for corporate and individual professional communications in terms of diffusion of innovation theory and Maslow's hierarchy of needs.

Chapter 11. Discussion and interpretation

11.1 Introduction

This chapter starts by proposing a possible unifying theoretical model across the different topic areas as presented in Chapters 4 to 10, drawing on a variety of frameworks to identify the main factors which have been found to determine levels of access to published information, and to represent the ways in which they interact. It goes on to set some of the main findings within a wider context.

Wilson's updated model of information behaviour (Wilson, 1997, 1999; 2.4.2) suggests that information seeking behaviour is influenced by what he termed *intervening variables*. These are contextual factors, the impact of which may be "supportive of information use as well as preventive" (1999, p. 256); they may be psychological, demographic, role-related or interpersonal, and environmental in nature. In terms of this model, the present study has focused on environmental variables of a technical and organisational nature with NHS Trusts. The data analyses, taken in conjunction with the literature review, suggested that the environmental factors in operation could be categorised under the following major headings:

- Power, culture, trust and risk in information security (11.3). 11.3 is subdivided into six discrete areas, each of which is discussed in turn: blocking of websites (11.3.2) and mandatory use of encrypted portable media (11.3.3); empowerment, engagement and access to information (11.3.4), information security / governance risk (11.3.5), and impact of information governance / security incidents (11.3.6). Blocking of websites and mandatory use of encrypted portable media (11.3.2, 11.3.3) are discussed in terms of the "satisficing" and information source horizon concepts (Sonnenwald, 1999; Fourie and Claasen-Veldsman, 2011) (2.4.2) and of Inglesant and Sasse's (2011a, 2001b) application of Clegg's (1989) circuits of power theory to information security (2.5.6.2). Staff empowerment, engagement and access to information (11.3.4) are discussed in relation to Kanter's (1993) theory of structural empowerment (2.5.6.1). The discussion of information security / governance risk (11.3.5) makes reference to sociological theories of risk (2.7.1).

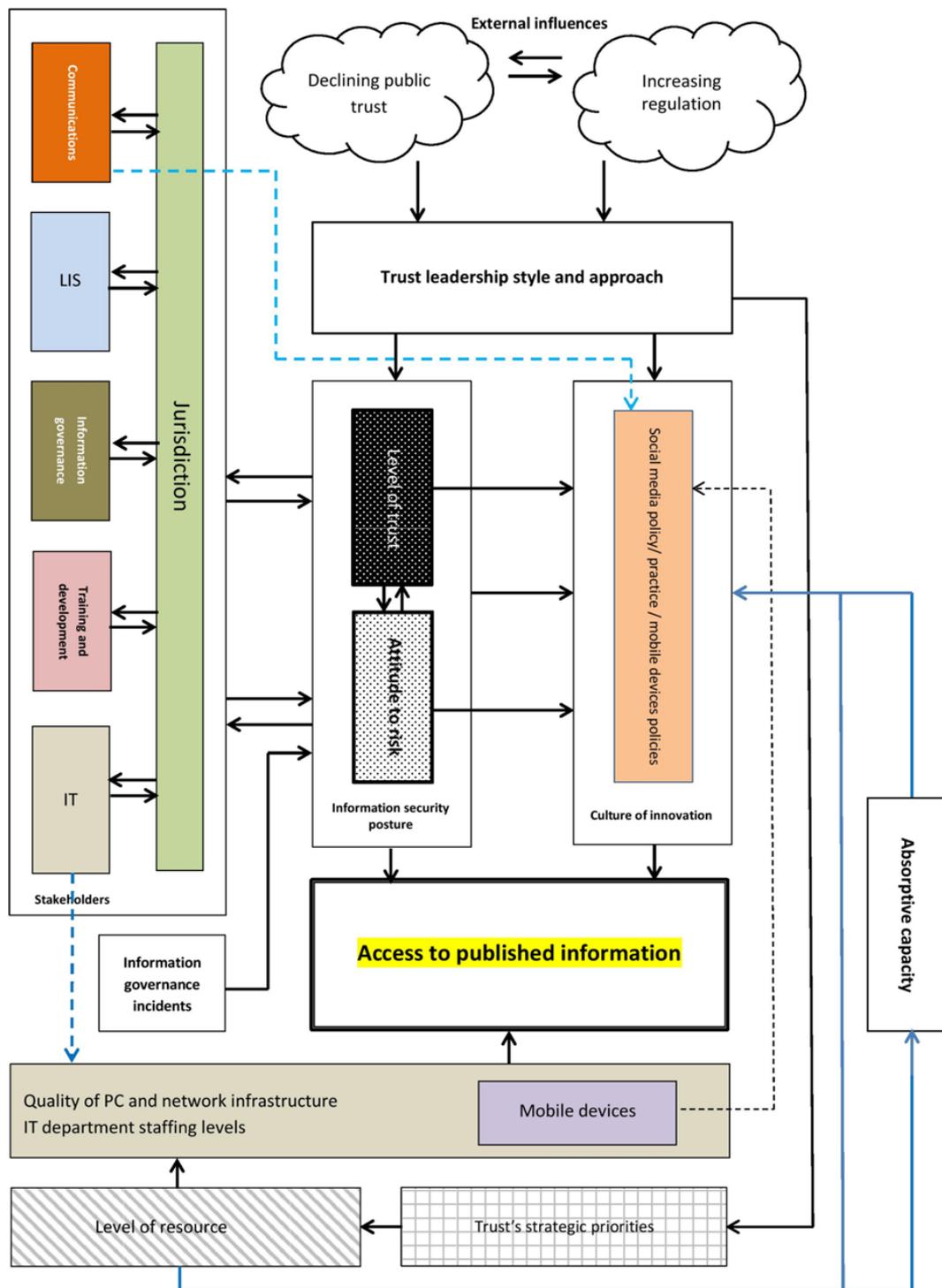


Figure 11.1 Factors determining access to published information within the NHS

Legend

Solid black arrows: *lines of organisational influence*

Dashed blue arrows: *lines of departmental responsibility*

Dotted black arrow: *pertinent infrastructure issue*

Solid blue arrow: *line of influence of level of resources*

Coloured boxes for stakeholder groups: *colours are those of the thematic maps (Chapters 4-9)*

- Professional relationships (11.5). The consideration of professional relationships (11.5) draws extensively on Abbott's theory of the system of professions (1988)(2.5.4).
- Approaches to innovation (11.4). These are considered in terms of theories of diffusion of innovations, principally that of Rogers (1966/2003)(2.8). Discussion of Web 2.0 and social media use in particular refers to the theory of IT-culture conflict (Koch, Gonzalez, & Leidner, 2011; Leidner & Kayworth, 2006)(2.8.4) and to Maslow's hierarchy of needs concept, as adapted by Chretien and Kind (2014) in relation to social media adoption within health services (2.8.5).

11.2 Proposed theoretical model

This chapter discusses three main theoretical areas of relevance and interest: interactions of power, culture, trust and risk in information security; approaches to innovation; and the effects of inter-professional conflicts and competition. This section proposes at the outset a theoretical model which unifies and generalises these.

The study as a whole was expected and intended to be of an exploratory nature (3.3), hence the conclusions are presented as a model to stimulate further exploration and testing. Figure 11.1 proposes an explanatory model of the majority of factors found to be operative in determining access to online published information within NHS organisations. Not all the findings could be represented, e.g. those related to the relative priority of professional education.

The role of Trust leadership in establishing appropriate attitudes to risk fostered by a culture of trust, and the relationship of these to a Trust's culture of innovation, was discussed in the literature review, Section 2.8.2. Information security posture is defined by Young (2008, p. 4) as "the current state [of information security] in terms of the role of information security in the organization, degree of integration of information security in business planning, and employee/management attitudes towards information security". It thus includes a substantial attitudinal component. Organisational responses to technical information security threats may depend upon the organisation's attitude to risk and preferred balance of risk and reward, as discussed in Section 2.7.1.

It is proposed that six main factors are involved, which may be grouped into two main categories:

1) *Declining public trust* in and 2) *increased regulation* of public services, e.g. via data protection provisions as implemented within the Information Governance Toolkit, interact with each other, as

shown at the top of Figure 11.1, and constitute important external influences on a Trust's *leadership style and approach*, as discussed in Section 2.5.5.2. They may also affect organisational policies more directly. Leadership style and approach in turn directly influence two key aspects of organisational culture, these being the Trust's *information security posture*, of which two of the key determinants, as shown in Figure 11.1, are *organisational trust* (in this context, managers' and IT professionals' trust of staff) and *attitude to risk* (in this context, tolerance of failures in the interest of organisational learning), and its *culture of innovation*, of which its level of implementation of e-learning and its policies and practices relating to use of Web 2.0, social media and mobile devices form a part. These are represented by the two boxes in the centre. Information security posture as a whole and its contributory components, organisational trust and attitude to risk, have further direct influences on culture of innovation; indeed, attitude to risk may be considered as a component aspect of culture of innovation (Mulgan & Albury, 2003); compare the discussion of risk and innovation in Section 2.8.2. Information security posture is also directly influenced by past information governance or security incidents, *cf.* Section 11.3.6; these tend to raise the priority given to security (compare the discussion in Section 2.7.2.4.1). Leadership style and approach has an additional direct effect upon the Trust's overall *strategic priorities*. Strategic priorities in turn are likely to affect the position and status of IT services, and thereby to determine the *level of resource* available for IT staffing and infrastructure, and hence the quality and level of development of IT services provided within the Trust, including PC and network infrastructure, and the adequacy of IT department funding levels. These are represented at the foot of Figure 11.1. They may also determine specific IT priorities. Within T1 and T4, for example, EPR implementation was a major strategic priority, which would have placed considerable strain on budgets and staffing levels in respect of other areas of their IT departments' work (4.4.1). They are also likely to determine the levels of resource available for other corporate functions such as information governance and communications. As we have seen, overall cultural attitudes to IT are also likely to inform strategic priorities relating to IT (2.8.5, 6.4.5), although this is not represented within the model. Level of resource in turn influences culture of innovation, both directly and via absorptive capacity, as shown by the solid blue arrows on the right.

2) *Contested jurisdiction* between library and information services, communications, training and development, information governance, and IT departments, as represented by inter-professional conflicts. This is discussed in relation the study findings in Section 11.5 below. This contested jurisdiction (8) also impinges upon 4) information security posture, which in turn influences 5) the Trust's culture of innovation, and hence its use of mobile devices and of Web 2.0 and social media applications, by services and by individuals. Both information security posture and culture of

innovation thus directly affect access to published information online. It also has an influence upon the quality of IT services, as shown by the blue dashed arrow to the bottom left.

Mobile device implementation is an aspect of innovation in its own right, but bears also on social media adoption, especially where Bring Your Own Device (BYOD) policies have been implemented, as indicated by the black dotted arrow on the right. The specific responsibilities of IT departments for IT infrastructure and of communications departments for Web 2.0 and social media strategy are indicated by the blue dashed arrows. The effects of level of resource (7) on culture of innovation (5), both directly and via absorptive capacity (*cf.* the discussions in Section 2.8.1 and 11.3 above), are represented by the solid blue arrows on the right. Among the Trusts in the study, only the very large teaching hospital T4 currently had the resources available within its IT department to be able to implement BYOD, which carries a considerable overhead (2.8.3). BYOD allowed staff a better level of access to Web 2.0 and social media than was available via the T4 network (9.2.1).

Other possible influences on culture of innovation are not shown. The deficiencies of IT infrastructure and staffing identified in the results chapters (4-10) relate to the relatively low percentage annual expenditure on IT by health services in the United Kingdom as a whole compared with other sectors. Owing to the fragmented nature of the NHS in England following the “Lansley” reforms (Health and Social Care Act 2012), it was not possible to derive a national figure for expenditure on information technology by NHS organisations. Contributory factors to the relative lack of investment in IT within the NHS are cited above (Section 2.8.5). As stated above, level of resource, being a factor in culture of innovation (Apekey et al., 2011; Section 2.8.1 above) is likely to affect culture of innovation both directly and via its effects on absorptive capacity; such an influence could be said to have been apparent particularly in T1, in which staffing levels across corporate departments, particularly communications, were relatively low.

11.3 Power, culture, trust and risk in information security

11.3.1 Introduction

General aspects of NHS information technology were described in Section 1.4.3. The literature review presented an overview of the general characteristics of the NHS as an organisation (2.5.5), and outlined some of the problems perceived with information technology innovation with the NHS (2.8.5). The results chapters (4 to 10) described in further detail some characteristic features of the manner in which IT infrastructure and security are managed within the NHS in England, as exemplified within the three Trusts in the study. The study findings can be set within a context of

declining public and organisational trust relating both to the quality of health services provision and to data protection, as discussed above (1.4.4, 2.5.5.2), and also of increasing regulation of health services and social care, as described by Hillman and others (Hillman et al., 2013). Also, both the study findings and the literature review indicate a further contextual factor of low levels of organisational resource devoted to information technology (2.8.5, 4.4, 7.2.3). It is suggested that, being focused on technological rather than behavioural solutions to security issues, and offering users limited information, discretion, scope for decision-making or involvement in policy-making, the approach to information security and cybersecurity within the case study NHS Trusts was of a functionalist, authoritarian type (*cf.* 2.7.2.4.1). It accords culturally with this overall picture, in being low in trust of end-users and highly risk-averse in character. In relation to information behaviour, two areas of activity appeared to be perceived in particular as presenting potentially unacceptable levels of risk: PWU (T4, T3 to some extent) and any form of use of popular social media platforms (particularly T1). This is in keeping with overall organisational characteristics (2.5.5). This argument is elaborated further within the following sections, and related to the proposed theoretical model .

11.3.2 Blocking of websites

False positives have been termed the “friendly fire of information security” (Johnson, Goetz, & Pfleeger, 2009, p. 14). The level of blocking of work-related web content (over-blocking), also termed false positives, in T4 was relatively high, while that in the other Trusts was reportedly low (as discussed in 8.5.1). As stated in 10.3 above, this is likely due to three specific technical factors: 1) the high number of categories of web content that were blocked by SWG4 by default, i.e. its restrictive configuration, 2) (related to 1) a possible inherent lack of accuracy of SWG4 in identifying and blocking inappropriate content, malware, or both, leading to a great many false positives, and 3) the practice in T4, in marked contrast to the other Trusts, of blocking advertising as a possible malware risk on account of “malvertising”. The discussion of ROC curves in Appendix L is relevant here: for a given “real-world” content classifier, in general terms, specificity decreases, and the proportion of false positives increases, as sensitivity is increased. However, the greater the area under the curve, the greater is the specificity of the device for a given level of sensitivity. It may be recalled that 1) in T4 blocking of image content seemed in some instances to block the site entirely, and 2) that levels of over-blocking were also reported as low by P2 in another Trust where another secure web gateway SWG3 was in use (8.3). The high levels of over-blocking at T4 were reported as giving rise to complaints which the IT manager responsible for the device acknowledged were not being acted upon. The recorded negative observations about SWG4 reported in Section 8.3 raise the further technical question of what proportion of “malvertising” content would have been blocked as malware by SWG4 had it not already been blocked as advertising.

As well as technical factors, organisational and cultural factors were apparently involved, including lack of communication. As stated above in Section 10.4, there had been very little involvement of end-users at T4 in the development of AU4Int, as evidenced by the lack of formal consultation with stakeholders (8.2). In addition, it may be recalled that the IT department at T4 was reported by the records and governance manager T4-09 as prone to making decisions regarding systems design and security measures in isolation without appropriate consultation with information governance managers or other stakeholders (4.5.1, 4.5.2). Information governance managers not only had little effective communication with IT, they lacked a direct reporting channel to appropriate senior managers through which they could raise any concerns (4.4.1). A possible channel via which representations could have been made to the IT department about high rates of website over-blocking was thus not available, and it was possible for T4-20 to ignore individual user complaints. Adams and Sasse (1999) suggest that unwillingness or failure of IT departments to communicate with users about security practices may be underlain by the “need to know”, principle, based upon the idea that disclosing information about security processes makes them easier to subvert; it is held that restricting access to this information, therefore, is likely to increase security. Users may therefore have incomplete and insufficient knowledge of security issues that concern them. However, since end-user involvement in the formulation of information security policies is often cited as a motivating factor in ongoing compliance (e.g. Adams & Sasse, 1999; Albrechtsen, 2007) this overall situation within T4 may not represent good information security practice.

The information source horizon concept (Section 2.4.2 above) suggests that perceived non-availability of resources affects clinicians’ established habits of information seeking. The effects are likely to be accentuated under time pressure. The findings from other information behaviour research relating to time pressures and time available for answering clinical questions have also been discussed (Section 2.4.4 above): Brennan *et al.* (2014) reported the doctors interviewed for their study as saying that such were the pressures of their work that even login requirements were an obstacle to information-seeking for them. *A fortiori* it must be inferred that blocked websites present an even greater obstacle. “Satisficing” behaviour (see above, Section 2.4.2) is a factor here also; staff may set “stop rules” for their searching in relation to material that is unavailable, looking for alternative sources (*cf.* T4-03, Section 8.5.3), or just managing without it.

Sasse's (2015, p. 82) observations about the need for security to be usable are applicable to the blocking of websites as well as to authentication requirements for information systems and electronic resources: “In real-world environments, authentication fatigue isn’t hard to detect: users

reorganize their primary tasks to minimise exposure to secondary security tasks, stop using devices and services with onerous security, and don't pursue innovative ideas because they can't face any more 'battles with security' that they anticipate on the way to realising those ideas." Another of her observations (2015, p. 83) is also pertinent: that users' experiencing false positives reduces the overall credibility of information security, thereby tending to undermine its effectiveness. Sasse's concerns here relate also to the concept of security fatigue, as described in Section 2.7.2; reluctance to report blocked websites can be perceived as an aspect of this.

The decision-making process of users faced with blocked websites can be represented diagrammatically in Figure 11.2. The diagram lists the key questions, in a suggested order, which may contribute to a user's decision whether or not to report a blocked website. Affirmative answers contribute to the likelihood of a decision to report, while negative ones reduce it. From the participants' comments cited in Section 8.5.3 it was apparent that the willingness of end-users to report blocked sites depended to a degree upon:

- 1) the importance of the information to the user in the particular instance
- 2) the availability of the information elsewhere (on the web, or via a university or home computer)
- 3) the likely future usefulness of the information – will reporting the site pay dividends later in ensuring its future availability, for myself or for colleagues?
- 4) the relative urgency of the information need – can it wait for a few days?
If so ...
- 5) the overall frequency of encountering blocked websites: high frequencies acted as a demotivator and strong disincentive on account of the negative feelings, time and effort involved (*cf.* 2.5.5.3; 11.2.4)
- 6) the outcomes of earlier requests, including the time taken, or reasons given for refusal to unblock a site
- 7) (partly consequent upon 3 and 6) the degree to which the user felt trusted by IT department staff in placing the request. This factor would have applied in principle across all the Trusts, although in practice far more sites were being blocked within T4 than there were either in T1 or in T3.

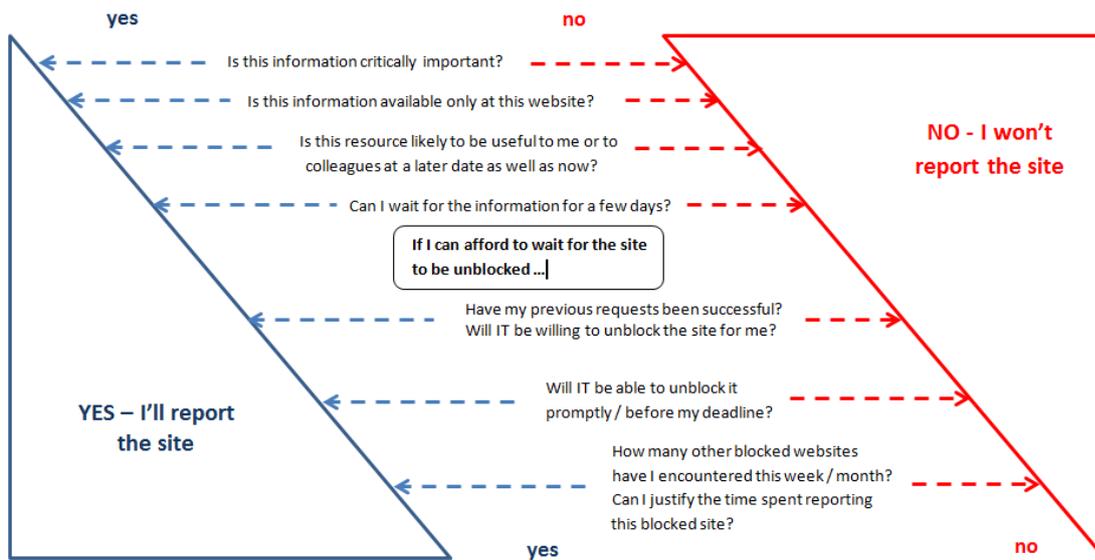


Figure 11.2 Likelihood of users to report blocked websites

The primary purpose of web content filtering within an organisation’s secure web gateway is to represent its Internet acceptable use policy and ensure, as far as possible, that it is followed. The configuration of content filtering settings can therefore be considered part of the policy process. As an aspect of good governance, NHS Trusts are generally keen to monitor the effectiveness of their policies and to minimise unintended negative consequences by evaluating and monitoring their impacts, via measures such as impact assessment, consultations with stakeholders and scheduled reviews.

We have seen, however, that even in a Trust (T4) where complaints to the IT department about false positives were being made regularly (the IT manager T4-20 reported receiving emails from dissatisfied end-users: 8.3), the content of blocked websites notified via automatic alerts or cited in calls to the helpdesk, and hence the accuracy of blocking, was according to T4-20, not being monitored, evaluated or reported (8.3). Other security devices implemented on corporate networks, notably intrusion detection systems, are known to generate large numbers of false positives, which can overwhelm system administrators (Lemos, 2015); from the security management point of view, it is conceivable that alerts generated by the secure web gateway had been perceived as similar to these in character, and the effects of the many false positives on end-users not heeded. All the Trust IT departments were reported, either by end-users (T1, T4) or by one of their own managers (T3) to be under-resourced and under-staffed, and accordingly focused their attention primarily on the support of clinical systems, sometimes at the expense of other IT services (7.2.3.5, 8.2). It is likely that, faced with such pressures, IT security efforts were focused primarily on “housekeeping” (cf. T1-

11's comment in Section 4.5.4 above) and on demonstrating compliance with national standards, i.e. fulfilling the Section 300 requirements of the Information Governance Toolkit (Department of Health, s.d.). It is possible that lack of resources rather than cultural factors (risk aversion, low trust of end-users) may have been the primary operative factor in the lack of prioritisation of over-blocking in T4, although its effect is likely to have been compounded by poor communication (see Section 11.4 below).

The censorship aspect of web filtering (Sections 2.7.3.4.1, 2.7.3.4.2) obviously raised major issues for NHS library services, since librarians generally held as part of their professional value set a strong commitment to freedom of enquiry (Trushina, 2004). CILIP's ethical framework stated that access to information should be blocked on legal grounds alone (CILIP Code of Professional Practice, cited by Brown and McMenemy, 2013). The *IFLA/UNESCO Internet Manifesto Guidelines* (IFLA & UNESCO, 2006, p. 14) stated that "libraries providing access to information on the Internet should do so in accordance with the principles of Article 19 of the Universal Declaration on Human Rights, which states that everyone has a right to ... seek, receive and impart information and ideas through any media ...". The American Library Association, unlike its British counterpart CILIP, had campaigned strongly against web content filtering.⁹⁸

Resnick *et al.* (2004, p. 11) raised the question, "how much over-blocking or under-blocking is too much?" Their view is that people differ in their assessments of the benefits of blocking bad sites and the costs of blocking legitimate sites; the debate hence needs be redirected to organisational and professional values. Here, organisational culture is relevant (2.5). Prince *et al.* (2010) raised a similar fundamental issue, relating to values, of the balance of risk and reward, that is, the possibly negative security risks of less restricted access versus the negative consequences and risks of over-blocking, which, as we have seen, can be considerable. The comparison with higher education is perhaps instructive. Within health services, confidentiality of patient information is of paramount importance, whereas within higher education, networks are highly segmented (S. Pinfield, personal communication), and discussions regarding information security are strongly informed by the need to safeguard academic freedom as a fundamental organisational value. This may be perceived as an

⁹⁸ See, for instance, material on the ALA Filters and Filtering resource page: <http://www.ala.org/offices/oif/ifissues/filtersfiltering> [accessed 12/01/16]

organisational challenge for information security management (e.g., O'Connell, 2005); compare the comments of Werlinger *et al.* (2009) cited above in Section 2.7.2.4.1.

The comments of the SWG vendor's product manager SWG3-01 regarding the impossibility and undesirability of blocking all illegal or potentially illegal content were noted above (Section 4.4.4). Many of the subject areas defined as illegal may not appear to present a problem for legitimate information access and use; however, breach of copyright appears to present a particular issue (*cf.* the comment cited in Section 3.9). It raises the question of the extent to which an organisation can, or should, endeavour to prevent its staff from breaching copyright, or accessing illegally copied or reproduced material, via technical means rather than through information governance training.

As stated in the literature review (Section 2.5.6.2), the application of Clegg's (1989) circuits of power theory to issues of information security policy and compliance by Inglesant and Sasse (Inglesant & Sasse, 2011a, 2011b), is highly relevant to the present study. An outline of the theory, including a general diagrammatic representation, was provided in the literature review. These authors (2011b) used it in conjunction with actor network theory (ANT) to represent two information security scenarios, both very similar to circumstances encountered within the NHS Trusts in the current study, and it is possible to adapt their approach to model the study findings (as shown in Figures 11.3 and 11.4 below). In Scenario 1 within their paper, compliance with restrictive system and acceptable use policies was actively enforced by technological means: restricted use of software on the organisation's personal computers and laptops was enforced through a "closed build" which required approval by a manager and action by IT support staff to install or configure software. A similar policy restricted acceptable use of the Internet through a web filtering device. In Figure 11.2 the three levels represent the three circuits of Clegg's circuits of power theory: *agency*, *social integration* and *system integration*, which correspond to three types of power, *causal* (expressed within information infrastructure controls), *dispositional* (a capacity to wield power) and *facilitative* (methods of enforcement) (*cf.* Figure 2.5).

Comparing the current study findings with Inglesant and Sasse's Scenario 1, one can identify in Figures 11.3 and 11.4 the same three categories of user response: acceptance, resistance and avoidance. The "acceptance" response is illustrated by the finding that, while library staff discussed their need to obtain the IT department's support for the use of alternative browsers (5.3), only one participant (T4-22) mentioned the lack of a facility to install software as an obstacle to his work (6.3). Inglesant and Sasse (2011b, p. 4) suggested that the individuals offering such "acceptance"

responses are, while complying with the policy, in fact affected by it, “not by what they are ‘got to do’, nor even by what they are prevented from doing, but in what they do not even consider doing”. In situations such as these it can be said that the [organisation] has successfully stabilised the meaning of “acceptable use” to the extent that staff members comply without even considering alternatives. In terms of actor network theory (2.5.6.2) they suggested that the various (human and non-human) actors are “enrolled” in a “problematization” that asserts locked-down access as an obligatory passage point (represented by the hexagon on the left of the diagram (Figure 11.3 below) through which access to software must pass. This form of exercise of power may be compared with Lukes’ (1974) characterisation of symbolic power as insidiously shaping people’s perceptions, preferences and values.

Trust IT departments, while sometimes allowing the use of non-standard software where indicated by business need, tried to keep it to a minimum for reasons of ease of maintenance and cost; the process of negotiating its use took time and effort on the part of end-users, as illustrated by the comments of participants in response to the browser survey quoted in Appendix J.

There are two other possible responses of end-users to Scenario 1, those of “resistance” and “avoidance”. Requests for websites to be made accessible, or for non-standard software to be installed on one’s PC or laptop for reasons of business need, or (as T4-22 had done, 6.2) installing software on an apparently unrestricted laptop with the semi-connivance of an IT support staff member, would have constituted “resistance” in these terms. So also would requests for sites to be unblocked, or complaints to IT management (as occurred within T4) or line management about levels of website blocking. Using one’s home computer to access blocked websites (as T4-05 habitually did, Section 8.5.3) or use of an application on one’s personal mobile device to access work-related e-learning material that was not available within the Trust (as a student of T1-04’s had done, Section 6.6), would have constituted “avoidance”.

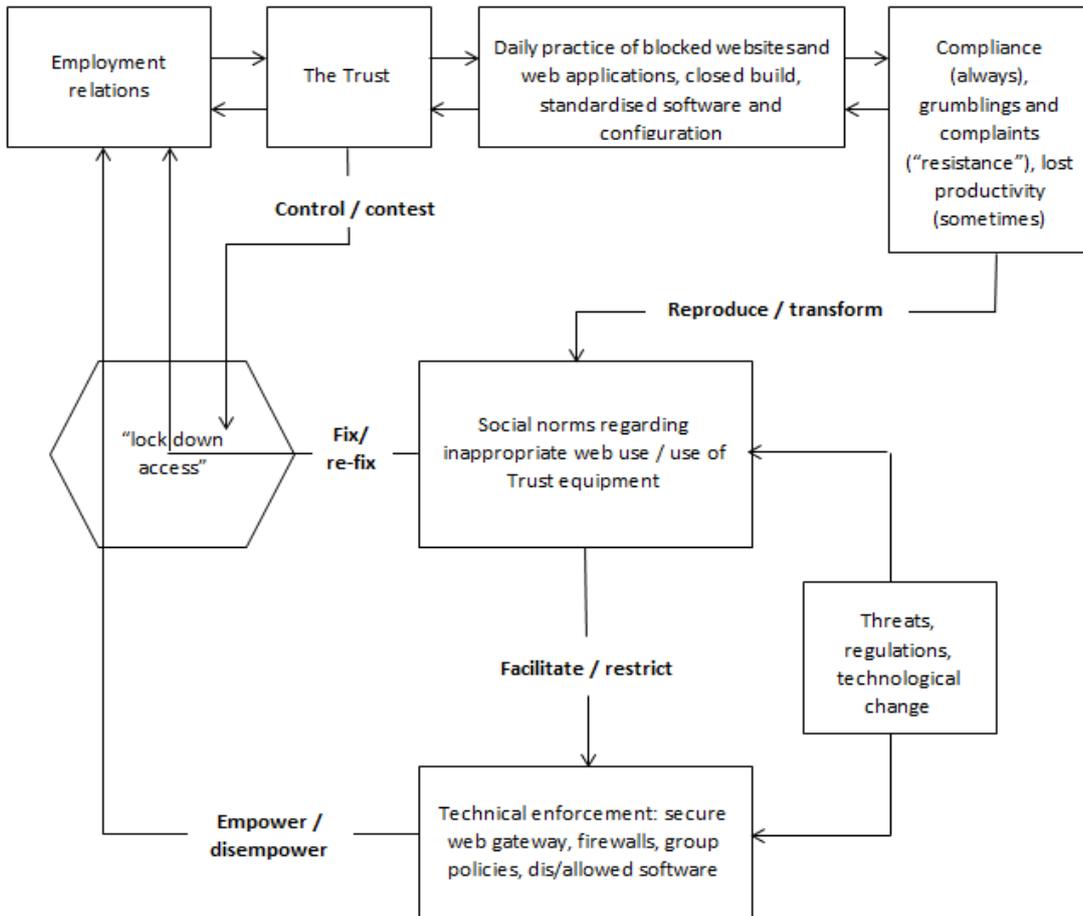


Figure 11.3 Locked-down access to “closed build” PCs and external Internet

Adapted from Inglesant and Sasse, 2011b, p. 4, with permission

Avoidance, as Inglesant and Sasse (2011b) noted, allows users to get the job done. They feel forced to avoid the rules, and are inconvenienced (and lose productivity) in circumventing the operation of the policy by negotiations regarding the installation of the software or unblocking of the website, or in accessing the blocked website(s) at home. Resistance can also involve lost productivity on account of the time involved. Both avoidance and resistance represent total or partial breakdowns of the actor network.

As the authors remarked, the closed build, while simplifying the provision of technical support and reducing risks from software incompatibilities, breach of licence terms or malware, carries a cost in terms of employee time and hence productivity, and also of organisation within the IT department. In effect, the power exercised by the IT department within the organisation is maintained by disempowering staff members. In terms of ANT, the secure web gateway, group policies etc.

constitute *obligatory passage points* (OPPs) through which access to software and to information must pass (see Section 2.5.6.2 above). However the policy and its means of enforcement are bypassed relatively easily by staff using their home computers instead. Using a home computer avoids the resistance, but may be subject in its turn to information governance policy restrictions on account of the risk potential data loss which it presents. There is contested meaning here, in that the security policy constructs points through which all access must pass, whereas staff members ascribed meaning to their own resistance or avoidance behaviour in alternative terms, as relating to business need. The authors suggest, as an alternative to the OPPs, that an attempt should be made instead to stabilise meaning around business needs, so that these become the main “actor”, as in Figure 11.3 below. In this scenario, a less restrictive configuration of the secure web gateway, together with wider options to install and use software which is needed, meets business needs, as shown in the middle pathway, without any need for the resistance which is shown in the right and left hand pathways .

The definition of “black box” in a software development or other IT context is “any device whose workings are not understood by or accessible to its user”. Correspondingly, black box testing is “a ... method in which the tester has no knowledge of the inner workings of the program being tested. The tester might know what is input and what the expected outcome is, but not how the results are achieved” (WhatIs.com, 2008). Commercially available SWGs may be described as black boxes (e.g. Ayre, 2004) in that the details of their workings are kept commercially confidential and are not understood in detail by those who implement them.

This definition may be contrasted with the way in which actor network theory uses the term “black box”. For ANT, a black box is “a technical artifact that appears self-evident and obvious to the user” (Cressman, 2009, p. 6) or “A frozen network element, often with properties of irreversibility” (Walsham, 1997, p. 468). “Black-boxing”, so-called, is a process of closing questions and debates (Levy, 2003). The term “punctualisation” is used to refer to the process by which complex actor networks are black-boxed and linked with other networks to create larger actor networks. An actor network may be considered a “black box”, when its identity has become established, its role, function and presence are no longer questioned, and it has acquired a commonly agreed set of meanings (Goff, 2014). SWGs are seen as technical, but their implementation actually requires management decisions to be made (e.g. regarding the types of content to be blocked, “rationing” of access to web applications, establishing different levels of access for different user groups, etc.). It is suggested that it is particularly easy for systems implemented as black boxes in the IT sense to

become black boxes in the ANT sense, and thus for IT staff to “hide behind” a supposedly given system, failing to accept responsibility for implementing configuration options that meet local needs and preferences and accord with organisational values.

There appeared to be no clinical counterpart to the value of “academic freedom” in higher education in claiming the right of unrestricted access to published information; the notion of “clinical freedom” or “clinical autonomy”, sometimes cited in criticism of evidence-based medicine, refers purely to clinical practice (Hampton, 1983; Parker, 2005). This initially unexpected finding may possibly be accounted for as follows. Regulatory and clinical governance requirements generally exist for clinical practice to be evidence-based or for an evidence base to be demonstrable and documented within the patient record (2.4.4). Such requirements, and hence evidence searching, may be associated by clinicians with the curtailment, rather than the exercise, of clinical autonomy (Brown, 2008). In practice this may, in many instances, involve explicit adherence to NICE and other guidelines, affording relatively little scope for professional judgment; also, specialist advice on medicines is frequently sought from a medicines information pharmacist within a Trust, again documented within the patient record, thereby reducing the need for other clinicians to seek medicines-related information (Kerr, 2009). Website blocking may thus be perceived by clinical staff rather as a (tedious, but tolerable or negotiable) aspect of a defensive NHS bureaucracy than as an infringement of professional rights and prerogatives.

11.3.3 Mandatory use of encrypted portable media

In Scenario 2 of Inglesant and Sasse’s (2011b) paper, the policy requirement described was to use a particular type of encrypted portable media device for transferring files, namely a company-issued, 256-bit encrypted drive of a specified brand. This is very similar to the policy in T1 and T3, although, as it happened, not within T4; while the use of encrypted media for transporting sensitive information was still required within local policies, the Trust IT department there had ceased to issue encrypted USB memory sticks, and port blocking had not been implemented (8.4). Within the terms of Clegg’s (1989) circuits of power theory, implementation within T1 and T3 can be said to have relied strongly upon episodic power; the emphasis was on micro-techniques of enforcement, with very little leeway allowed for alternative interpretations of policy requirements. Concurrent with the encrypted portable media requirement were the restrictions (T1) or blocks on the use of common cloud storage applications, which further enforced the policy by effectively denying users an alternative means of storing and transmitting files.

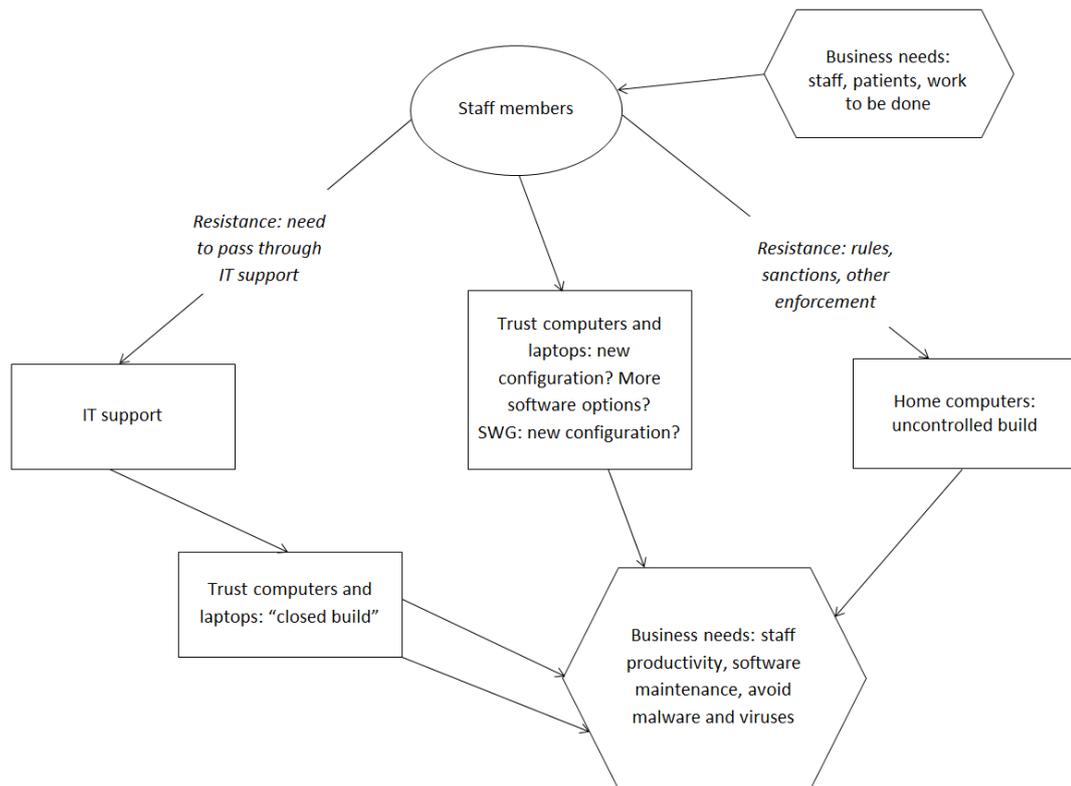


Figure 11.4 Re-thinking circuits of power in acceptable use enforcement

Adapted from Inglesant and Sasse, 2011b, p. 7, with permission

Within T4, the power circuits of social and system integration were more important. However, within both the episodic and the social/system integration circuits, there were factors operating within T4 that discouraged compliance with the policy. Before the IT department in T4 had ceased to issue them, approved encrypted memory sticks had been expensive and relatively difficult to obtain, and were also hard to obtain in T1. The devices were also perceived as having inherent limitations, mostly relating to slow loading of content, causing some inconvenience when making presentations at events (5.2.1). In the absence of port blocking at T4, their use had effectively become dependent upon user compliance and user effort, thereby involving what has been identified (Beautement & Sasse, 2009; Beautement et al., 2008) as the *compliance budget* (2.7.2.4.2). Hence it can be seen that there are considerable tensions between system and social integration within the Trusts' security systems and processes, in respect of the prohibition on software installation (for T4-22), the blocking of websites (T4 generally), and the requirement to use only approved encrypted portable media provided by the IT department (T1, T4 generally). It will be recalled that system integration refers primarily to technological means of control, whereas social integration involves the *meaning* attached to entities, whether social or technological, through which controls are exercised; it also involves rules of practice and membership categories (2.5.6.2). The actors here were not able to

enact the rules which they had accepted and wished to enact, because security processes did not offer the conditions which would allow them to do so (Oliveira, 2010). Inglesant and Sasse (2011b) suggest that attention should be given to the *meanings* attached by users to information security practices: they ask: “How can meaning be most successfully stabilized around the needs of the business?” (p. 7). They also suggest that the concept of “business need” is primary in establishing information security practices that are acceptable to end-users, usable and stable.

11.3.4 Empowerment, engagement and access to information

According to Kanter’s theory of structural empowerment, access to information, that is both published information relating to professional expertise and information about one’s organisation, is one of the structural conditions of staff empowerment (Laschinger et al., 2010; see literature review, 2.5.6.1). It should therefore follow that lack of access to professionally-relevant information is *ipso facto* disempowering. It is disempowering for another reason: barriers to accessing and using online published information that result from organisationally-imposed access controls represent a limitation of staff autonomy, and could be construed as an expression of lack of trust of staff by IT and other managers (see literature review, Section 2.5.5.3; also above, 11.1.3). Greco *et al.*’s (2006) model of the antecedents and consequences of empowerment and engagement (Section 2.5.5.3) suggests that these forms of disempowerment can directly contribute to staff disengagement. In terms of antecedents and consequences, it proposes a possible causal route through which levels of access to information and to job resources such as adequate computer infrastructure could affect levels of staff engagement, and thereby organisational effectiveness and performance, including clinical outcomes (Figure 11.1). Level of organisational trust is represented within the overall theoretical model (Section 11.1, Figure 11.1) as constitutive of information security posture.

It is suggested, therefore, that barriers to information seeking and use can have both direct and indirect negative effects upon both clinical and organisational effectiveness. The direct effects have been described in detail within the results chapters (5 to 10) above. The links to clinical and organisational effectiveness may readily be identified within the “infrastructure” and “quality methods” areas of the clinical governance process (shown in Figure 1.2): directly in the elements of “access to evidence”, “information technology infrastructure supports practice”, and “well trained staff”, and less directly in “clinical policies evidence-based” and “good practice spread”. The indirect effects occur via the mechanism proposed below in Figure 11.5, i.e. structural empowerment and staff engagement.

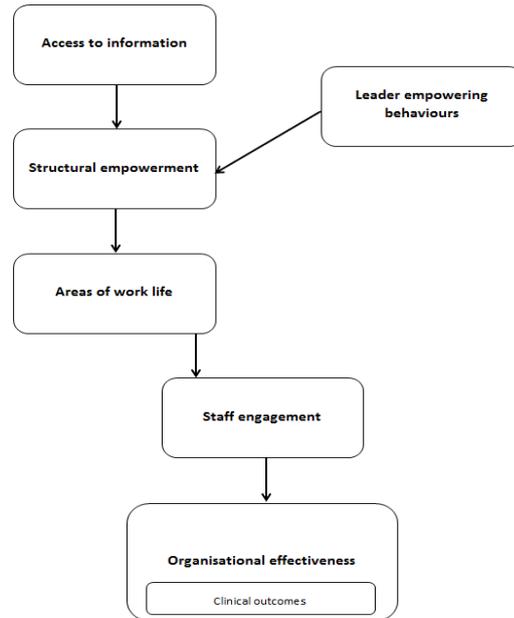


Figure 11.5 Proposed mechanism of effect of access to information on organisational effectiveness
Adapted from Leiter & Maslach, 2003

11.3.5 Information security / governance risk

Very few explicit references were made by any of the IT managers to management of information security or cybersecurity risks. The implicit nature of risk minimisation, as well as coverage of information security risk management in official documents, may go some way to explaining this. For instance ITIL v3, formerly referred to as the *IT Infrastructure Library*, makes explicit reference to identifying and managing risks as part of the service design phase (Faber & Faber, 2010; Sheikhpour & Modiri, 2012). ITIL provides internationally recognised best practice guidance for all aspects of IT service management (Cabinet Office, 2011a, 2011b, 2011c, 2011d, 2011e). It can be used to provide comprehensive information on how to implement the information security standards mandated via ISO/IEC 27001 or the NHS IG Toolkit (Clinch, 2009). Although the use of ITIL was not mandatory, it was supported by the former NHS Connecting for Health and was widely used within the NHS (Haw, Derry, & Gowing, 2006). Another contributory factor may have been the tacit nature of much decision-making in information security management, as described by Werlinger and associates (Botta et al., 2010; Werlinger, Hawkey, Botta, et al., 2009)(2.7.2).

The work of Werlinger's team has implications for the nature of risk analysis and risk management in information security and cybersecurity. In the literature review (2.4.7) it was noted that tacit

decision-making had also been observed in clinical contexts, regarding the applicability of forms of encoded knowledge to particular cases. On these grounds Alaszewski, Alaszewski and Potter (2006) expressed criticism of what they term the “expert” approach as represented within formal methods of clinical risk management: it fails to recognise the ways in which social context influences the ways in which risks are identified and managed, and in particular the agency of individuals in structuring risks. Analogous criticisms were expressed by Baskerville (1991) and others (see Section 2.7.2) of conventional methods and techniques of information security risk assessment and management; for Baskerville, they represented not a fully “scientific” approach, but a valid means of generating contextually-situated professional knowledge using intuitive judgements.

Lafferty (2013, 2015) had suggested that the understanding of social media in general within the NHS was poor, and failed to balance risks and benefits (2.7.3.4.2). One of the few extended discussions of risk took place with T1-07 (senior nurse manager) regarding the catastrophic impacts of breaching confidentiality and therefore patients’ trust via social media. In her view, the enormity of the negative consequences of breaching patient confidentiality via social media justified a total ban on accessing social media via the Trust’s network (9.2.1). Social media risks were also mentioned by the communications officer T3-12, who spoke of a necessary balance of risk and reward, and of the need to have safeguards in place (9.2.4.1). In her view, these risks had been evaluated within her Trust and deemed to be acceptable.

The sociological theories of risk reviewed briefly in Section 2.7.1 above indicate that different groups have different perceptions and understandings of risk (Vaast, 2007), and that risk management in general is a highly political process, in which values play an important role (Douglas & Wildavsky, 1982; Douglas, 1992; Jasanoff, 1998; *cf.* Section 2.5.5.2 above). Use and regulation of Web 2.0 and social media applications was evidently a contentious area, as evidenced by the wide range of opinions and attitudes to them among study participants, ranging from considerable enthusiasm to strong dislike and disapproval (7.5). One aspect of the cultural theory of risk (Douglas & Wildavsky, 1982a), the propensity of subjects to evaluate activities of which they disapprove as high risk, may therefore be particularly applicable to social media policy. Social media issues are discussed further in 11.3 below. Attitude to risk is represented in the proposed theoretical model (Section 11.5, Figure 11.1) as a key constituent of information security posture.

11.3.6. Impact of information governance / security incidents

The literature review suggested in Section 2.7.2 that serious incidents involving actual or potential breaches of confidentiality of patient or staff personal data occurring within the past few years would have had an adverse impact managers’ trust of staff, leading to more restrictive attitudes and practices in information governance, relating particularly to storage devices and services, Internet

acceptable use policies and social media (cf. Ezingear, Bowen-Schrire, & Birchall, 2007; Volpentesta, Ammirator, & Palmieri, 2011). This indeed proved to be the case in respect of social media, with a highly restrictive policy having been introduced at T1 following a single breach of confidentiality incident (as described in Section 9.2.1). Conversely, in the opinion of one participant (the records and governance manager T4-09), the relative laxity at T4 regarding technical enforcement of information security measures (encryption, port blocking etc.) was attributable to the fact that none of the Trust board members had had experience of data breaches and their consequences. He felt that a serious data breach would need to occur in order to highlight to them the importance of such measures (Section 4.4.3; cf. Sections 1.4.4, 2.7.2). The effects of information governance incidents on organisational trust, attitude to risk and hence on overall information security posture are represented in the overall theoretical model, Figure 11.1.

11.4 Approaches to innovation

Rogers' (1966/2003) theory of diffusion of innovations (2.8.1) may usefully be applied to aspects of the study findings relating to Web 2.0 and social media policies and use of mobile devices, which exemplify the Trust's approaches to innovation. There are two aspects of the Trusts' social media policies which need to be considered: corporate use of Web 2.0 and social media applications, and regulation of the individual use of them within Trust networks. Within the proposed theoretical model (Figure 5.11), these are said to constitute key components of an organisation's overall culture of innovation. One part of the DoI theory concerns the manner in which characteristics of innovations influence the rate of their adoption. It suggests that there are five pertinent ones: *relative advantage, compatibility, complexity, trialability, and observability*.

Relative advantage: the relative advantages of using Web 2.0 and social media for professional purposes did not seem readily apparent to participants who were accustomed to more conventional methods of professional networking; indeed they were often perceived negatively as wasting time. Existing work-related uses of Twitter were sometimes deprecated as being trivial (T4-10, 5.5). Some participants expressed awareness of the potential uses of social media for patient and public engagement (9.2.4.1). It is likely that Facebook in particular was perceived by some participants as essentially a platform for the exchange of social trivia (e.g. T1-09, 9.2.3), and this perception was generalised to other social media as a "technology cluster" (Archibald & Clark, 2014; Rogers, 2003, p. 249), leading to the non-recognition of their potential benefits.

Compatibility: social media were perceived as incompatible with participants' existing values in that they were perceived as a risk to confidentiality and the maintenance of appropriate professional boundaries. Participants were explicitly aware of the risks of misuse and of previous instances of

misuse (e.g., 7.5). T1-02 spoke of professional social media use being perceived negatively as “slacking”, and of a perception that work environments were not conducive to it (9.2.4.1).

Complexity: while not necessarily perceiving social media as technologically complex, participants felt very much in need of training and guidance from their Trusts on what was permissible in the professional use of social media (7.5). They did not feel comfortable in the online environment, or that professional usage of social media would be “natural” to them, unlike their younger colleagues, students or children (9.2.3).

Trialability: perception of the trialability of social media for corporate use varied between organisations and participants. A decision had been made in T1 to experiment with small-scale corporate use of Facebook and Twitter in limited contexts for specific purposes, reflecting a perception that it was trialable, and that usage could be extended if results were favourable. However, in T3 one participant (T3-09, 9.2.4.1) spoke of “breaching [*sic*] the Rubicon”, reflecting a sense that venturing on to social media was a commitment that was essentially irreversible.

Observability: participants in T3 had become aware of the increasing levels of social media use by other organisations within the Trust’s environment, such as suppliers, regulators and professional bodies (9.2.4.1). Observability was not raised as an issue by participants, for either individual or corporate use of social media. In T1, methods of evaluating the visibility and impact of the Trust’s experimental social media presence were not mentioned. Communications staff in T3 and T4 did not discuss any forms of monitoring of their Trusts’ social media presences.

Another part of Rogers’ theory (2.8.1) concerns the processes of individual and group decision-making relating to innovations. Four main stages are involved: *knowledge*, *persuasion*, *implementation*, and *confirmation*. Prior conditions such as *previous practices*, *individual needs*, *propensity towards innovation* and *social system norms* influence the process. Regarding social system norms, it was suggested in the literature review (Section 2.8.4) that restrictions on access to social media applications within the workplace could reflect an IT-culture conflict (Koch et al., 2011; Leidner & Kayworth, 2006); these authors expressed the view that a perceived inherent conflict with organisational or professional culture and values could act to restrict access and to inhibit staff from exploring possible uses of different Web 2.0 and social media applications (e.g. discussion forums, blogs and wikis) within the workplace to support professional activities. The overall culture of the NHS has been described as risk-averse, bureaucratic, highly regulated, and compliance-focused (Alaszewski & Horlick-Jones, 2002; Maddock, 2002; Matthews, 2009). It is suggested that an IT-culture conflict of this nature was operating within all three Trusts to varying degrees: most strongly within T1 and least strongly within T3 in relation to corporate use, and strongly in both Trusts in

relation to individual use. Within T4 a mixed picture was apparent: corporate use was well established within some services, but for individual use this was far less so.

Some of the factors identified by Rogers (2003) and others (Section 2.7 above) as being relevant to organisational readiness appear to be salient within the study and for the NHS as a whole. NHS Trusts are comparable in their degrees of centralisation, formalisation, and complexity, all of which are high. According to Rogers (2003), centralisation and formalisation inhibit innovativeness; complexity encourages organisation members to grasp the value of innovations, but may make them difficult to implement on account of the difficulties experienced in reaching consensus. We have also seen that, while a certain appetite for risk is required for successful innovation, external pressures on NHS organisations tend to drive them toward risk aversion (2.5.5.2 above). It may be concluded, then, that the NHS organisational environment is generally not conducive to innovation, even though innovation has been cited as a major strategic priority for the NHS (Department of Health, 2011b; Royal College of Nursing, 2012a; Young Foundation, 2011).

T1, T3 and T4 varied in their levels of interconnectedness. T1 had one main site and two subsidiary sites, possibly facilitating greater interconnectedness among staff based at the main site; T3, typically of mental health and community services, was a multi-site organisation, reducing possibilities for interconnectedness among some staff groups. T4 incorporated a number of specialist hospitals, which (as discussed in 4.1.2.2 above) tended to function as discrete communities. The Trusts varied also in size (T4 was much larger than the other two) and degree of organisational “slack”; it was evident to the researcher at an early stage that T1’s level of organisational “slack”, as indicated by the low staffing levels of corporate functions such as communications, information governance, training, research support and human resources, was relatively very low. Correspondingly, the Trust had outsourced the drawing-up of its IT strategy, and was a late adopter of several innovations including e-learning, the corporate use of social media and of electronic patient records (EPR); it may be inferred that its absorptive capacity was also low. T4 also had not yet implemented EPR, but was devoting considerable resources within its informatics department to developing its own system rather than implementing a commercially available one (4.4.1). It was also planning a number of other IT innovations.

End user policies are a primary governance vehicle employed by organisations to respond to employees’ use of social media (Cain, 2011; Cox, 2014). The work of Vaast and Kaganer on organisational social media policies (Kaganer & Vaast, 2010; Vaast & Kaganer, 2013) is directly relevant to the study’s findings on social media policy and access within the three Trusts. It will be recalled (Section 2.8.5) that these authors analysed corporate responses to user-driven technologies in terms of a shifting of the comprehension or shared understanding element of decision making

about possible adoption into the time frame of implementation and assimilation. Decision makers are thus faced with a pressing need to devise policies just as they are starting to make sense of the innovation themselves. This corresponds closely with the blocking observed within T1 of all social media activity until the Trust's policy had been developed (9.2.3). Social media policies, and those relating to mobile devices, are represented within the proposed theoretical model (Section 11.1, Figure 11.1) as a major component of culture of innovation.

In both T1 and T3, participants reported that shifts had occurred recently in corporate thinking about social media, regarding its use for corporate communications as well as by individual professionals. It is suggested that a version of the processes described in Figure 2.15 (Chretien and Kind, p. 1139) may have been taking place within the case study Trusts in relation to social media at a number of levels: organisation-wide, among professional groups, and at the level of the individual clinician; this application of Maslow's hierarchy of needs to social media therefore has some explanatory potential. T1-07 (reported in Section 9.2.1) spoke of addressing security concerns via disciplinary action imposed on staff who misused social media as a precursor to introducing a Trust social media policy. As to the reflection and discovery phase, the Trust, as stated earlier, was starting to experiment with the use of Facebook and Twitter for patient and public engagement, and had implemented more granular controls in line with current industry trends. The librarian T1-01, through her innovative efforts to make use of applications such as blogs and Prezi to provide new library services, had gone some way towards educating information governance managers about their workings and character, thereby facilitating the processes of reflection. One participant in T3 (T3-09) spoke of changes in practice regarding social media as "gently washing in" following very extensive (but inconclusive) discussions across the organisation of possible corporate risk. The library service at T4 was also leading the processes of discovery via its use of social media applications to provide a current awareness portal and a Pinterest infographics site (5.5). NHS Employers had persuasively championed via its publications the use of social media within the NHS (NHS Employers, 2013a, 2013c, 2013d, 2014). The increased availability of policy guidance on the use of social media produced by professional regulators (General Medical Council, 2013; Health and Care Professions Council, s.d.; Nursing and Midwifery Council, 2015) and other professional bodies (British Medical Association, 2011; Royal College of General Practitioners, 2013; Royal College of Nursing, 2009; Royal Pharmaceutical Society, s.d.), as well as the increasingly-common inclusion of "e-professionalism" as a topic within health professions' pre-registration and post-registration training curricula, may have served to address security concerns, enabling policymakers to consider the issues of how best to use social media, both corporately and individually, in support of the Trust's business objectives.

Several participants (9.2.3) spoke of marked generational differences in attitudes to social media use. Similarly Sandars and Schroter (2007)(among UK doctors and medical students), and Taylor, McMinn, Bufford, and Chang (2010)(among USA-based psychologists) identified age-related differences, likely due to a cohort effect, in understanding the workings of social media and in perception of what constituted appropriate social media use. Students and younger professionals were far more likely to be familiar with social networking technologies and to use social networking websites than older ones. According to Jones and Hayter (2013, p. 1496), older professionals' lack of involvement with social media presents a risk: "More experienced and more cautious practitioners may be less likely to use these technologies and potentially are more likely to encourage others to avoid their use, increasing the likelihood of students failing to engage in helpful discussions about privacy and professionalism ... It is ... important that clinicians involved in mentoring students are engaged with the issues associated with social media and can reinforce good practice from the clinical perspective". The applicability of their comments to teaching and training taking place within NHS settings is readily apparent. The indications presented of a generational divide in attitudes to social media have potential implications for the delivery of LIS (Lacey Bryant, 2016).

11.5 Professional jurisdictions, professional projects

The general point which can be made about IT support, which may be applicable to the T4 findings in particular, is that, despite the widespread use within the NHS of ITIL (Cabinet Office, 2011), which should inculcate a service orientation, IT departments in general can display a tendency to be technology-focused rather than customer focused, and do not always appreciate the impact of their activities on the business of the organisation (Bruton, 2002; Cater-Steel, 2009, 2010).

Indications of disputes over areas of jurisdiction, or of potential or actual professional projects (Abbott, 1988; Kirkpatrick, Ackroyd, & Walker, 2007; Larson, 1977) were provided by several participants. Reference was made in Sections 7.2.1 and 7.2.3.8 to apparent disputes over areas of jurisdiction between the T1 library manager and IT staff regarding the Trust's new intranet, and at T4 between the records and governance manager T4-09 and the IT department regarding EHR developments; generally T4-09 felt that the information governance function within T4 was treated as an "afterthought" and was not able to operate effectively (4.5.1, 4.5.2). There were also indications of considerable variability in jurisdiction relating to information governance and information security (P2, T4-09, T3-03; 4.5.2). (Lomas (2010) attributed the assumption of responsibility for information security on the part of records managers to the aftermath of the October 2007 HMRC data loss; see Section 2.5.5.2 above.) The library manager at T1's proposed service initiatives, based upon Web 2.0 or social media platforms, during the previous few years had been consistently blocked by integrated governance while the social media policy was being

developed (9.2.3). The senior risk and governance manager T1-12 felt that the IT department tended to abdicate what she felt were its information governance responsibilities in favour of a purely technical role (4.5.2). The records and governance manager T1-09 felt that the records management aspects of information governance were under-developed and not well understood within the NHS, compared with the government department in which she had previously worked (4.5.3). The IT manager T3-06 was surprised to discover that the training department retained the services of a full-time e-learning developer (6.2). Overt conflicts involving communications staff were not mentioned by participants; however, it should be borne in mind that adoption of social media for corporate and departmental communications would have involved a loss of monopoly control of output and also the need to respond in a timely fashion to comments made via social media by patients, carers and members of the public, thereby entailing significant changes to the roles of communications staff, with the addition of training and supervisory responsibilities (T3-12). Within the overall model (Figure 11.5), the overall outcomes of disputes over jurisdiction constitute a key determinant of information security posture, and hence of culture of innovation.

As well as disputes over jurisdiction, and hence an element of power struggle (discussed in Section 2.5.4), it is likely that fundamental differences in professional cultures, identities and values were involved here between groups of staff and managers responsible for information governance, information security, library and information services, and communications. Conflicts between and within professional groups in the NHS over information security and access to information are described by Adams, Blandford and Lunt (2005) and by Adams and Blandford (2005). Such differences could potentially include differences in information security culture and approaches to information security (Kolkowska, 2011) (see Section 2.7.2.4.1 above). Habits of information technology use in general (Boudreau, Serrano, & Larson, 2014; Stein, Galliers, & Markus, 2012), and information behaviour in particular, are strongly influenced by professional group affiliations (Edwards et al., 2013) and are fundamental to, or even constitutive of, professional identity (Brown & Duguid, 2001; Lloyd, 2009; Sundin & Hedman, 1996). It is unsurprising therefore that information systems and services become a primary arena for inter-professional conflicts. One would expect the values and opinions of NHS library and information professionals strongly to emphasise freedom of information, as outlined in the IFLA and CILIP codes (CILIP, 2004; IFLA & UNESCO, 2006). These would include upholding the view that restrictions on access should be the minimum required by law, and prioritising the support of information seeking and use, including the development of new information services (Dole, Hurych, & Koehler, 2000; Koehler, 2003). Within IT occupational values, the need for following formal, structured control processes was identified by Jacks and Palvia (2011) as a major theme. Similarly one would expect clinicians to emphasise the confidentiality of patient information (e.g. Adams & Blandford, 2005; Fernando, Choudrie, Lycett, & De Cesare, 2012) and records and governance professionals to focus on the task of information governance in general.

According to the HSCIC (Health and Social Care Information Centre, 2015b), information governance provides a framework to bring together all the legal rules, ethical guidance and best practice that apply to the handling of information, allowing implementation of central advice and directives, compliance with the law, and year-on-year improvement plans. Its fundamental task, according to Lomas (2010, p. 184) is that of “putting in place information management programmes to ensure that information is controlled to ensure it is ‘appropriately’ available but that its security is not compromised.” This was clearly expressed by T4-09 in his comment about the role of information governance in electronic patient record implementation (4.5.2).

The literature review (2.5.4, 2.5.5.1) made reference to the ways in which professional cadres within a professional bureaucracy are able to exercise power to resist service developments they do not like via their monopolies of specialist operating knowledge. Not only do IT systems themselves function as key instruments of organisational control (Silva, 2007), but the overall high level of dependence that organisations have on IT means that IT professionals generally constitute a powerful and influential group within organisational politics (Markus & Bjørn-Andersen, 1987; Setterstrom & Pearson, 2013). In particular, they may exert a strong influence on both the formulation and the implementation of information security policies (Lapke & Dhillon, 2008). Notwithstanding the general lack of representation of IT management at Trust board level (Hoeksma, 2015), it is suggested that IT managers within the NHS, as well as clinicians, may function as an expert group with strong powers of veto. In particular, their judgments relating to information system practices, information security or cybersecurity are unlikely to be questioned by senior management, who may not appreciate the limitations of information security risk management knowledge and practice (2.7.2, 11.3.5). This type of process is described by Hickson, Hinings, Lee, Schneck, and Pennings (1971, p. 217), according to whom “the division of labor becomes the ultimate source of intra-organizational power”. Power in their definition is strongly linked to the ability to cope with uncertainty on behalf of other parts of the organisation. It is also linked to centrality within the workflow. The power of IT managers may also relate to the “revered” form of IT organisational culture identified and described by Kaarst-Brown and Robey (2006). Such an exercise of power is not linked specifically to a professionalisation strategy as such; as we have seen (2.5.4), information technology practitioners as a group within the UK are marked by “weak professionalisation”. It seems that information security experts are content for current and prospective employers to judge them purely on the quality of their work; they do not appear to perceive any need to pursue a conventional professionalisation strategy (Reece & Stahl, 2015).

Several features of the typical functionalist information security management scenario conceptualised by Rastogi and von Solms (2012) (see 2.7.2.4.1 above) are identifiable within the information security management arrangements of the Trusts: the somewhat negative tone of

AU4Int (8.2); the lack of monitoring of the impact of the AUP and of its enforcement (all three Trusts) (8.2); the expression sometimes of patronising attitudes towards users on the part of IT support staff at T4 (7.2.3.6; cf. Guzman et al., 2004; Guzman, Stam, & Stanton, 2008; Rao & Ramachandran, 2011); IT managers' focussing their attention more on misuse of the Web, i.e. on insider threats, rather than on facilitating professional information seeking and use (T3, T4) (8.5.4); and apparent lack of consultation with staff in formulation of AU4Int and AUPSec (8.2). As far as wider organisational values are concerned, there is the general issue here of the appropriateness, as well as effectiveness and consequences, of enforcing acceptable use policies solely via technical measures rather than primarily as a disciplinary matter; of treating NHS staff, in fact, as responsible adults who are able to make informed decisions about information resources and manage their use of time at work appropriately (B. O'Leary, personal communication, October 2011); the findings suggest that this was not consistently being done. The possibility arises that negative attitudes to information seeking (2.4.5) may have wider effects, "legitimised" by information governance and security concerns, on organisational decisions regarding computer facilities for staff and strategic priorities for IT infrastructure within NHS Trusts. Levels of organisational trust / distrust may play a part here, as may also conflict between and within professional groups over information security and access to information (Adams & Blandford, 2005).

The IT department at T4 was reported by T4-09 to manage projects in an exclusive, non-consultative fashion (4.5.1, 4.5.2) and, in particular, as failing to involve representatives from information governance in a major electronic patient record implementation project. Greenhalgh *et al.*'s (2010) case study of a Summary Care Record implementation within primary care services suggested that exclusion of information governance could have potentially serious consequences regarding the incorporation of measures to ensure legitimate access to records, etc.; so also do the work of Baskaran, Davis, Bali, Naguib, and Wickramasinghe (2013); Linsley, Kane, and Owen, (2011); and Singleton, Pagliari, and Detmer (2008). In contrast with prevailing practice within the other Trusts, information governance staff also were not involved in the management of web filtering practice, or in other aspects of information security policy. The IT department at T4 had purchased an email encryption solution, but had not publicised it or produced any operating procedures for it; the records and governance managers had done so once they became aware of the situation. Communication between the two departments appeared to be minimal, and cooperation between them to be confined to technical investigation by IT of reported information governance incidents (4.5.2).

There are issues relating to national structures that are of relevance here. The view of a senior manager at NICE, NICE-01, that the history of problems with HDAS raised major questions about strategic responsibility within the NHS for the overall quality of IT provision within Trusts, was

reported earlier (5.3). It was noted in particular that responsibility for providing access to evidence sources, which was located within the National Institute for Health and Care Excellence (NICE), was split off both from areas of other health informatics responsibility, which sat with the National Information Board within NHS England (strategy), with the Health and Social Care Information Centre (provision of information, data and IT systems) and from NHS Library and Knowledge Services, which were the responsibility of Health Education England. The series of transfers between different organisations of the National electronic Library for Health / National Library for Health / NHS Evidence were described above (Section 1.4.5). Apart from indicating volatility within the organisational and political climate, this history of instability suggested a possible cultural unwillingness on the part of the NHS informatics community to assume responsibility for the support of access to published information, or perhaps even to recognise the significance of the management of information and knowledge services as a legitimate aspect of health informatics activity (*cf.* Sections 1.4.5, 1.4.7, 2.5.4). The organisational separation, complained of by NICE-01, also considerably reduced the leverage for possible improvements in IT infrastructure to support knowledge and learning services.

The design of the NHS information governance system, encompassing as it does concepts of management, information security, public accountability and legal compliance, clearly implied that information governance and records managers should hold a level of management responsibility for information security (1.4.4; Lomas, 2010). However, despite the existence of the information governance group on which they were represented, the records and governance managers in T4 were apparently not able to exercise one (4.5.1).

11.6 Summary

This chapter has discussed three main theoretical areas of relevance and interest: interactions of power, culture, trust and risk in information security; approaches to innovation; and the effects of inter-professional conflicts and competition. It has also proposed an explanatory theoretical model unifying these different perspectives to represent the major factors influencing access to online published information within the NHS in England. It has been made evident that the roots of problems with access to, and use of, such information lie deep within the culture and organisational characteristics of the NHS and its use of IT. The following chapter goes on to present overall conclusions from the study and recommendations for further research and for policy.

Chapter 12. Conclusion and recommendations

12.1 Introduction

As explained in Chapter 1, the study set out to explore organisational and technical barriers to online information seeking, sharing and use by health professionals and managers within the NHS in England, in support of professional development and of clinical and management decision making. Such barriers were perceived as potentially affecting adversely both the quality of clinical care provided and organisational effectiveness. In doing so the research focused in particular on investigating an apparent contradiction in the implementation and effects of regulatory policies and practices. These at once supported staff training and development, and required that clinical and management decisions be made according to the most current best practice evidence, but also appeared to result in restrictions on access to, use and sharing of published information, as attested to by clinical educators and information professionals.

This chapter revisits the background to the study (12.1) and summarises its overall conclusions (12.2). It goes on to discuss the extent to which the research objectives have been met (12.3), and its methodological limitations (12.5), with an outline of its contribution to new knowledge (12.6). This is followed by recommendations for further research (12.7) and recommendations for practice within the NHS (12.8), including information security and governance practice and social media training, with a final concluding section (12.9).

12.2 Overall conclusions

On the basis of the foregoing discussion (Chapter 11), it is suggested that barriers to accessing published information resulted from a variety of factors; they:

- 1) arose from the relative inadequacies of IT infrastructures and from historical constraints on infrastructure (e.g. from NPfIT legacy systems) – themselves reflecting low levels of expenditure on IT in relation to turnover and historically negative cultural attitudes to IT on the part of health professionals and managers (6.4.5; *cf.* the roles of level of corporate resource, and of quality of IT infrastructure and its management in Figure 11.1);
- 2) reflected a support priority given to clinical and corporate systems (4.5.4, 5.2, 7.2.3.5, 7.2.3.9), and adoption of cybersecurity “coping strategies” (e.g. implementing default configuration of secure web gateways, and not fully implementing their available functionality or monitoring their performance) by under-staffed NHS Trust IT departments (4.5.4);

- 3) represented a “side-effect” of measures implemented to address information security concerns related to PII, e.g. mandatory encryption of portable media (5.2.1). This, in turn, reflected a high priority given to data protection and privacy, and possibly also a high level of fear in relation to it, both organisationally and individually, on account of the possible disciplinary and financial sanctions that could be imposed for data breaches (4.5; *cf.* 1.4.4);
- 4) related to this, reflected an apparent lack of awareness, or prioritisation, of the importance of the NHS as an environment for pre-registration and post-registration professional educational and training, and of the information needs of students on placement and of trainees, as reflected particularly in problems with providing access to Trust networks and networked applications (4.2.2, 5.2.2.1, 6.2);
- 5) reflected a relatively authoritarian, centralist service culture within some NHS IT departments, and insufficient business alignment or customer focus (*cf.* 11.3.1);
- 6) reflected a lack of organisational readiness for user-driven innovation, in particular regarding mobile devices and the use of social media (11.4). This latter may have been linked with an expectation, based on recent history but disavowed in current NHS IT strategy (McBeth, 2016b), that significant IT innovation in the NHS should be centrally driven and funded, that is, “top down” rather than user- or clinically-driven (*cf.* the role of “culture of innovation” in Figure 11.1);
- 7) reflected degrees of IT-culture conflict (Leidner & Kayworth, 2006) between particular information technology applications bearing upon information behaviour (secure web gateways, Web 2.0 applications, popular social media platforms) and the organisational culture of the NHS (11.4).
- 8) reflected a fragmentation in responsibilities for NHS IT services, in particular the separation of responsibility for NHS Evidence, which lay within the remit of NICE, from the rest of NHS IT (governed by the Department of Health, NHS England, and HSCIC) and from NHS library services (governed by Health Education England)(1.4.5).

With such a strong cultural focus on the secure management of personal information, including patient records and confidential business information, including activity and performance data (4.5.4), sight was apparently being lost at corporate levels, and within IT departments within the NHS, of the need to facilitate access to, use and sharing of published information to support professional development and decision making. IT and IG staff, and senior clinicians and managers, in keeping with the generally risk-averse culture of the NHS, could also be exclusively focused on insider threats, such as risks or possibilities of misuse of access to the Web and Web applications, rather than on the benefits of their proper use, which may have been insufficiently encouraged or

supported. It is also possible that policy “silos” at national and at Trust level (*cf.* the findings of Smith and Katikireddi (2013) relating to policy making in public health) may have been involved, reflecting an organisational tendency to perceive information security and cybersecurity solely as a technical matter, unrelated to other areas of policy and practice. Since the theoretical model of 11.1 is partial in its representation of relevant organisational factors, and some of the proposed constructs are abstract in nature, only points 1) and 6) of these conclusions readily map to it.

12.3 Extent to which overall research aim has been met

The stated overall aim of the research was as follows:

To investigate barriers to online professional information seeking, use and sharing occurring within the NHS in England, their possible effects (upon working practices, working lives, education and clinical and organisational effectiveness), and possible explanatory or causative factors.

Since there had been little previous work in this area, the research was intended and planned as an exploratory and explanatory case study. The scope of possible issues to be addressed proved to be wide-ranging and complex. In some respects, the study was of insufficient scope, in terms of the methods it was able to adopt, to address the research aim as originally conceived.

The study aimed to investigate the nature and extent of barriers to online information seeking. A range of different barriers occurring within the Trusts of the study were identified and described in detail. However, it was not possible to include within it any national survey or log file analysis element, hence the overall prevalence and frequency of occurrence of different types of barriers to accessing information could not be estimated, and the “extent” aspect of the research aim could not be met.

The study also aimed to investigate the effects of barriers to online information seeking. It was successful in doing so to a certain degree, as described in 12.3 above under Objective 2 / RQ2.

The study aimed to identify “possible causal factors”. It was able to delineate technical factors in considerable detail, but its investigation of organisational factors was much less complete. In particular, the literature had indicated that issues of risk, risk management and attitudes to risk were likely to be of central importance. The study provisionally identified a wide range of possible

organisational factors relating to barriers to information seeking (12.2); an explanatory theoretical framework for some of these was proposed which involved the construct “attitude to risk” (11.1). However, risk as such was little discussed by participants, other than in relation to Web 2.0 and social media (11.3.5). It would have been desirable to explore further participants’ understandings of the relevant aspects of risk in relation to information seeking, use and sharing. However, it would have been impossible to access tacit or implicit understandings of risk without spending considerably more time in the field and undertaking an ethnographic study; implicit understandings are not readily accessible via texts, speech or discursive materials (Tracy, 2010)

12.4 Extent to which specific research objectives have been met

The following section discusses the extent to which the research objectives have been met and the corresponding research questions answered.

Objective 1: to establish in detail the nature and extent of barriers to accessing to published information online within the NHS in England, related to the functionality of information technology infrastructure or from aspects of policy and practice relating to the use of information technologies.

RQ1: What limitations currently exist on access to online published information to support professional development, clinical and management decision making, and research within NHS organisations arising from organisational strategies, policies and practices as they are implemented in relation to IT infrastructures and information technology use?

To address RQ1, a wide variety of types of barriers to accessing, storing and using published information were identified and described, as detailed within Chapters 5 to 9. The accounts varied in specificity and detail according to the backgrounds of the participants. The barriers included a variety of problems with PC hardware and software, problems with email content or attachments, problems with system policies and permissions, insufficient bandwidth on Trust networks, poor or non-existent wireless network coverage, inability to connect to 3G or 4G networks from smartphones being used within NHS premises, difficulty in obtaining the encrypted USB memory sticks mandated by NHS portable media policies, lack of continuity of funding for access to

mandatory e-learning, restrictive policies on the use of mobile devices, and blocking of websites and web applications, including Web 2.0 and social media applications.

Objective 2: to determine the effects that these barriers might have on professional information-seeking, learning and decision-making in the contexts of clinical and management practice, education and research, and the possible consequences for working practices, for working lives and for clinical and organisational effectiveness.

RQ2: What effects do these limitations (as cited in RQ1 above) have on professional information seeking, use and sharing, on the working practices and working lives of health professionals, on the education of students, and on clinical and organisational effectiveness?

For RQ2, general indications were provided by the participants who described them of the consequences and effects of technically-related restrictions on accessing, using and sharing published information for a variety of clinical, managerial and educational purposes (answering clinical questions, providing patient information, creating educational material, professional learning, and external relations). In some instances, particularly with the clinical educators, it was clear from the participants' accounts that these restrictions were encountered frequently and presented a considerable obstacle to their work. In one instance, the participant's work-life balance was being seriously affected through her resulting frequent need to undertake work at home (8.5.3). However, in many cases the main research method (semi-structured interviewing) did not prove to be as suitable as the researcher had hoped in generating detailed accounts of particular instances of such restrictions in their contexts, since participants were generally not able to recall events with the required degree of accuracy, and hence were unable also to provide precise accounts of their effects. The account of the problems in T3's community services with accessing e-learning, described in Section 6.2, was an exception; a detailed internal report had been written concerning these. While this was not made available to the researcher, she was provided with a succinct account of its contents via telephone by the senior IT analyst T3-17 who had participated in the preceding investigation. Identifying and analysing negative effects is notably difficult. In many cases, barriers to information seeking as described by participants are likely to have constituted a general "drag factor" on the work of the professionals involved, the effects of which are difficult to categorise or evaluate. A distinction should be made between contributory and direct effects; as Brettell, Maden, and Payne (2016) indicated, many factors may contribute to information behaviour, working practices, etc.

Objective 3: to investigate the norms, practices, attitudes, values, interests and presuppositions of the relevant staff groups regarding information seeking, business need and risk management which might be involved, and the influences they might be exerting on the phenomena identified in relation to Objective 1).

RQ3: What are the organisational issues within NHS Trusts (policy drivers, legal and regulatory requirements, organisational values, cultural attitudes and presuppositions, professional norms, and practices) which bear on a) how IT infrastructure enabling access to online published professional information, including e-learning content, is managed, and b) how acceptable use policies, social media policies and web content filtering are implemented? How do these issues interact?

For RQ3, three main theoretical areas were identified as being of relevance: interactions of power, culture, trust and risk in information security; diffusion of innovation in the use and regulation of Web 2.0 and social media; and the effects of inter-professional conflicts and competition. IT infrastructure relating to information provision and its management, relevant policy drivers, legal and regulatory requirements, and professional norms, with some of their interactions, were identified and described in detail. Under-resourcing of IT infrastructure and staffing, and security decisions consequent upon these, were also pinpointed as major contributory factors. Here the interview content yielded rich data relating to the context and background of health professionals' information behaviour. However it was not generally possible, using the adopted research methods, to elicit the basic assumptions identified by Schein (1996) as a constituent of organisational culture, which are generally tacit in nature and accessible via only via observations of processes and behaviour (*cf.* Section 2.7.2.4.1).

12.5 Limitations of the study

The three organisations included as nested sites of data collection within the study, although selected to represent the greatest possible variety of organisational forms, did not exemplify the full possible range of different types of NHS organisation; this would have prolonged the data collection excessively. Although all the Trusts included some community services, NHS community trusts as such, and specialist NHS acute trusts (covering services such as oncology, orthopaedics or thoracic medicine) were not included.

Recruitment of participants was dependent not only upon the identification of suitable potential participants by other parties (librarian, research office assistant) in some cases, but also upon the willingness of those contacted to participate in the study, hence the participants represented a group of willing volunteers. It is likely that the participants had had some prior interest in the subject of the study; hence bias may have been introduced into the participant sample, leading to a possible overstatement of the effects of barriers to accessing and using information. This may have been true particularly within T1, where the researcher experienced considerable difficulties in recruiting participants.

The participant sampling strategy had aimed to achieve as good a level of data saturation as possible in each Trust within the constraints of the limited time available for data collection (3.4). While the researcher felt that she had obtained a reasonably clear and consistent picture from her interviews at T1 and T3, the huge size of T4, and the organisational complexity of its specialist clinical services and research activities, made this far less achievable, and created a much greater degree of uncertainty regarding the generalisability of the findings across the organisation as a whole. In particular it would have been desirable to investigate further the apparent dysfunction identified in the relationship between T4's informatics and information governance services, and its apparently decentralised approach to social media policy, but there was no opportunity to do this.

The researcher's aim had been to recruit participants in similar roles across the three Trusts in accordance with her purposive sampling strategy. However, it did not prove possible to recruit across all participant staff categories for all the Trusts. As previously noted, the researcher was unable to recruit an interview participant within the outsourced IT provider S3. In T1 it proved impossible to recruit a radiography educator, in T3 the clinical psychologist whose name was put forward by the research manager was unwilling to participate, and in T4 no human resources manager was contactable. At T3 the education pharmacist did not respond to the researcher's email requesting an interview, so the drug information pharmacist was interviewed instead. In addition, in T4 an education facilities manager (as he proved to be), rather than a postgraduate medical educator or medical education manager, was put forward by the research office as the preferred participant. The possible full range of experiences may therefore not have been presented by participants within these categories. It was thereby also less possible to capture common patterns of data across the specialist areas they represented (Neergaard, 2006).

It was difficult in interviews with the IT managers to cover risk and security issues adequately in the time available as well as to gather from them the large amount of background information that was required about their Trust's IT infrastructure and services.

Participants' perceptions of the quality of their Trust's IT services were set out within a "home-grown" framework (Section 7.2.3). Transferability of the findings could perhaps have been improved through the use of a standard framework such as ServQual (Parasuraman, Zeithaml, and Berry, 1988, cited by van Velsen, Steehouder, & De Jong, 2007), which has been widely used in IT service quality research.

It should be noted that the researcher had no prior "intelligence" about barriers to information seeking and use in any of the Trusts, hence the findings that high levels of website blocking were occurring in T4, and that T3's community services had experienced a major problem with technical support of e-learning, were entirely fortuitous. The fact that blocking of websites was found to be common in only one Trust out of the four represented within the study indicates its sporadic nature; it also limits to some extent the transferability of the findings regarding website blocking.

It could be argued that the researcher's previous experience of working in the NHS as a library manager prevented her from taking a fully objective view of its structures and practices. However, her "insider" position provided in her view a highly advantageous background knowledge of the NHS as an organisation, of its information systems and services, and of the information needs of its health professionals, greatly enhancing her ability to establish effective rapport with interview subjects and to ask appropriate questions (*cf.* Silva & Backhouse, 2003). As her research progressed, she was able to reflect on her previous negative experiences, and to set them in the context of a deepening theoretical understanding of the relevant information behaviour, information security and organisational issues (*cf.* Section 3.9).

12.6 Contribution to new knowledge

Problems of access to and use of published information within the NHS for health professionals and managers, and the effects these could possibly have on the quality of care, had previously been highlighted informally by library and e-learning practitioners, but hitherto little studied (as discussed above in Sections 1.1, 1.2.1 and 2.7.3.4). The thesis presents the first detailed qualitative study of technical and organisational obstacles to professional information seeking, use and sharing to have

been undertaken within any part of the UK National Health Service. Previous investigations, while providing detailed accounts in some instances of problems caused by blocked websites, blocked web applications, including e-learning and social media resources, and other barriers to storing, using and sharing information, had been based either on survey data or on informal reports by information or e-learning professionals, and had focused largely on describing phenomena and their effects without studying the organisational background and context in which they were occurring or attempting to offer any analysis of possible causative factors. The explanatory model presented in Chapter 11, although it omits some aspects of the findings (Figure 11.1), is wide-ranging in scope, bringing together perspectives drawn from the fields of information behaviour, information security and cybersecurity, health service management studies, social theories of risk, diffusion of innovation theory, and the sociology of professions.

More specifically, the study has:

- Provided a detailed account of commonly occurring problems with PC hardware, PC software, system policies and permissions, and network infrastructures;
- Created a diagrammatic representation of the decision-making process of users faced with blocking of legitimate websites by web filters (11.3.2; Figure 11.3);
- Discussed this and the overall findings relating to blocking of websites in relation to the information horizon and satisficing concepts;
- Adapted in relation to these findings Inglesant and Sasse's analysis (2011a, 2011b), which was based upon Clegg's circuits of power theory and actor network theory, of the effects upon end-users of information security measures ;
- Offered a detailed account of operational difficulties encountered by training staff and users with the then-existing National Learning Management System for managing e-learning, including inherent deficiencies in its functionality and problems with its implementation in the contexts of the Trusts of the study;
- Identified the direct negative effects of barriers to information seeking and use upon both clinical and organisational effectiveness within the NHS via a process of mapping to the different facets of the clinical governance process (Figure 2.4);
- Adapted Greco *et al.*'s (2006) model (2.4.9, Figure 2.5) of the antecedents and consequences of empowerment and engagement to indicate a possible causal route through which levels of access to information, and to job resources, such as adequate computer infrastructure, could indirectly affect levels of staff engagement, and thereby organisational effectiveness

and performance, including clinical outcomes. This indirect effect is additional to the direct effect described above;

- Explored aspects of culture, behaviour and attitudes relating to the use of IT, in particular the mutually reinforcing effects of poor digital literacy and poor IT infrastructure provision (7.4.1);
- Applied Chretien and Kind's (2014) "hierarchy of needs" model of changing perceptions of risks and benefits of social media use among health professionals to explain the study findings relating to use and non-use of social media by clinicians and their perceptions of social media-related risk;
- Demonstrated the applicability to the study findings regarding levels and processes of social media adoption within the three Trusts of Kaganer and Vaast's analysis (Kaganer & Vaast, 2010; Vaast & Kaganer, 2013) of the process social media adoption by organisations based on social representations theory;
- Adapted Abbott's theory of professions (1988) and its application to the construction of professional identity in nursing in relation to information behaviour by Sundin and associates (Johannisson & Sundin, 2007; Sundin & Hedman, 1996) in putting forward an explanation of the study findings of contested jurisdiction between different health informatics professions within the NHS (1.4.7, 2.5.4, 11.5).
- Provided a detailed account of professional norms relating to the use of social media and mobile devices within the three Trusts;
- Investigated perceived IT department service quality in respect of IT support needs relating to information behaviour.

This section has set out the contribution to new knowledge made by the study. Areas for further research are discussed in the following section.

12.7 Recommendations for further research

The study has indicated a great many possibilities for further research, as follows.

The original TDAG survey (Technical Design Authority Group, 2009a, 2009b) was pivotal in establishing a warrant for the present research. It would be valuable as part of the Knowledge for Healthcare LIS strategy agenda (Health Education England, 2014) to conduct an updated version of the TDAG survey among NHS library managers in England to see what changes in barriers to information access, use and sharing have occurred since 2008, when it was first conducted. E-

learning, mobile devices and social media in particular are all rapidly changing areas, in terms both of resources and of policy; it is likely that significant changes in infrastructure, policy and practice would be shown to have taken place. It could also be valuable to conduct surveys of individual professional groups; this could be done via their associations with the appropriate permissions, and would not need NHS research governance approval. Design of the survey could be informed by the findings of the present study (Bunton, 2016).

In principle, the diary interview method (Bartlett, 2012; Zimmerman & Wieder, 1977) could be an effective way of obtaining from health professionals detailed accounts of the nature and context of obstacles they encounter to information seeking, use and sharing, and to elucidate their impact. It is, however, inherently difficult to evaluate negative impacts; *cf.* the work of Farnan *et al.* (2008) in attempting to assess the impact on patient care of clinical questions going unanswered. Also time pressure could militate against effective and comprehensive diary keeping. Since barriers to information access, use and sharing may be encountered only relatively infrequently by many NHS staff, the diary keeping would also need to take place over a relatively long period to capture enough material of interest, bringing possible attendant problems of continuity and participant motivation. Success with the data collection would be more likely with a brief, structured format for the recording of access problems. Prompts for participants' record keeping could be adapted from those commonly used in library impact studies, such as the NHS Library and Knowledge Services impact toolkit (Weightman & Urquhart, 2008). Alternatively, a "critical incident" (Flanagan, 1954; Urquhart *et al.*, 2003; *cf.* Payne, Maden-Jenkins, & Brettle, 2011) for assessing the impact of blocked websites could be used. However this would depend on recall rather than contemporaneous recording of data, and would hence be subject to the same problems as semi-structured interviews (12.2).

It was originally envisaged that the present study would include a log file analysis element; however, this was dropped for lack of time. Log file analysis, given the required anonymisation (so that web traffic monitoring and Internet activity could not be tracked to individual users), would provide insight into the accuracy of secure web gateway categorisations of websites and into staff web use, both work-related and non-work-related, in a manner which would not depend on user or system administrator reporting. Obtaining such log files would obviously be a sensitive matter, requiring the researcher to establish a high level of trust with the host organisation. Log file analysis been successfully used, however, by a number of researchers to investigate PWU at work, e.g. in conjunction with subject categorisation tools by Valli, (2004), Johnson and Ugray (2007) and Shepherd, Mejias and Klein (2014). It should be noted that both these groups of researchers

encountered the problem of whether to categorise particular instances of web use by an individual employee as legitimate or otherwise without knowing in any detail about the nature and context of the employee's work. It would be a much simpler matter, however, to establish whether or not a particular blocked website were potentially legitimate for information purposes. In particular, it would also be desirable to investigate the effects of accuracy of web filtering of configuration decisions to block advertising. It might be possible to use some form of case-control approach for this, using matched pairs of Trusts with the same SWG, where one Trust blocked advertising, the other did not.

Procurement and implementation processes for secure web gateways could be worth investigating via documentary analysis of tender documents and system documentation, and non-participant observation at relevant meetings, etc. The interest here would be in the process of drawing up the documents and in how different selection criteria are weighted within the selection process, also in how SWGs are implemented and decision made about their configuration.

The relative paucity of UK-based studies of Web 2.0 and social media use in health professions practice and education, including social media policies, was noted above (2.4.1). Aspects of social media use within NHS services, including types of use in relation to information behaviour / professional learning, provision of training, staff attitudes and individual social media usage, as well as NHS social media strategies and policies, would all be fruitful areas of study.

IT service quality and responsiveness to business need is an important determinant of organisational effectiveness in general; it also impinges upon culture of innovation and upon information behaviour. While digital maturity has been evaluated within NHS organisations (1.4.3), to the researcher's knowledge, there have been no studies conducted of IT services management, service quality, or service climate within health services (2.8.5). An investigation along these lines, possibly using the evaluation instrument devised by Jia and associates (Jia & Reich, 2011, 2013; Jia, Reich, & Pearson, 2008) would be of considerable interest.

It was noted above (2.7.3.2.2) that there is very limited evidence concerning the effectiveness of security education, training and awareness (SETA) in reducing unintentional information security / cybersecurity incidents. The publication of a revised version of the Information Governance Toolkit, planned for April 2018 ("IG Toolkit update from NHS Digital," 2017), and its attendant mandatory e-learning, could provide an ideal opportunity to undertake evaluations of pilot e-learning

programmes in terms of security awareness and reductions in numbers of incidents. Something similar could possibly be undertaken with digital literacy initiatives, such as the joint HEE/RCN programme *Every nurse an e-nurse* (Cumming & Davies, 2017); however, security is only one of the domains of digital literacy which it identifies, so the security-related content may be limited.

While it illustrated considerable variations in information governance structures and *modus operandi* in relation both to information security and other risk governance areas, the research was not able to establish any correlation between such arrangements and problems of access to published information, other than to suggest a possible association between high rates of blocking of websites and poor communication between IT and other services. This again could be an interesting area of study, particularly in relation to outsourced services.

12.8 Recommendations for practice

It is evident from the study findings (Chapter 5, *passim*) that improvements in all aspects of PC and network hardware and infrastructure within the NHS are needed to support information seeking and use. In particular it was clear that Wi-Fi coverage, which is required to support the use of mobile devices, was variable within all three Trusts in the study. General network bandwidth issues were identified in T1 and T3. Following Marcus Baw's surveys (Baw, 2013; Sachdeva, 2014), and a recommendation from Tim Kelsey, formerly the National Director for Patients and Information (Meek, 2015b), the need for improved Wi-Fi connectivity has been addressed at DH policy level ("Free wi-fi to be provided in all NHS buildings - Jeremy Hunt," 2015), and implementation has begun (Whitfield, 2016a)(*cf.* Section 1.4.3, above). It is to be hoped that other infrastructure issues can be addressed as part of the modernisation, paperless agenda (Moore-Colyer, 2016). It would also be highly desirable for the planned Health and Social Care Network (formerly named the Public Services Network for Health) (McBeth, 2016a; Meek, 2015a) to be able to provide higher bandwidth and better web connectivity and facilities than the existing N3 network, for which the national contract was due to expire in 2017.⁹⁹

A clear requirement emerged for access to approved secure individual cloud storage to facilitate information sharing (5.2.6). This would, in many cases, obviate the need to use encrypted portable media, with the attendant problems of obtaining them. A cloud storage facility is available within the

⁹⁹ N3/HSCN: <http://psnc.org.uk/contract-it/pharmacy-it/new-national-network-n3/>

new NHS secure email system, NHSmail 2, although only as an add-on service using Microsoft OneDrive for Business and Microsoft SharePoint 2013 rather than as part of the core suite of applications (Accenture & Health and Social Care Information Centre, 2015). It is unclear whether or to what extent this service permits sharing of files across organisational boundaries, the need for which emerged clearly (5.2.6).¹⁰⁰

The deficiencies identified in the NLMS provided by McKesson in 2008, which was in use at the time of the study (6.2, 6.3.4) were set to be addressed within the new Oracle Learning Management (OLM) being developed by IBM, which was also planned to provide much-needed new functionality: compatibility with mobile operating systems, support for web conferencing, integration with Web 2.0 and social media applications, and a range of local configuration options including links to local intranets (Bussey, 2015). The problems with HDAS were similarly intended to be addressed by the redevelopment initiated in 2015 and launched in October 2016 (Section 5.3).

It was apparent from the findings (8.5.5) that the NHS Library and Knowledge Services whitelist of essential websites was not being publicised effectively, either to librarians or to IT managers. It is clear that, for the whitelist to be an effective tool with which librarians can maximise access to published information for their end-users, efforts must be made to engage librarians with its maintenance and updating. It must be publicised more effectively to IT managers, and robust local systems put in place for IT departments to be notified of updates. This work could be co-ordinated with the assistance of local library service leads and electronic services officers, where these exist; NICE could also have a role in this. It would be desirable also for updating purposes to collect information about website unblocking requests received and implemented by Trust IT departments, though this might not be readily available.

Existing IT training within NHS Trusts may be limited in coverage and not always available when needed. To address digital literacy deficits, Trust IT departments should conduct digital literacy and cybersecurity training needs analyses among Trust staff and develop appropriate digital literacy training programmes, in line with Baroness Martha Lane Fox's recommendations of December 2015 (NHS England, 2015). This work could be informed by Health Education England's work on digital

¹⁰⁰ Transition to the new NHSmail 2 service began on May 6th 2016.

literacy.¹⁰¹ Digital literacy issues can most appropriately be addressed within information literacy training relating to web use, so there is a strong argument for combined training provision covering both information and digital literacy, devised and offered in conjunction with library and information services (*cf.* Willard, 2010, Ofsted, 2010).

The HSCIC practice guide on social media stated that problems are best addressed via user education rather than via technical controls (Health and Social Care Information Centre, 2012). NHS Trusts should provide training and guidance for all staff on the professional uses of common social media platforms such as Twitter, LinkedIn, YouTube and Facebook, and publish clear guidelines and recommendations for different types of corporate and professional use (health promotion, research dissemination, publicising events etc.) Library and information services could provide part of this training, either face-to-face or via e-learning, as part of user education in effective web searching. Training should inform staff about the major security and privacy issues specific to social media (described in Section 2.6 above).

Verma, Kavita, and Budhiraja (2012, p. 212) suggested as a general principle that the Hippocratic injunction *primum non nocere* ("First, do no harm"), should become the watchwords of information security staff; in other words, they should be at pains to avoid blocking the good when attempting to prevent the bad. Rather, they should, as far as possible, adopt context-aware security practices (Covington, 2015; Dimensional Research, 2015) which do not hinder employee productivity, focusing on providing the security protection that enables information to flow through the organisation (Harkins, 2013). Trust acceptable use policies should give clear examples of uses of information systems that are acceptable and which the Trust wishes to encourage (Gallagher, McMenemy, & Poulter, 2015).

In addition, to avoid possible negative impacts on organisational trust, it is important that responses to information security incidents, including disciplinary sanctions for misuse of Trust IT systems, are proportionate (Lippert, 2004). Trust IT and information governance departments should consult more widely than was commonly occurring at the time of the study with stakeholders in the development and revision of Internet acceptable use policies. They should communicate with

¹⁰¹ HEE Digital Literacy: <https://www.hee.nhs.uk/our-work/research-learning-innovation/technology-enhanced-learning/digital-literacy>

stakeholders concerning web filtering practices and policies, and they should monitor and evaluate their impacts, encourage the reporting of false positives as applicable, and institute processes for responding promptly (within hours if possible) to requests to unblock legitimate sites. Greater use could be made of the facilities available within SWGs to establish different policy levels for clinical and clinical support staff groups, if this were thought desirable (see above, Section 2.7.3.4.2). For maximum effectiveness, information security training and awareness (SETA) interventions should aim at aligning the information security / cybersecurity frames of reference of different staff groups (Sedlack & Tejay, 2011; cf. Vaast, 2007).

Library, education and training functions need to be more closely involved than at the time of this study in information technology business planning and strategy via appropriate consultative structures; this could help to raise the priority of IT service requirements in these areas. In particular, local policies need to be established by NHS Trusts for access by students on placement to networked resources and systems in line with their educational needs, and clear workflows and processes need to be established for this to be provided in a timely fashion.

Lack of IT support for the Macintosh platform by Trust IT services emerged as presenting a hindrance to development of e-learning in-house, and thereby possibly leading to additional cost being incurred through outsourcing (Section 6.2). Consideration should be given to establishing such support services, possibly at regional level, via outsourcing arrangements if necessary.

12.9 Conclusion

Professional information seeking, use and sharing online within the networks of NHS Trusts in England has been shown to be adversely affected in some organisations by restrictions relating to a wide variety of technical and organisational factors. These include aspects of leadership and culture, in particular organisational trust, attitude to risk, and culture of innovation; professional attitudes to IT and norms of behaviour; variations in cybersecurity practices; inter-professional conflicts; external policy drivers; and poor levels of resourcing for IT infrastructure and staffing. It is important that the problems underlying difficulties in accessing, using and sharing published information be addressed, both for the organisational effectiveness of NHS organisations in the future and for the quality of their clinical care.

References

- 'IT Slave'. (2011). Your Web Filtering Policy Agnostic or Nazi? Retrieved October 29, 2014, from http://community.spiceworks.com/topic/130090-your-web-filtering-policy-agnostic-or-nazi?source=content_fltr_guide
- #WeNurses. (2015). Are barriers to the use of technology in learning a real issue for healthcare professionals? Retrieved March 2, 2016, from <http://www.wecomunities.org/tweet-chats/chat-details/2578>
- Abbott, A. (1988). *The system of professions: an essay on the division of expert labor*. Chicago: Chicago, IL.
- Abbott, A. (1998). Professionalism and the future of librarianship. *Library Trends*, 46, 430–444. Retrieved from https://www.ideals.illinois.edu/bitstream/handle/2142/8161/librarytrendsv46i3c_opt.pdf?seq
- Abric, J.-C. (1993). Specific processes of social representations. *Papers on Social Representations*, 5(1), 77–80.
- Accenture, & Health and Social Care Information Centre. (2015). *NHSmail 2 executive summary: Introduction to NHSmail 2*.
- Ackroyd, S. (2004). Methodology for management and organisation studies: some implications of critical realism. In S. Fleetwood & S. Ackroyd (Eds.), *Critical realist applications in organisation and management studies* (pp. 137–163). London: Routledge.
- Adams, A., & Blandford, A. (2002a). Acceptability of medical digital libraries. *Health Informatics Journal*, 8(2), 58–66. <https://doi.org/10.1177/146045820200800202>
- Adams, A., & Blandford, A. (2002b). The unseen and unacceptable face of digital libraries. *International Journal on Digital Libraries*, 4(2), 71–81. <https://doi.org/10.1007/s00799-003-0071-7>
- Adams, A., & Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies*, 63(1–2), 175–202. <https://doi.org/10.1016/j.ijhcs.2005.04.022>
- Adams, A., Blandford, A., & Lunt, P. (2005). Social empowerment and exclusion: a case study on digital libraries. *ACM Transactions on Computer-Human Interaction*, 12(2), 174–200.
- Adams, A., & Blandford, A. (2001). Digital libraries in a clinical setting: friend or foe? *5th European Conference on Digital Libraries*, 2163, 213–224. Retrieved from http://dx.doi.org/10.1007/3-540-44796-2_19
- Adams, A., & Sasse, M. A. (1999). Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12), 41–46.

- Akbulut-Bailey, A., & Motwani, J. (2011). An investigation of students' stereotypes of IS professionals. In *Decision Sciences Institute Midwest DSI annual conference* (p. 167). Grand Rapids, MI. Retrieved from http://www.cis.gvsu.edu/mwdsi2012/2012_MWDSI_Proceedings.pdf#page=178
- Al-Amoudi, I., & Willmott, H. (2011). Where constructionism and critical realism converge: interrogating the domain of epistemological relativism. *Organization Studies*, 32(1), 27–46. <https://doi.org/10.1177/0170840610394293>
- Alaszewski, A., Alaszewski, H., & Potter, J. (2006, January 31). Risk, uncertainty and life threatening trauma: analysing stroke survivor's accounts of Life after stroke. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*. Retrieved from <http://www.qualitative-research.net/index.php/fqs/article/view/53/109>
- Alaszewski, A., & Horlick-Jones, T. (2002). *Risk and health: review of current research and identification of areas for further research*. Canterbury.
- Albrechtsen, E. (2007). A qualitative study of users' view [sic] on information security. *Computers and Security*, 26(4), 276–289. <https://doi.org/10.1016/j.cose.2006.11.004>
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29(4), 432–445. <https://doi.org/10.1016/j.cose.2009.12.005>
- Allen, D. K., & Wilson, T. D. (1998). Exploring the contexts of information behaviour : proceedings of the Second International Conference on Research in Information Needs, Seeking and Use in Different Contexts 13/15 August, 1998, Sheffield, UK. In D. K. (David K. Allen & T. D. Wilson (Eds.), *International Conference on Research in Information Needs: Seeking and Use in Different Contexts (2nd : 1998 : Sheffield, England)* (p. 625). London: Taylor Graham, c1999.
- Allen, M. (2008). Web 2.0: an argument against convergence. *First Monday*, 13(3). Retrieved from <http://firstmonday.org/ojs/index.php/fm/article/view/2139/1946>
- Allen, M., Currie, L. M., Graham, M., Bakken, S., Patel, V. L., & Cimino, J. J. (2003). The classification of clinicians' information needs while using a clinical information system. In *AMIA 2003 Symposium Proceedings* (pp. 26–30). <https://doi.org/D030003347> [pii]
- Allen, R. (2014). *The role of the social worker in adult mental health services*. s.l. Retrieved from http://www.tcsw.org.uk/uploadedFiles/TheCollege/Policy/MH_Launch_Document_April_2014.pdf
- Allen, V., & Brodzinski, E. (2009). Deconstructing the toolkit: creativity and risk in the NHS workforce. *Health Care Analysis : HCA : Journal of Health Philosophy and Policy*, 17(4), 309–17. <https://doi.org/10.1007/s10728-009-0134-z>
- Allsop, J. (2006). Medical dominance in a changing world: the UK case. *Health Sociology Review*, 15(5), 444–57. <https://doi.org/10.5172/hesr.2006.15.5.444>

- Althaus, C. E. (2005). A disciplinary perspective on the epistemological status of risk. *Risk Analysis an Official Publication of the Society for Risk Analysis*, 25(3), 567–588. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/16022691>
- Alvesson, M. (2003). Beyond neopositivists, romantics, and localists: a reflexive approach to interviews in organizational research. *Academy of Management Review*, 28(1), 13–33. <https://doi.org/10.5465/AMR.2003.8925191>
- Amedume, K. (2012). BYOD in the NHS: address the challenges and improve patient care. *British Journal of Healthcare Computing*. Retrieved from <http://www.bj-hc.co.uk/views/views-news-detail.html?news=2208&lang=en&feed=124>
- Anandarajan, M. (2002). Profiling web usage in the workplace : a behavior-based artificial intelligence approach. *Journal of Management Information Systems*, 19(July 2015), 243–266. <https://doi.org/10.1080/07421222.2002.11045711>
- Anandarajan, M., Paravastu, N., & Simmers, C. a. (2006). Perceptions of personal Web usage in the workplace: a Q-methodology approach. *CyberPsychology and Behavior*, 9(3), 325–35. <https://doi.org/10.1089/cpb.2006.9.325>
- Andersen, P. H., & Kragh, H. (2010). Sense and sensibility: Two approaches for using existing theory in theory-building qualitative research. *Industrial Marketing Management*, 39(1), 49–55. <https://doi.org/10.1016/j.indmarman.2009.02.008>
- Anderson, A. S., & Klemm, P. (2008). The Internet: friend or foe when providing patient education? *Clinical Journal of Oncology Nursing*, 12(1), 55–64.
- Anderson, B., & Speed, E. (2010). *Social media and health: implications for primary health care providers. Report to Solihull Care Trust*. Colchester.
- Andrade, A. D. (2009). Interpretive research aiming at theory building: adopting and adapting the case study design. *Qualitative Report*, 14(1), 42–60.
- Andrews, J. E., Pearce, K., Ireson, C., & Love, M. M. (2005). Information-seeking behaviors of practitioners in a primary care practice-based research network (PBRN). *Journal of the Medical Library Association*, 93(April), 206–12. Retrieved from <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1082937&tool=pmcentrez&rendertype=abstract>
- Andriole, S. J. (2015). Who owns IT? *Communications of the ACM*, 58(3), 50–57.
- Angus, J. E., & Clark, A. M. (2012). Using critical realism in nursing and health research: promise and challenges. *Nursing Inquiry*, 19(1), 1–3. <https://doi.org/10.1111/j.1440-1800.2011.00580.x>
- Apekey, T. A., McSorley, G., Tilling, M., & Siriwardena, A. N. (2011). Room for improvement? Leadership, innovation culture and uptake of quality improvement methods in general practice. *Journal of Evaluation in Clinical Practice*, 17(2), 311–318. <https://doi.org/10.1111/j.1365-2753.2010.01447.x>

- Archibald, M. M., & Clark, A. M. (2014). Editorial: Twitter and nursing research: how diffusion of innovation theory can help uptake. *Journal of Advanced Nursing*, 70(3), e3–e5.
<https://doi.org/10.1111/jan.12343>
- Arthur, C. (2010). Why the NHS can't get its browser act together. Retrieved May 30, 2013, from <http://www.guardian.co.uk/technology/2010/jan/22/internet-explorer-nhs-vulnerability>
- Arthur, S., Mitchell, M., Lewis, J., & McNaughton Nicholls, C. (2014). Designing fieldwork. In J. Ritchie, J. Lewis, C. McNaughton Nicholls, & R. Ormston (Eds.), *Qualitative research practice: a guide for social science students and researchers* (2nd ed., pp. 148–176). London: Sage.
- Ashenden, D. (2008). Information security management: a human challenge? *Information Security Technical Report*, 13(4), 195–201. <https://doi.org/10.1016/j.istr.2008.10.006>
- Associates, R. H. (2005). *Financing NHS libraries and information resources: final report*. Pontypridd. Retrieved from <https://www.dropbox.com/s/27egx26hxkagezf/FinancingNHSLibrariesFINALREPORT20thMay2005.doc?dl=0#>
- Atkinson, P., & Coffey, A. (2010). Analysing documentary realities. In D. Silverman (Ed.), *Qualitative research* (3rd ed., Vol. 2010, pp. 77–92). London: Sage.
- Austin, R. D., & Darby, C. A. (2003). The myth of secure computing. *Harvard Business Review*, 81(6), 120–6, 138. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/12800722>
- Ayatollahi, H., Bath, P. A., Goodacre, S., Lo, S. Y., Draegebo, M., & Khan, F. A. (2013). What factors influence emergency department staff attitudes towards using information technology? *Emergency Medicine Journal*, 30(4), 303. <https://doi.org/10.1136/emered-2011-200446>
- Ayre, L. B. (2004a). History and development of filters. *Library Technology Reports*, 40(2), 8–25.
- Ayre, L. B. (2004b). Selecting a filter. *Library Technology Reports*, 40(2), 26–48.
- Azzurri Communications. (2013). An award winning case study: UCLH's BYOD development. Azzurri.
- Bada, M., & Sasse, A. (2014). *Cyber security awareness campaigns: why do they fail to change behaviour?* Oxford.
- Banday, M. T., & Shah, N. A. (2010). *A concise study of web filtering* (Sprouts: working papers on information systems No. 10(31)). *Sprouts: Working Papers on Information Systems* (Vol. 10). Retrieved from <http://sprouts.aisnet.org/10-31>
- Bandey, B. (2011a). *A perspective of the legal exposure that arises for companies when employees misuse the workplace Internet and e-mail systems (UK law)*. Leeds.
- Bandey, B. (2011b). Legal exposure and the corporation (UK law). Retrieved July 5, 2013, from [http://www.smoothwall.net/whitepaper-library/legal-exposure-and-the-corporation-\(uk-law\)/](http://www.smoothwall.net/whitepaper-library/legal-exposure-and-the-corporation-(uk-law)/)

- Barnett, S., Jones, S. C., Bennett, S., Iverson, D., & Bonney, A. (2013). Perceptions of family physician trainees and trainers regarding the usefulness of a virtual community of practice. *Journal of Medical Internet Research*, 15(5), e92. doi:10.2196/jm. *Journal of Medical Internet Research*, 15(5), e92. <https://doi.org/10.2196/jmir.2555>
- Bartlett, R. (2012). Modifying the diary interview method to research the lives of people with dementia. *Qualitative Health Research*, 22(12), 1717–1726. <https://doi.org/10.1177/1049732312462240>
- Baskaran, V., Davis, K., Bali, R. K., Naguib, R. N., & Wickramasinghe, N. (2013). Managing information and knowledge within maternity services: privacy and consent issues. *Informatics for Health and Social Care*, 38(3), 196–210. Retrieved from <http://www.researchgate.net>
- Baskerville, R. L. (1991). Risk analysis as a source of professional knowledge. *Computers & Security*, 10(8), 749–764. [https://doi.org/10.1016/0167-4048\(91\)90094-T](https://doi.org/10.1016/0167-4048(91)90094-T)
- Bath, P. A. (2008). Health informatics: current issues and challenges. *Journal of Information Science*, 34(4), 501–518. <https://doi.org/10.1177/0165551508092267>
- Baw, M. (2013). May 2013 – National NHS WiFi survey. Retrieved September 28, 2015, from <http://www.bawmedical.co.uk/2013/05/02/may-2013-national-nhs-wifi-survey/>
- Baxter, G. J., & Rudman, R. J. (2010). Incremental risks in Web 2.0 applications. *The Electronic Library*, 28(2), 210–230. Retrieved from <http://dx.doi.org/10.1108/02640471011033585>
- Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, 13(4), 544–559.
- Bazeley, P. (1999). The bricoleur with a computer: piecing together qualitative and quantitative data. *Qualitative Health Research*, 9(2), 279–287.
- Bazeley, P. (2013). *Qualitative data analysis: practical strategies*. London: Sage.
- BCS ASSIST. (2012). *BCS ASSIST's response to the Information Governance Review: a response from informatics professionals and information governance specialists*. Swindon.
- Beagle, D. (1999). Conceptualizing an information commons. *Journal of Academic Librarianship*, 25(2), 82–89. [https://doi.org/10.1016/S0099-1333\(99\)80003-2](https://doi.org/10.1016/S0099-1333(99)80003-2)
- Beaumont, A. (2005). Implementation of e-learning and the teaching hospital: a local perspective. *Health Information and Libraries Journal*, 22(supplement 2), 66–88. [https://doi.org/10.1002/\(SICI\)1097-0177\(199909\)216:1<1::AID-DVDY1>3.0.CO;2-T](https://doi.org/10.1002/(SICI)1097-0177(199909)216:1<1::AID-DVDY1>3.0.CO;2-T)
- Beautement, A., & Sasse, M. A. (2009). The compliance budget: the economics of user effort in information security. In *Proceedings of the 2008 workshop on new security paradigms* (pp. 47–58). ACM. <https://doi.org/10.1145/1595676.1595684>
- Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. *Security*, (335), 47–58. Retrieved from <http://discovery.ucl.ac.uk/1301853/>

- Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: Sage. Retrieved from <http://www.amazon.co.uk/Risk-Society-Modernity-Published-association/dp/0803983468>
- Beddoe, L. (2010). Investing in the future: social workers talk about research. *British Journal of Social Work, 41*(3), 557–575. <https://doi.org/10.1093/bjsw/bcq138>
- Beke-Harrigan, H., Hess, R., & Weinland, J. A. (2008). A survey of registered nurses' readiness for evidence-based practice: a multidisciplinary project. *Journal of Hospital Librarianship, 8*(4), 440–448.
- Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly, 11*(3), 369–386.
- Bennett, N. L., Casebeer, L., Zheng, S., & Kristofco, R. (2006). Information-seeking behaviors and reflective practice. *Journal of Continuing Education in the Health Professions, 26*(2), 120–127. <https://doi.org/10.1002/chp>
- Benton, T., & Craib, I. (2011). *Philosophy of social science: the philosophical foundations of social thought* (2nd ed.). Basingstoke: Palgrave Macmillan. Retrieved from <http://www.loc.gov/catdir/toc/hol051/2001027372.html>
- Berke, D. M., Rozell, C., Hogan, T. P., Norcross, J. C., & Karpiak, C. P. (2011). What clinical psychologists know about evidence-based practice: familiarity with online resources and research methods. *Journal of Clinical Psychology, 67*(4), 329–39. <https://doi.org/10.1002/jclp.20775>
- Bertino, E., Ferrari, E., & Perego, A. (2006). Web content filtering. In E. Ferrari & B. Thuraisingham (Eds.), *Web and information security* (pp. 112–132). Hershey, PA: IRM Press.
- Bertulis, R. (2008). Barriers to accessing evidence-based information. *Nursing Standard, 22*(36), 35–39.
- Bertulis, R., & Cheeseborough, J. (2008). The Royal College of Nursing's information needs survey of nurses and health professionals. *Health Information and Libraries Journal, 25*(3), 186–197. <https://doi.org/10.1111/j.1471-1842.2007.00755.x>
- Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security, 23*(3), 253–264. <https://doi.org/10.1016/j.cose.2003.09.002>
- Betts, B. (2016). Shadow data and the risks posed by cloud storage and apps. Retrieved January 13, 2017, from <http://www.computerweekly.com/news/450298345/Shadow-data-and-the-risks-posed-by-cloud-storage-and-apps>
- Beverley, C. A., Booth, A., & Bath, P. A. (2003). The role of the information specialist in the systematic review process: a health information case study. *Health Information and Libraries Journal, 20*(2), 65–74. <https://doi.org/10.1046/j.1471-1842.2003.00411.x>
- Bhaskar, R. (1978). *A realist theory of science*. Hassocks: Harvester Press, 1978.
- Bhaskar, R. (1998). *The possibility of naturalism: a philosophical critique of the contemporary human sciences*. (R. Bhaskar, Ed.) (3rd ed.). Abingdon: Routledge.

- Bilham, T. I. M. (2009). e-Learning in medical education: Guide supplement 32.5 – Viewpoint 1. *Medical Teacher*, 31, 449–451. <https://doi.org/10.1080/01421590902835049>
- Bingham, H., & Wright, A. (2008). Strategy for e-learning and libraries 2008-2010. Winchester: NHS Education South Central.
- Black, C. (2012). Why healthcare organisations must look after their staff. *Nursing Management*, 19(6), 27–30. Retrieved from <http://journals.rcni.com/doi/abs/10.7748/nm2012.10.19.6.27.c9319>
- Blackwelder, M. B. (1996). The image of health sciences librarians: how we see ourselves and how patrons see us. *Bulletin of the Medical Library Association*, 84(3), 345–50. Retrieved from <http://www.pubmedcentral.nih.gov>
- Blaikie, N. W. H. (2009). *Designing social research: the logic of anticipation* (2nd ed.). Cambridge: Polity Press.
- Blair, J. (2006). The use of the internet by learning disability nurses in their practice. *Tizard Learning Disability Review*, 11(2), 35–44.
- Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*, 24(3), 1067–1084. <https://doi.org/10.1016/j.chb.2007.03.008>
- Blenkinsopp, J. (2008a). Bookmarks: web blocking – giving Big Brother a run for his money. *He@lth Information on the Internet*, (62), 10–11.
- Blenkinsopp, J. (2008b). Re: NHS - blocking web sites. Retrieved August 12, 2013, from <http://www.jiscmail.ac.uk/lists/lis-medical>
- Bloomfield, B. P., & Danieli, A. (1995). The role of management-consultants in the development of information technology - the indissoluble nature of sociopolitical and technical skills. *Journal of Management Studies*, 32(1), 23–46. <https://doi.org/10.1111/j.1467-6486.1995.tb00644.x>
- Blue Coat Systems. (2015). *Do not enter: Blue Coat research maps the web's shadiest neighborhoods*. Sunnyvale, CA. Retrieved from <https://www.bluecoat.com/>
- Bodhani, A. (2012). E-health: keep taking the tablets? *Engineering & Technology*, 7(11), 82–85. <https://doi.org/10.1049/et.2012.1120>
- Boeije, H. (2010). *Analysis in qualitative research*. London: Sage.
- Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing and Management*, 48(6), 1031–1052. <https://doi.org/10.1016/j.ipm.2012.01.001>
- Bond, C. S. (2009). Nurses, computers and pre-registration education. *Nurse Education Today*, 29(7), 731–4. <https://doi.org/10.1016/j.nedt.2009.02.014>

- Bonis, P. A., Pickens, G. T., Rind, D. M., & Foster, D. A. (2008). Association of a clinical knowledge support system with improved patient safety, reduced complications and shorter length of stay among Medicare beneficiaries in acute care hospitals in the United States. *International Journal of Medical Informatics*, 77(11), 745–753. <https://doi.org/10.1016/j.ijmedinf.2008.04.002>
- Booth, A. (2005). The body in questions. *Health Information and Libraries Journal*, 22, 150–155.
- Booth, A., Levy, P., Bath, P. A., Lacey, T., Sanderson, M., & Diercks-O'Brien, G. (2005). Studying health information from a distance: refining an e-learning case study in the crucible of student evaluation. *Health Information and Libraries Journal*, 22 Suppl 2, 8–19. <https://doi.org/10.1111/j.1470-3327.2005.00610.x>
- Botta, D., Muldner, K., Hawkey, K., & Beznosov, K. (2010). Toward understanding distributed cognition in IT security management: the role of cues and norms. *Cognition, Technology & Work*, 13(2), 121–134. <https://doi.org/10.1007/s10111-010-0159-y>
- Botta, D., Werlinger, R., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). Studying IT security professionals: research design and lessons learned. In *Workshop on security user studies: methodologies and best practices*. San Jose, CA.
- Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). Towards understanding IT security professionals and their tools. In *Proceedings of the 3rd symposium on Usable privacy and security - SOUPS '07* (pp. 1–12). Pittsburgh, PA: ACM Press. <https://doi.org/10.1145/1280680.1280693>
- Boudreau, M. C., Serrano, C., & Larson, K. (2014). IT-driven identity work: creating a group identity in a digital environment. *Information and Organization*, 24(1), 1–24. <https://doi.org/10.1016/j.infoandorg.2013.11.001>
- Boulos, K. M. N., & Wheeler, S. (2007). The emerging Web 2.0 social software: an enabling suite of sociable technologies in health and health care education. *Health Information and Libraries Journal*, 24(1), 2–23. <https://doi.org/10.1111/j.1471-1842.2007.00701.x>
- Bourke, B. (2014). Positionality: reflecting on the research process. *The Qualitative Report*, 19(33), 1–9. Retrieved from <http://nsuworks.nova.edu/tqr/vol19/iss33/3>
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Box, D., & Pottas, D. (2014). A model for information security compliant behaviour in the healthcare context. *Procedia Technology*, 16, 1462–1470. <https://doi.org/10.1016/j.protcy.2014.10.166>
- Bozeman, B., & Kingsley, G. (1998). Risk culture in public and private organizations. *Public Administration Review*, 58(2), 109–118. Retrieved from <http://www.researchgate.net>
- Bradbury, D. (2010). Avoiding URL hell. *Network Security*, 2010(11), 4–6. [https://doi.org/10.1016/S1353-4858\(10\)70133-1](https://doi.org/10.1016/S1353-4858(10)70133-1)

- Brady, R., Chitnis, S., Stewart, R. W., Graham, C., Yalamarathi, S., & Morris, K. (2012). NHS connecting for health: healthcare professionals, mobile technology, and infection control. *Telemedicine Journal and E-Health : The Official Journal of the American Telemedicine Association*, 18(4), 289–91. <https://doi.org/10.1089/tmj.2011.0147>
- Brady, R. R. W., Verran, J., Damani, N. N., & Gibb, A. P. (2009). Review of mobile communication devices as potential reservoirs of nosocomial pathogens. *The Journal of Hospital Infection*, 71(4), 295–300. <https://doi.org/10.1016/j.jhin.2008.12.009>
- Brailsford, S. C., Bolt, T. B., Bucci, G., Chausalet, T. J., Connell, N. a. D., Harper, P. R., ... Taylor, M. (2013). Overcoming the barriers: a qualitative study of simulation adoption in the NHS. *Journal of the Operational Research Society*, 64(2), 157–168. <https://doi.org/10.1057/jors.2011.130>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Breakwell, G. M., Hammond, S., Fife-Schaw, C., & Smith, J. A. (Eds.). (2006). *Research methods in psychology* (3rd ed.). London: Sage. Retrieved from <http://www.loc.gov/catdir/enhancements/fy0659/2005935774-t.html>
- Brennan, N., Edwards, S., Kelly, N., Miller, A., Harrower, L., & Mattick, K. (2014). Qualified doctor and medical students' use of resources for accessing information: what is used and why? *Health Information and Libraries Journal*, 31(3), 204–14. <https://doi.org/10.1111/hir.12072>
- Brette, A., Hulme, C., & Ormandy, P. (2007). Effectiveness of information skills training and mediated searching: qualitative results from the EMPIRIC project. *Health Information and Libraries Journal*, 24(1), 24–33.
- Brette, A., Maden, M., & Payne, C. (2016). The impact of clinical librarian services on patients and health care organisations. *Health Information and Libraries Journal*, 100–120. <https://doi.org/10.1111/hir.12136>
- Brette, A., & Urquhart, C. (Eds.). (2012). *Changing roles and contexts for health library and information professionals*. London: London : Facet, 2012.
- Brice, A. (2003). Building knowledge communities in the National electronic Library for Health. *Health Information on the Internet*, (34), 9–10.
- Bristol, T. J. (2013). Tablets in nursing education. *Teaching and Learning in Nursing*, 8(4), 164–167. <https://doi.org/10.1016/j.teln.2013.07.007>
- British Association of Social Workers. (2012). BASW social media policy. Birmingham: British Association of Social Workers. Retrieved from http://cdn.basw.co.uk/upload/basw_34634-1.pdf
- British Medical Association. (2011). Using social media: practical and ethical guidance for doctors and medical students. London: British Medical Association. Retrieved from <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Using+social+media+:+practical+and+ethical+guidance+for+doctors+and+medical+students#0>

- British Psychological Society. (2012). Supplementary guidance on the use of social media. Leicester: British Psychological Society. Retrieved from http://www.bps.org.uk/system/files/images/2012_ethics_committee_social_media.pdf
- British Telecommunications. (2012). N3 overview. Retrieved April 6, 2015, from <http://www.n3.nhs.uk/TechnicalInformation/N3NetworkOverview.cfm>
- Broucek, V., Turner, P., & Zimmerli, M. (2010). Managing university internet access: balancing the need for security, privacy and digital evidence. *Journal in Computer Virology*, 7(3), 189–199. <https://doi.org/10.1007/s11416-010-0147-z>
- Brown, G. T., & McMenemy, D. (2013). The implementation of internet filtering in Scottish public libraries. *Aslib Proceedings*, 65(2), 182–202. <https://doi.org/10.1108/00012531311313998>
- Brown, J. S., & Duguid, P. (2001). Knowledge and organization: a social-practice perspective. *Organization Science*, 12(2), 198–213. <https://doi.org/10.1287/orsc.12.2.198.10116>
- Brown, L., & Osborne, S. P. (2013). Risk and innovation. *Public Management Review*, 15(2), 186–208. <https://doi.org/10.1080/14719037.2012.707681>
- Brown, P. R. (2008). Trusting in the new NHS: instrumental versus communicative action. *Sociology of Health and Illness*, 30(3), 349–363. <https://doi.org/10.1111/j.1467-9566.2007.01065.x>
- Brown, P. R., Alaszewski, A., Pilgrim, D., & Calnan, M. (2011). The quality of interaction between managers and clinicians: a question of trust. *Public Money & Management*, 31(1), 43–50. <https://doi.org/10.1080/09540962.2011.545546>
- Brusco, J. M. (2011). Tablet and e-reader technology in health care and education. *AORN Journal*, 93(6), 775–781.
- Bruton, N. (2002). *How to manage the IT helpdesk: a guide for user support and call centre managers* (2nd ed.). Oxford: Butterworth-Heinemann.
- Bryman, A. (2008). *Social research methods* (4th ed.). Oxford: Oxford University Press.
- Bryman, A. (2011). Conducting mixed methods research. Retrieved from <http://vimeo.com/21253052>
- Budd, J. M., Hill, H., & Shannon, B. (2013). Inquiring into the real: a realist phenomenological approach. *Library Quarterly*, 80(3), 267–284. <https://doi.org/http://www.jstor.org/stable/10.1086/652876>
- Burke, H. (2011). Using an external agency or individual to transcribe your qualitative data. Manchester: ESRC National Centre for Research Methods.
- Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, 57, 24–27. <https://doi.org/10.1145/2556936>
- Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organizational analysis*. London: Heinemann.

- Byrne, A. (2005). IFLA position on Internet governance. Retrieved April 2, 2014, from <http://www.ifla.org/publications/ifla-position-on-internet-governance>
- Byrne, Z. S., Dvorak, K. J., Peters, J. M., Ray, I., Howe, A., & Sanchez, D. (2016). From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. *Computers in Human Behavior*, 59, 456–468. <https://doi.org/10.1016/j.chb.2016.02.024>
- Cabinet Office. (2011a). *ITIL continual service improvement* (2011 ed.). London: TSO.
- Cabinet Office. (2011b). *ITIL service design* (2011 ed.). London: TSO.
- Cabinet Office. (2011c). *ITIL service operation* (2011 ed.). London: TSO.
- Cabinet Office. (2011d). *ITIL service strategy* (2011 ed.). London: TSO.
- Cabinet Office. (2011e). *ITIL service transition* (2011 ed.). London: TSO.
- Cahill, K., & Chalut, R. (2009). Optimal results: what libraries need to know about Google and search engine optimization. *The Reference Librarian*, 50(3), 234–247. <https://doi.org/10.1080/02763870902961969>
- Cain, J. (2011). Social media in health care: the case for organizational policy and employee education. *American Journal of Health-System Pharmacy : AJHP : Official Journal of the American Society of Health-System Pharmacists*, 68(11), 1036–40. <https://doi.org/10.2146/ajhp100589>
- Calder, A. (2013). *Risk assessment and ISO 27001*. Ely: Vigilant Software.
- Caldicott, F. (1997). *Report on the review of patient-identifiable information*. London. Retrieved from http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf
- Caldicott, F. (2013). *Information: to share or not to share? The information governance review*. London. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
- Callaghan, L., Doherty, A., Lea, S. J., & Webster, D. (2008). Understanding the information and resource needs of UK health and social care placement students. *Health Information and Libraries Journal*, 25(4), 253–60. <https://doi.org/10.1111/j.1471-1842.2008.00769.x>
- Campion-Awwad, O., Hayton, A., Smith, L., & Vuaran, M. (2014). *The national programme for IT in the NHS: A case history*. University of Cambridge. Retrieved from <https://www.cl.cam.ac.uk/~rja14/Papers/nffit-mpp-2014-case-history.pdf>
- Canaan Messarra, L., Karkouljian, S., & McCarthy, R. (2011). To restrict or not to restrict personal internet usage on the job. *Education, Business and Society: Contemporary Middle Eastern Issues*, 4(4), 253–266. <https://doi.org/10.1108/17537981111190042>

- Canadian Health Services Research Foundation. (2000). Health services research and evidence-based decision-making. Ottawa: Canadian Health Services Research Foundation= *Fondation canadienne de la recherche sur les services de santé*.
- Can I use... support tables for HTML5, CSS3, etc. (s.d.). Retrieved December 9, 2014, from <http://caniuse.com/>
- Canali, D., Bilge, L., & Balzarotti, D. (2014). On the effectiveness of risk prediction based on users [sic] browsing behavior. *ACM Symposium on Information, Computer and Communications Security*, 171–182. <https://doi.org/10.1145/2590296.2590347>
- Care Quality Commission. (2016). *Safe data, safe care*. London. Retrieved from http://www.cqc.org.uk/sites/default/files/20160701_Data_security_review_FINAL_for_web.pdf
- Carlinet, Y., Mé, L., Debar, H., & Gourhant, Y. (2008). Analysis of computer infection risk factors based on customer network usage. *Proceedings - 2nd Int. Conf. Emerging Security Inf., Systems and Technologies, SECURWARE 2008, Includes DEPEND 2008: 1st Int. Workshop on Dependability and Security in Complex and Critical Inf. Sys.*, 317–325. <https://doi.org/10.1109/SECURWARE.2008.30>
- Carlisle, D. (2015). Clear and present danger. Retrieved December 9, 2015, from <http://www.digitalhealth.net/includes/features/2015/SR/cybersecurity/cyberfeature-page/cyberfeaturepage.html>
- Carlsson, S. A. (2003). Critical realism: a way forward in IS research. In *ECIS 2003 Proceedings* (pp. 348–362).
- Carney, P. A., Poor, D. A., Schifferdecker, K. E., Gephart, D. S., Brooks, W. B., & Nierenberg, D. W. (2004). Computer use among community-based primary care physician preceptors. *Academic Medicine*, 79(6), 580–590. Retrieved from http://journals.lww.com/academicmedicine/Fulltext/2004/06000/Computer_Use_among_Community_Based_Primary_Care.17.aspx
- Carrion, M., Woods, P., & Norman, I. (2004). Barriers to research utilisation among forensic mental health nurses. *International Journal of Nursing Studies*, 41(6), 613–9. <https://doi.org/10.1016/j.ijnurstu.2004.01.006>
- Casebourne, I. (2012). *Research report: mobile learning for the NHS*. Brighton: Epic.
- Cater-Steel, A. (2009). IT service departments struggle to adopt a service-oriented philosophy. *International Journal of Information Systems in the Service Sector*, 1(2), 69–77. <https://doi.org/10.4018/jjiss.2009040105>
- Cater-Steel, A. (2010). IT service personnel: changing the focus from technology to service. In J. Wang (Ed.), *Information systems and new applications in the service sector: models and methods* (Vol. 30, pp. 183–193). Hershey, PA: IGI Global.
- Cattermole, G., Johnson, J., & Roberts, K. (2013). Employee engagement welcomes the dawn of an empowerment culture. *Strategic HR Review*, 12(5), 250–254. <https://doi.org/10.1108/SHR-04-2013-0039>

- Cavaye, A. L. M. (1996). Case study research: a multi-faceted approach for IS. *Information Systems Journal*, 6, 227–242.
- Cavendish, C. (2013). *The Cavendish review: an independent review into healthcare assistants and support workers in the NHS and social care settings*. s.l. Retrieved from <http://rcnpublishing.com/doi/pdfplus/10.7748/ns2013.08.27.51.67.s57>
- Cecez-Kecmanovic, D. (2001). Doing critical IS research: the question of methodology. In E. M. Trauth (Ed.), *Qualitative research in information systems: issues and trends* (pp. 142–163). Hershey, PA: Idea Group Publishing.
- Cecez-Kecmanovic, D. (2005). Basic assumptions of the critical perspectives in information systems. In D. Howcroft & E. M. Trauth (Eds.), *Handbook of critical information systems research: theory and application* (pp. 19–46). Cheltenham: Edward Elgar.
- Cecez-Kecmanovic, D. (2011). On methods, methodologies and how they matter. In *ECIS 2011 Proceedings*.
- Cecez-Kecmanovic, D., & Kennan, M. A. (2013). The methodological landscape: information systems and knowledge management. In K. Williamson & G. Johanson (Eds.), *Research methods: information, systems and contexts: techniques and questions* (pp. 113–137). Prahran, Victoria: Tilde University Press.
- Cecez-Kecmanovic, D., Klein, H. K., & Brooke, C. (2008). Exploring the critical agenda in information systems research. *Information Systems Journal*, 18(2), 123–135. <https://doi.org/10.1111/j.1365-2575.2008.00295.x>
- Ceeney, N. (2009). Information management -- headache or opportunity?: The challenges that the recent focus on information management is presenting to senior leaders in the public sector. *Public Policy and Administration*, 24(339), 339–347. <https://doi.org/10.1177/0952076709103815>
- Chamberlain, D., Elcock, M., & Puligari, P. (2015). The use of mobile technology in health libraries: A summary of a UK-based survey. *Health Information and Libraries Journal*, 32(4), 265–275. <https://doi.org/10.1111/hir.12116>
- Chase, N. (2008). An exploration of the culture of information technology: focus on unrelenting change. *Journal of Information, Information Technology and Organizations*, 3, 135–150.
- Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal*, 14, 197–235.
- Chi, M. (2011). *Security policy and social media use*.
- Chickowski, E. (2013, August). 10 web-based attacks targeting your end-users. *Dark Reading*, 3–12. Retrieved from http://twimsgs.com/darkreading/drdigital/080713s/DarkReading_SUP_2013_08.pdf

- Childs, S., Blenkinsopp, E., Hall, A., & Walton, G. (2005). Effective e-learning for health professionals and students--barriers and their solutions. A systematic review of the literature--findings from the HeXL project. *Health Information and Libraries Journal*, 22(supplement 2), 20–32.
<https://doi.org/10.1111/j.1470-3327.2005.00614.x>
- Cho, J., Laschinger, H. K. S., & Wong, C. (2006). Workplace empowerment, work engagement and organizational commitment of new graduate nurses. *Nursing Leadership*, 19(3), 43–60.
<https://doi.org/10.12927/cjnl.2006.18368>
- Chretien, K., & Kind, T. (2014). Climbing social media in medicine's hierarchy of needs. *Academic Medicine*, 89(10), 1318–1320.
- Chua, W. F. (1986). Radical developments in accounting thought. *Accounting Review*, 61(4), 601–632.
- CILIP. (s.d.). Professional knowledge and skills base. Retrieved September 8, 2015, from
<http://www.cilip.org.uk/sites/default/files/Professional Knowledge and Skills Base.pdf>
- CILIP. (2004). Code of professional practice for library and information professionals. London: CILIP.
- CILIP. (2005). Intellectual freedom, access to information and censorship. London: CILIP. Retrieved from
<http://www.cilip.org.uk/cilip/archived-policy-statements/statement-intellectual-freedom-access-information-and-censorship>
- Clarke, A. E. (2003). Situational analyses: grounded theory mapping after the postmodern turn. *Symbolic Interaction*, 26(4), 553–576.
- Clarke, E. J. (2009). Introduction of e-learning into the pre-registration midwifery curriculum. *British Journal of Midwifery*, 17(7), 432–437.
- Clarke, N. (2006). Why HR policies fail to support workplace learning: the complexities of policy implementation in healthcare. *The International Journal of Human Resource Management*, 17(1), 190–206. <https://doi.org/10.1080/09585190500367589>
- Clarke, S. (2005). Informed consent and electronic monitoring in the workplace. In J. Weckert (Ed.), *Electronic monitoring in the workplace: controversies and solutions* (pp. 227–259). Hershey, PA: Idea Group Publishing.
- Clatworthy, M., Mellett, H., & Peel, M. (2000). Corporate governance under “new public management”: an exemplification. *Corporate Governance*, 8(2), 166–176.
<https://doi.org/10.1111/1467-8683.00193>
- Clegg, S. (1989). *Frameworks of power*. Beverly Hills : Sage.
- Clinch, J. (2009). *ITIL v3 and information security*. Clinch Consulting White Paper. Retrieved from
http://www.apmg-library.org/Player/eKnowledge/itil_v_and_information_security.pdf
- Coffey, A. (2014). Analysing documents. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 367–380). London: Sage. <https://doi.org/10.4135/9781446282243>
- Cofta, P. (2007). *Trust, complexity and control: confidence in a convergent world*. Chichester: Wiley. Retrieved from <https://books.google.com/books?id=xRLqGKY8axwC&pgis=1>

- Cogdill, K. W. (2003). Information needs and information seeking in primary care: a study of nurse practitioners. *Journal of the Medical Library Association*, 91(2), 203–15.
[https://doi.org/10.1043/0025-7338\(2003\)091<0203:INAISI>2.0.CO;2](https://doi.org/10.1043/0025-7338(2003)091<0203:INAISI>2.0.CO;2)
- Cole, E. (2010). *Enabling social networking applications for enterprise usage*. Sunnyvale, CA: Palo Alto Networks.
- Cooke, L. (2006). Do we want a perfectly filtered world? *Library Student Journal*.
- Corden, A., & Sainsbury, R. (2006). *Using verbatim quotations in reporting qualitative social research: researchers' views*. York. Retrieved from
<http://www.york.ac.uk/inst/spru/pubs/pdf/verbquotresearch.pdf>
- Cova, M., Kruegel, C., & Vigna, G. (2010). Detection and analysis of drive-by-download attacks and malicious JavaScript code. *Proceedings of the 19th International Conference on World Wide Web - WWW '10*, 281. <https://doi.org/10.1145/1772690.1772720>
- Covington, R. C. (2015, September). Information security and employee productivity in conflict: How to achieve a security operation without weighing down your employees. *Computerworld*. Retrieved from <http://www.computerworld.com/article/2984123/security/information-security-and-employee-productivity-in-conflict.html>
- Cox, J. (2014, August). To tweet or not to tweet in the workplace? *The HR Director*. Retrieved from <https://www.hrdirector.com>
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, (October). Retrieved from <https://timreview.ca/article/835>
- Cranfield, S., Hendy, J., Reeves, B., Hutchings, A., Collin, S., & Fulop, N. (2015). Investigating healthcare IT innovations: a “conceptual blending” approach. *Journal of Health Organization and Management*, 29(7), 1131–1148. <https://doi.org/10.1108/JFM-03-2013-0017>
- Crawford, E. R., LePine, J. A., & Rich, B. L. (2010). Linking job demands and resources to employee engagement and burnout: a theoretical extension and meta-analytic test. *The Journal of Applied Psychology*, 95(5), 834–848.
- Cressman, D. (2009). A brief overview of actor-network theory: punctualization, heterogeneous engineering and translation. *Paper for Simon Fraser University ACT Lab/Centre for Policy Research on Science & Technology (CPROST)*, 1–17. Retrieved from
<http://blogs.sfu.ca/departments/cprost/wp-content/uploads/2012/08/0901.pdf>
- Creswell, J. W. (2007). *Qualitative inquiry and research design: choosing among five approaches* (2nd ed.). Thousand Oaks, CA: Sage.
- Crotty, M. (1998). *The foundations of social research: meaning and perspective in the research process*. St Leonards, NSW: Allen and Unwin.
- Cumming, I., & Davies, J. (2017). *Improving digital literacy*. London. Retrieved from
<https://www.hee.nhs.uk/sites/default/files/documents/3146-HEE RCN 20 Report 16 pages FINAL.pdf>

- Cunliffe, A. L. (2010). Crafting qualitative research: Morgan and Smircich 30 years on. *Organizational Research Methods*, 14(4), 647–673. <https://doi.org/10.1177/1094428110373658>
- Currie, G., Lockett, A., Finn, R., Martin, G., & Waring, J. (2012). Institutional work to maintain professional power: recreating the model of medical professionalism. *Organization Studies*, 33(7), 937–962. <https://doi.org/10.1177/0170840612445116>
- Currie, G., & Procter, S. J. (2005). The antecedents of middle managers' strategic contribution: the case of a professional bureaucracy. *Journal of Management Studies*, 42(7), 1325–1356. <https://doi.org/10.1111/j.1467-6486.2005.00546.x>
- Currie, W. L. (2014). Translating health IT policy into practice in the UK national health service. *Scandinavian Journal of Information Systems*, 26(2), 3–26.
- Currie, W. L., & Guah, M. W. (2007). Conflicting institutional logics: a national programme for IT in the organisational field of healthcare. *Journal of Information Technology*, 22(3), 235–247. <https://doi.org/10.1057/palgrave.jit.2000102>
- Daines, G. (2011). *Liberating the NHS: an information revolution. The response of the Chartered Institute of Library and Information Professionals*. London. <https://doi.org/10.1017/CBO9781107415324.004>
- Dalrymple, P. W. (2002). The impact of medical informatics on librarianship. *IFLA Journal*, 58(5/6), 312–217.
- Darzi, A. (2008). *High quality care for all: NHS next stage review final report*. London. Retrieved from http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_085828.pdf
- Davies, B. S., Rafique, J., Vincent, T. R., Fairclough, J., Packer, M. H., Vincent, R., & Haq, I. (2012). Mobile Medical Education (MoMed) - how mobile information resources contribute to learning for undergraduate clinical students: a mixed methods study. *BMC Medical Education*, 12(1), 1. <https://doi.org/10.1186/1472-6920-12-1>
- Davies, H. T. O., & Harrison, S. (2003). Trends in doctor-manager relationships. *BMJ British Medical Journal*, 326, 646–649.
- Davies, H. T. O., & Mannion, R. (2013). Will prescriptions for cultural change improve the NHS? *BMJ British Medical Journal*, 346, 1305. Retrieved from <http://research-repository.st-andrews.ac.uk/bitstream/10023/3406/1/Davies2013bmj.f1305Prescriptions.pdf>
- Davies, K. (2011a). Information needs and barriers to accessing electronic information: hospital-based physicians compared to primary care physicians. *Journal of Hospital Librarianship*, 11(3), 37–41. <https://doi.org/10.1080/15323269.2011.587103>
- Davies, K. (2011b). Physicians and their use of information: a survey comparison between the United States, Canada, and the United Kingdom. *Journal of the Medical Library Association*, 99(1), 88–91. <https://doi.org/10.3163/1536-5050.99.1.015>

- Davies, P. (2013). *The NHS handbook 2013/14: The essential guide to the new NHS in England* (14th ed.). London: NHS Confederation.
- Dawson, J. (2014). Engagement in the NHS: evidence from the Staff Survey. In *NHS Confederation Annual Conference 5th June 2014*.
- Dee, C. R., & Stanley, E. E. (2005). Nurses' information needs: nurses' and hospital librarians' perspective. *Journal of Hospital Librarianship*, 5(2), 1–13.
https://doi.org/10.1300/J186v05n02_01
- Dee, C., & Stanley, E. E. (2005). Information-seeking behavior of nursing students and clinical nurses: implications for health sciences librarians. *Journal of the Medical Library Association*, 93(2), 213–22. Retrieved from <http://www.pubmedcentral.nih.gov>
- Deighan, M., & Bullivant, J. (2006). *Integrated governance handbook: a handbook for executives and non-executives in healthcare organisations*. London: Department of Health.
- Deisz, J. (2005). *Internet filtering and how it affects security, efficiency and thriving in Norwegian companies*. Gjøvik University College. Retrieved from <http://www.bibsys.no>
- Del Fiol, G., Workman, T. E., & Gorman, P. N. (2014). Clinical questions raised by clinicians at the point of care: a systematic review. *JAMA Internal Medicine*, 174(5), 710–8.
<https://doi.org/10.1001/jamainternmed.2014.368>
- den Outer, B., Handley, K., & Price, M. (2012). Situational analysis and mapping for use in education research: a reflexive methodology? *Studies in Higher Education*, 1–18.
- Department of Health. (s.d.). Information Governance Toolkit: requirements. Retrieved June 4, 2013, from
<https://www.igt.hscic.gov.uk/requirementsorganisation.aspx?tk=414246814775024&cb=12c1af00-377b-4dc1-9d8e-4ee26518846a&Inv=2&clnav=YES>
- Department of Health. (1997). *The new NHS: modern. dependable*. London: NHS Executive. Retrieved from
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266003/new_nhs.pdf
- Department of Health. (1998). *A first class service: quality in the new NHS*. London: Department of Health. Retrieved from
http://webarchive.nationalarchives.gov.uk/+www.dh.gov.uk/en/publicationsandstatistics/publications/publicationspolicyandguidance/dh_4006902
- Department of Health. (1999a). Caldicott guardians in the NHS. *Health Service Circular: HSC 1999/012*. Leeds: Department of Health.
- Department of Health. (1999b). *Making a difference: strengthening the nursing, midwifery and health visiting contribution to health and healthcare*. London: Stationery Office.
- Department of Health. (2000). *The NHS plan: a plan for investment, a plan for reform*. London: Department of Health.

- Department of Health. (2001). *Building the information core: implementing the NHS plan*. London. Retrieved from http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4066946.pdf
- Department of Health. (2002a). Learning from Bristol: the Department of Health's response to the Report of the public inquiry into children's heart surgery at the Bristol Royal Infirmary 1984-1995: executive summary. London: Department of Health. Retrieved from <http://webarchive.nationalarchives.gov.uk>
- Department of Health. (2002b). *Making information count: a human resources strategy for health informatics professionals*. London: Department of Health. Retrieved from <http://www.connectingforhealth.nhs.uk/systemsandservices/capability/phi/library/newsletters/pdf/issue49.pdf>
- Department of Health. (2004). *The NHS Knowledge and Skills Framework (NHS KSF) and the Development Review Process*. Leeds: Department of Health. Retrieved from http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4090843
- Department of Health. (2008). NHS information governance: guidelines on use of encryption to protect person identifiable and sensitive information. London. Retrieved from <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/encryptionguide.pdf>
- Department of Health. (2009a). *Living well with dementia: a national dementia strategy*. London. Retrieved from http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_094051.pdf
- Department of Health. (2009b). *Using mobile phones in NHS hospitals*. London: Department of Health.
- Department of Health. (2009c, January). Standards for better health. London: Department of Health. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/20543241>
- Department of Health. (2010). *Liberating the NHS: an information revolution: a consultation on proposals*. London. <https://doi.org/10.1016/j.endeavour.2006.11.001>
- Department of Health. (2011a). *A framework for technology enhanced learning*. London: Department of Health. <https://doi.org/10.1037/e501112012-001>
- Department of Health. (2011b). *Innovation health and wealth: accelerating adoption and diffusion in the NHS*. London: Department of Health.
- Department of Health. (2012a). *Compassion in practice: nursing, midwifery and care staff: our vision and strategy*. London.
- Department of Health. (2012b). *Prime Minister's challenge on dementia*. London.

- Department of Health. (2012c). The ionising radiation (medical exposure) regulations 2000. London: Department of Health. Retrieved from <https://www.gov.uk/government/publications/the-ionising-radiation-medical-exposure-regulations-2000>
- Department of Health. (2012d). *The power of information: putting all of us in control of the health and care information we need*. London: Department of Health. Retrieved from http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_134205.pdf
- Department of Health. (2012e). *Transforming care: a national response to Winterbourne View Hospital*. London. [https://doi.org/Gateway reference 18348](https://doi.org/Gateway%20reference%2018348)
- Department of Health. (2013a). *A state of the nation report on dementia*. London.
- Department of Health. (2013b). *Patients first and foremost: the initial government response to the report of the Mid Staffordshire NHS Foundation Trust public inquiry*. London: Department of Health.
- Department of Health. (2013c). *The NHS Constitution*. London.
- Department of Health. (2014). *Hard truths: the journey to putting patients first: volume 2*. London: Department of Health.
- Department of Health. (2015a). *Annual report and accounts 2014-15*. London. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447002/DH_accounts_14-15_web.pdf
- Department of Health. (2015b). NHS Constitution for England. London: Department of Health.
- Department of Health Informatics Directorate. (2010). Technology Bulletin : Microsoft Internet Explorer Security Vulnerability – 979352 – “Aurora.” Leeds: Department of Health Informatics Directorate. Retrieved from <http://webarchive.nationalarchives.gov.uk/20100203172543/http://www.connectingforhealth.nhs.uk/newsroom/news-stories/ie6guidance.pdf>
- Derbentseva, N., Fraser, B., Gibbon, S., & Hawton, A. (2016). *What do we know about threats from well-intentioned users, a literature review [sic]*. [Ottawa].
- Detlefsen, E. G. (1998). The information behaviors of life and health scientists and health care providers: characteristics of the research literature. *Bulletin of the Medical Library Association*, 86(3), 385–90. Retrieved from <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=226386&tool=pmcentrez&rendertype=abstract>
- Devitt, N., & Murphy, J. (2004). A survey of the information management and technology training needs of doctors in an acute NHS trust in the United Kingdom. *Health Information & Libraries Journal*, 21, 164–172. <https://doi.org/10.1111/j.1471-1842.2004.00492.x>

- Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security Industrial Management & Data Systems Computer Security Iss*, 7(4), 171–175. <https://doi.org/10.1108/09685229910292664>
- Dickinson, A. D., & Scott, M. (2012). *Diffusion of innovations in the National Health Service: a case study investigating the implementation of an electronic patient record system in a UK secondary care Trust*. Newcastle.
- Dikko, M. (2016). Establishing construct validity and reliability: pilot testing of a qualitative interview for research in takaful (Islamic insurance). *The Qualitative Report*, 21(3), article 6.
- Dimensional Research. (2015). *Context aware security: a survey of IT and business professionals*. Round Rock, TX: Dell.
- Dobson, P. J. (2001). The philosophy of critical realism — an opportunity for information systems research. *Information Systems Frontiers*, 3(2), 199–210.
- Dobson, P. J. (2012). Critical Realism and IS Research. In *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems* (pp. 63–81). IGI Global. <https://doi.org/10.4018/978-1-4666-0179-6.ch004>
- Dobson, P. J., & Love, P. E. D. (2004). Realist and postmodernist perspectives on information systems research: points of connection. *Australian Journal of Information Systems*, 12(1), 94–102.
- Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6), 449–457. <https://doi.org/10.1016/j.ijinfomgt.2009.05.003>
- Dole, W. V., Hurych, J. M., & Koehler, W. C. (2000). Values for librarians in the information age: an expanded examination. *Library Management*, 21(6), 285–297. <https://doi.org/10.1108/01435120010327597>
- Donaldson, A., & Walker, P. (2004). Information governance--a view from the NHS. *International Journal of Medical Informatics*, 73(3), 281–4. <https://doi.org/10.1016/j.ijmedinf.2003.11.009>
- Doney, L., Barlow, H., & West, J. (2005). Use of libraries and electronic information resources by primary care staff: outcomes from a survey. *Health Information and Libraries Journal*, 22(3), 182–8. <https://doi.org/10.1111/j.1471-1842.2005.00561.x>
- Dopson, S., & Fitzgerald, L. (Eds.). (2005). *Knowledge to action?: evidence based health care in context*. New York: New York : Oxford University Press, 2005.
- Doran, D. M., Haynes, R. B., Kushniruk, A., Straus, S., Grimshaw, J., Hall, L. M., ... Jedras, D. (2010). Supporting evidence-based practice for nurses through information technologies. *World Views on Evidence-Based Nursing*, 1(1), 4–15. Retrieved from http://www.nurseone-infusion.ca/docs/NurseOne/KnowledgeFeature/EIDM/Supporting_Evidence-Based_Practice_for_Nurses_through_Information_Technologies.pdf
- Douglas, M. (1992). *Risk and blame : essays in cultural theory*. London : Routledge. Retrieved from http://www.leeds.eblib.com/EBLWeb/patron/?target=patron&extendedid=E_508321_0

- Douglas, M. (1994). *Dominant rationality and risk perception* (Occasional papers No. 4). Sheffield: PERC.
- Douglas, M., & Wildavsky, A. (1982a). How can we know the risks we face? Selection is a social process. *Risk Analysis*, 2(2), 49–51.
- Douglas, M., & Wildavsky, A. (1982b). *Risk and culture: an essay on the selection of technical and environmental dangers*. Berkeley, London : University of California Press.
- Dowse, F. M., & Sen, B. A. (2007). Community outreach library services in the UK: a case study of Wirral Hospital NHS Trust (WHNT). *Health Information and Libraries Journal*, 24(3), 177–87. <https://doi.org/10.1111/j.1471-1842.2007.00714.x>
- Dromey, J. (2014). *Meeting the challenge: successful employee engagement in the NHS*. London. Retrieved from <http://www.ipa-involve.com/news/meeting-the-challenge-blog/>
- Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: current practices, trends and recommendations. *MIS Quarterly*, 27(4), 597–636.
- Dubois, E., & Mouratidis, H. (2010). Guest editorial: security requirements engineering: past, present and future. *Requirements Engineering*, 15(1), 1–5. <https://doi.org/10.1007/s00766-009-0094-8>
- Duffy, M. (2000). The Internet as a research and dissemination resource. *Health Promotion International*, 15(4), 349–353. <https://doi.org/10.1093/heapro/15.4.349>
- Dunleavy, P. (2005). New public management is dead--long live digital-era governance. *Journal of Public Administration Research and Theory*, 16(3), 467–494. <https://doi.org/10.1093/jopart/mui057>
- Dunn, J. E. (2016). The EU-US Privacy Shield agreement explained - preparing for uncertainty. Retrieved February 9, 2016, from <http://www.computerworlduk.com/security/eu-us-privacy-shield-agreement-explained-preparing-for-uncertainty-3634740/>
- e-Learning for Healthcare. (2008). Technical requirements for accessing all e-learning for healthcare products, (December), 10pp.
- e-mpirical. (2006). *Modernising healthcare training: e-learning in healthcare services; a report commissioned by the National Workforce Group (for the Strategic Health Authorities) and the Department of Health (England)*. Reading: e-mpirical. Retrieved from <http://kingsfund.koha-ptfs.eu/cgi-bin/koha/opac-detail.pl?biblionumber=37333>
- Eason, K. (2007). Local sociotechnical system development in the NHS National Programme for Information Technology. *Journal of Information Technology*, 22(3), 257–264. <https://doi.org/10.1057/palgrave.jit.2000101>
- Easton, G. (2010). Critical realism in case study research. *Industrial Marketing Management*, 39(1), 118–128. <https://doi.org/10.1016/j.indmarman.2008.06.004>
- Ebell, M. H., & Shaughnessy, A. (2003). Information mastery: integrating continuing medical education with the information needs of clinicians. *The Journal of Continuing Education in the Health Professions*, 23 Suppl 1, S53-62. <https://doi.org/10.1002/chp.1340230409>

- Ebenezer, C. (2000). Health libraries under financial constraint. *ASSIGNation*, 18(1), 14–19.
- Ebenezer, C. (2005). The new National Library for Health. *ASSIGNation*, 22(2), 35–41.
- Edwards, C., Fox, R., Gillard, S., Gourlay, S., Guven, P., Jackson, C., ... Drennan, V. (2013). *Explaining health managers' information seeking behaviour and use*. London.
- Egele, M., Kirda, E., & Kruegel, C. (2009). Mitigating drive-by download attacks: challenges and open problems. *iNetSec-Open Research Problems in Network Security*, 52–62.
- Elcock, M. (2016). Summary of responses: access to YouTube / streamed services query (July 18) [Electronic mailing list message]. Retrieved from <http://www.jiscmail.ac.uk/lis-medical>
- Elder-Vass, D. (2008). Searching for realism, structure and agency in Actor Network Theory. *The British Journal of Sociology*, 59(3), 455–73. <https://doi.org/10.1111/j.1468-4446.2008.00203.x>
- Elejabarrieta, F. (1994). Social positioning: a way to link social identity and social representations. *Social Science Information*, 33(2), 241–253. <https://doi.org/10.1177/053901894033002006>
- El Ouiridi, M., El Ouiridi, A., Segers, J., & Henderickx, E. (2014). Social media conceptualization and taxonomy: A Lasswellian framework. *Journal of Creative Communications*, 9(2), 107–126. <https://doi.org/10.1177/0973258614528608>
- Eley, R., Fallon, T., Soar, J., Buikstra, E., & Hegney, D. (2009). Barriers to use of information and computer technology by Australia's nurses a national survey. *Journal of Clinical Nursing*, 8, 1151–1158.
- Ely, J. W., Osheroff, J. A., Ebell, M. H., Bergus, G. R., Levy, B. T., & Chambliss, M. L. (1999). Analysis of questions asked by family doctors regarding patient care. *BMJ British Medical Journal*, 319, 358–361.
- Ensmenger, N. L. (2001). The “question of professionalism” in the computer fields. *IEEE Annals of the History of Computing*, 23(4), 56–74. <https://doi.org/10.1109/85.969964>
- Erickson, B. H. (1979). Some problems of inference from chain data. *Sociological Methodology*, 10(1), 276–302. <https://doi.org/10.2307/270774>
- Eshete, B., Villafiorita, A., Weldemariam, K., & Kessler, F. B. (2011). Malicious website detection: effectiveness and efficiency issues. In *SysSec Workshop (SysSec), 2011 First* (pp. 123–126).
- Estabrooks, C. A., O'Leary, K. A., Ricker, K. L., & Humphrey, C. K. (2003). The Internet and access to evidence: how are nurses positioned? *Journal of Advanced Nursing*, 42(1), 73–81. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/12641814>
- Estabrooks, C. A., Rutakumwa, W., O'Leary, K. A., Profetto-McGrath, J., Milner, M., Levers, M. J., & Scott-Findlay, S. (2005). Sources of practice knowledge among nurses. *Qualitative Health Research*, 15(4), 460–476. <https://doi.org/10.1177/1049732304273702>
- Evans, M., Maglaras, L., He, Y., & Janicke, H. (2016). Human Behaviour as an aspect of Cyber Security Assurance. *arXiv Preprint arXiv:1601.03921*, 1–22. <https://doi.org/10.1002/sec.1657>

- Evetts, J. (2003). The sociological analysis of professionalism: occupational change in the modern world. *International Sociology*, 18(2), 395–415.
<https://doi.org/10.1177/0268580903018002005>
- Evetts, J. (2011). A new professionalism? Challenges and opportunities. *Current Sociology*, 59(4), 406–422. <https://doi.org/10.1177/0011392111402585>
- Evetts, J. (2013). Professionalism: value and ideology. *Current Sociology*, (March).
<https://doi.org/10.1177/0011392113479316>
- Expensive iPads go to NHS board members. (2011, October). *Express and Star*. Retrieved from <http://www.expressandstar.com/news/2011/10/04/expensive-ipads-go-to-nhs-board-members/>
- Exworthy, M., Powell, M., & Mohan, J. (1999). The NHS: quasi-market, quasi-hierarchy and quasi-network? *Public Money and Management*, 19(4), 15–22. <https://doi.org/10.1111/1467-9302.00184>
- Eysenbach, G. (2008). Medicine 2.0: social networking, collaboration, participation, apomediation, and openness. *Journal of Medical Internet Research*, 10(3), e22.
<https://doi.org/10.2196/jmir.1030>
- Ezingear, J.-N., Bowen-Schrire, M., & Birchall, D. (2007). Triggers of change in information security management. *Journal of General Management*, 32(4), 53–72.
- F-Secure. (2012). Disabling Java plug-ins. Retrieved May 30, 2013, from http://www.f-secure.com/en/web/labs_global/disabling-java-plugins#more
- Faber, M., & Faber, R. (2010). *ITIL® and corporate risk alignment guide*. Norwich. Retrieved from http://www.best-management-practice.com/gempdf/ITIL_and_Corporate_Risk_Alignment_Guide.pdf
- Fagan, M., & Khan, M. M. H. (2016). Why do they do what they do? A study of what motivates users to (not) follow computer security advice. *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, (Soups). Retrieved from <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan>
- Fan, S., Radford, J., & Fabian, D. (2016). A mixed-method research to investigate the adoption of mobile devices and Web 2.0 technologies among medical students and educators. *BMC Medical Informatics and Decision Making*, 16(1), 43. <https://doi.org/10.1186/s12911-016-0283-6>
- Farahmand, F., Atallah, M., & Konsynski, B. (2008). Incentives and perceptions of information security risks. In *ICIS 2008*. Retrieved from <http://aisel.aisnet.org/icis2008/25>
- Farmer, J., Richardson, A., & Lawton, S. (1999). Improving access to information for nursing staff in remote areas: the potential of the Internet and other networked information resources. *International Journal of Information Management*, 19(1), 49–62.
[https://doi.org/10.1016/S0268-4012\(98\)00046-2](https://doi.org/10.1016/S0268-4012(98)00046-2)

- Farnan, J. M., Johnson, J. K., Meltzer, D. O., Humphrey, H. J., & Arora, V. M. (2008). Resident uncertainty in clinical decision making and impact on patient care: a qualitative study. *Quality and Safety in Health Care, 17*(2), 122–6. <https://doi.org/10.1136/qshc.2007.023184>
- Farrell, C., & Morris, J. (2003). The “neo-bureaucratic” state: professionals, managers and professional managers in schools, general practices and social work. *Organization, 10*(1), 129–156.
- Fast, I., Sørensen, K., Brand, H., & Suggs, L. S. (2015). Social media for public health: an exploratory policy analysis. *European Journal of Public Health, 25*(1), 162–166. <https://doi.org/10.1093/eurpub/cku080>
- Faulkner, P., & Runde, J. (2011). The social, the material, and the ontology of non-material technological objects. In *27th EGOS Colloquium, Gothenburg, July 6-9*. <https://doi.org/10.1017/CBO9781107415324.004>
- Faulkner, P., & Runde, J. (2013). Technological objects, social positions, and the transformational model of social activity. *MIS Quarterly, 37*(3), 803–818.
- Federation for Informatics Professionals. (s.d.). Federation for informatics professionals (Fed- IP): “re-energising professionalism.” London: UKCHIP.
- Fell, D. W., Burnham, J. F., & Dockery, J. M. (2013). Determining where physical therapists get information to support clinical practice decisions. *Health Information and Libraries Journal, 30*(1), 35–48. <https://doi.org/10.1111/hir.12010>
- Ferlie, E., Fitzgerald, L., Wood, M., & Hawkins, C. (2005). The nonspread of innovations: the mediating role of professionals. *Academy of Management Journal, 48*(1), 117–134. <https://doi.org/10.5465/AMJ.2005.15993150>
- Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: an informatics theory. *International Journal of Medical Informatics, 78*(12), 815–26. <https://doi.org/10.1016/j.ijmedinf.2009.08.006>
- Fernando, S., Choudrie, J., Lycett, M., & de Cesare, S. (2012). Hidden assumptions and their influence on clinicians’ acceptance of new IT systems in the NHS. *Information Systems Frontiers, 14*(2), 279–299. <https://doi.org/10.1007/s10796-010-9238-0>
- Fernando, S., Choudrie, J., Lycett, M., & De Cesare, S. (2012). Hidden assumptions and their influence on clinicians’ acceptance of new IT systems in the NHS. *Information Systems Frontiers, 14*(2), 279–299. <https://doi.org/10.1007/s10796-010-9238-0>
- Ferrar, M., Wood, J., Penny, M., & Date, V. (2009). General principles for securing information systems: good practice guideline. Leeds: NHS Connecting for Health.
- Fidel, R. (1984). The case study method: a case study. *Library and Information Science Research, 6*, 273–288.

- Fincham, R. (2006). Knowledge work as occupational strategy: comparing IT and management consulting. *New Technology, Work and Employment*, 21(1), 16–28.
<https://doi.org/10.1111/j.1468-005X.2006.00160.x>
- Fischer, E. A. (2016). *Cybersecurity issues and challenges: in brief*. Washington, DC.
- Fitzgerald, B., & Howcroft, D. (1998). Towards dissolution of the IS research debate: from polarization to polarity. *Journal of Information Technology*, 13(4), 313–326.
- Fitzgerald, L., & Ferlie, E. (2000). Professionals: back to the future? *Human Relations*, 53(5), 713–739.
<https://doi.org/10.1177/0018726700535005>
- Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin*, 51(4), 327–358.
 Retrieved from <http://www.analytictech.com/mb870/Readings/flanagan.pdf>
- Fléchain, I., Riegelsberger, J., & Sasse, M. A. (2006). Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 workshop on new security paradigms* (pp. 33–41). ACM.
- Fléchain, I., & Sasse, M. A. (2009). Stakeholder involvement, motivation, responsibility, communication: how to design usable security in e-Science. *International Journal of Human-Computer Studies*, 67(4), 281–296. <https://doi.org/10.1016/j.ijhcs.2007.10.002>
- Flemig, S., Osborne, S., & Kinder, T. (2016). Risky business—reconceptualizing risk and innovation in public services. *Public Money & Management*, 36(6), 425–432.
<https://doi.org/10.1080/09540962.2016.1206751>
- Flick, U., & Foster, J. (2008). Social representations. In C. Willig & W. Stainton-Rogers (Eds.), *The Sage handbook of qualitative research in psychology* (pp. 195–214). London: Sage.
- Flinn, S., & Lumsden, J. (2005). User perceptions of privacy and security on the web. In *Third Annual Conference on Privacy, Security and Trust (PST 2005)*. St Andrews, NB: National Research Council of Canada. Retrieved from <http://nparc.cisti-icist.nrc-cnrc.gc.ca/npsi/>
- Florance, V. (1992). Medical knowledge for clinical problem solving: a structural analysis of clinical questions. *Bulletin of the Medical Library Association*, 80(2), 140–9.
- Flynn, R. (2002). Clinical governance and governmentality. *Health, Risk & Society*, 4(2), 155–173.
<https://doi.org/10.1080/13698570220137042>
- Ford, J., & Korjonen, H. (2012). Information needs of public health practitioners: a review of the literature. *Health Information and Libraries Journal*, 29(4), n/a-n/a.
<https://doi.org/10.1111/hir.12001>
- Fourie, I., & Claasen-Veldsman, R. (2011). Exploration of the needs of South African oncology nurses for current awareness services available through the Internet. *Information Research*, 16(3), 14.
 Retrieved from [http://repository.up.ac.za/bitstream/handle/2263/19172/Fourie_Exploration\(2011\).pdf?sequence=1](http://repository.up.ac.za/bitstream/handle/2263/19172/Fourie_Exploration(2011).pdf?sequence=1)

- Fragos, C., Karyda, M., & Kiountouzis, E. (2007). Using the lens of circuits of power in information systems security management. In C. Lambrinoudakis, G. Pernul, & A. M. Tjoa (Eds.), *Trust, privacy and security in digital business: Lecture Notes in Computer Science Volume 4657* (Vol. 4657, pp. 228–236). Berlin, Heidelberg: Springer. <https://doi.org/10.1007/978-3-540-74409-2>
- Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology & Health, 25*(10), 1229–1245. <https://doi.org/10.1080/08870440903194015>
- Francis, R. (2013). *Report of the Mid Staffordshire NHS Foundation Trust public inquiry*. London. Retrieved from <http://www.midstaffpublicinquiry.com/report>
- Free wi-fi to be provided in all NHS buildings - Jeremy Hunt. (2015). Retrieved December 21, 2015, from <http://www.bbc.co.uk/news/uk-35147380>
- French, A. M., Guo, C., & Shim, J. J. P. Current status, issues, and future of Bring Your Own Device (BYOD), 35 Communications of the Association for Information Systems § (2014). Retrieved from <http://aisel.aisnet.org/cais/vol35/iss1/10>
- French, B. (2006). Uncertainty and information need in nursing. *Nurse Education Today, 26*(3), 245–52. <https://doi.org/10.1016/j.nedt.2005.10.005>
- Friedman, B., Nissenbaum, H., Hurley, D., Howe, D. C., & Felten, E. (2002). Users' conceptions of risks and harms on the web: a comparative study. In *CHI 2002, April 20-25, 2002*. Minneapolis, MN. Retrieved from <http://citeseer.uark.edu:8080/citeseerx/showciting?cid=3706597>
- Funkhouser, E., Agee, B. S., Gordan, V. V., Rindal, D. B., Fellows, J. L., Qvist, V., ... Gilbert, G. H. (2012). Use of online sources of information by dental practitioners: findings from The Dental Practice-Based Research Network. *Journal of Public Health Dentistry*. <https://doi.org/10.1111/j.1752-7325.2012.00373.x>
- Furnell, S., & Thomson, K.-L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security, 2009*(2), 5–10. [https://doi.org/10.1016/S1361-3723\(09\)70019-3](https://doi.org/10.1016/S1361-3723(09)70019-3)
- Gaglani, S. M., & Topol, E. J. (2014). iMedEd: the role of mobile health technologies in medical education. *Academic Medicine : Journal of the Association of American Medical Colleges, 89*(9), 1207–1209. <https://doi.org/10.1097/ACM.0000000000000361>
- Gagnon, K., & Sabus, C. (2015). Professionalism in a digital age: opportunities and considerations for using social media in health care. *Physical Therapy, 95*(3), 406–414. <https://doi.org/10.2522/ptj.20130227>
- Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology, 13*(1), 1. <https://doi.org/10.1186/1471-2288-13-117>

- Gallagher, C., McMenemy, D., & Poulter, A. (2015). Management of acceptable use of computing facilities in the public library: avoiding a panoptic gaze? *Journal of Documentation*, 71(3), 572–590.
- Galletta, D. F., & Polak, P. (2003). An empirical investigation of antecedents of Internet abuse in the workplace. *SIGHCI 2003 Proceedings*, 14.
- Gannon-Leary, P. (2006). Glut of information, dearth of knowledge? A consideration of the information needs of practitioners identified during the FAME project. *Library Review*, 55(2), 120–131. <https://doi.org/10.1108/00242530610649611>
- Gattine, K. (2014). Types of firewalls: An introduction to firewalls. Retrieved October 18, 2017, from <http://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-of-firewalls>
- Geenhuizen, M. van, & Faber, S. (2015). ICT adoption factors in medical hospitals: a European perspective and focus on the Netherlands. In *55th Congress of the European Regional Science Association*. Lisbon: Leibnitz-Informationszentrum Wirtschaft. Retrieved from http://www.econstor.eu/bitstream/10419/124669/1/ERSA2015_00590.pdf
- General Medical Council. (2013). Good medical practice: the duties of a doctor registered with the General Medical Council. London: General Medical Council.
- General Medical Council, & O'Brien, J. (2013). Doctors' use of social media: notes. Retrieved April 12, 2013, from https://m.facebook.com/note.php?note_id=549553408401395
- Georgaca, E., & Avdi, E. (2011). Discourse analysis. In D. Harper & A. R. Thompson (Eds.), *Qualitative research methods in mental health and psychotherapy* (pp. 147–161). Chichester: Wiley. <https://doi.org/10.1002/9781119973249.ch11>
- Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers and Security*, 24(1), 16–30. <https://doi.org/10.1016/j.cose.2004.11.002>
- Gerring, J. (2004). What is a case study and what is it good for? *American Political Science Review*, 98(2), 341–354. <https://doi.org/10.1017/S0003055404001182>
- Gerrish, K., Morgan, L., Mabbott, I., Debbage, S., Entwistle, B., Ireland, M., ... Warnock, C. (2006). Factors influencing use of information technology by nurses and midwives. *Practice Development in Health Care*, 5(2), 92–101. <https://doi.org/10.1002/pdh>
- Gibbs, S. (2014, April). UK government pays Microsoft £5.5m to extend Windows XP support. *Guardian*. Retrieved from <http://www.theguardian.com/technology/2014/apr/07/uk-government-microsoft-windows-xp-public-sector?CMP=EMCNEWEML6619I2>
- Giddens, A. (1999). Risk and responsibility. *Modern Law Review*, 62(1), 1–10.
- Gifford, W., Davies, B., Edwards, N., Griffin, P., & Lybanon, V. (2007). Managerial leadership for nurses' use of research evidence: an integrative review of the literature. *Worldviews on Evidence-Based Nursing*, 4, 126–145. <https://doi.org/10.1111/j.1741-6787.2007.00095.x>

- Gilbert, D. (2016). Is Skype safe and secure? What are the alternatives? Retrieved March 10, 2017, from <https://www.comparitech.com/blog/information-security/is-skype-safe-and-secure-what-are-the-alternatives/>
- Gilbert, F., & van der Heijden, M.-J. (2016). EU-U.S. Privacy Shield 2.0 signed, sealed and delivered. *Privacy and Security Law Report*, 15 PVLR 28.
- Gilmour, J. A., Huntington, A., Broadbent, R., Strong, A., & Hawkins, M. (2011). Nurses' use of online health information in medical wards. *Journal of Advanced Nursing*, 68(6), 1349–58. <https://doi.org/10.1111/j.1365-2648.2011.05845.x>
- Gilmour, J. A., Scott, S. D., & Huntington, N. (2008). Nurses and Internet health information: a questionnaire survey. *Journal of Advanced Nursing*, 61(1), 19–28. <https://doi.org/10.1111/j.1365-2648.2007.04460.x>
- Glassman, J., Prosch, M., & Shao, B. B. M. M. (2015). To monitor or not to monitor: effectiveness of a cyberloafing countermeasure. *Information and Management*, 52(2), 170–182. <https://doi.org/10.1016/j.im.2014.08.001>
- Glover, S. (2008). Practitioner Commentary on Toth B, Muir Gray JA, Fraser V, Ward R. National electronic Library for Health: progress and prospects. *Health Libraries Review* 2000, 17, 46-50. *Health Information and Libraries Journal*, 25 Suppl 1, 45–6. <https://doi.org/10.1111/j.1471-1842.2008.00805.x>
- Goff, M. (2014). *A critical investigation of electronic patient records in the NHS in England: tracing an elusive object through its actor network*. University of Salford.
- Goles, T., & Hirschheim, R. (2000). The paradigm is dead, the paradigm is dead...long live the paradigm: the legacy of Burrell and Morgan. *Omega*, 28, 249–268.
- Gomez Hidalgo, J. M., Sanz, E. P., Garcia, F. C., & Rodriguez, M. de B. (2009). Web content filtering. *Advances in Computers*, 76, 257–306.
- Gorman, P. N. (1995). Information needs of physicians. *Journal of the American Society for Information Science*, 46(10), 729–736.
- Gorman, P. N. (2001). Information needs in primary care: a survey of rural and nonrural primary care physicians. In V. et al. Patel (Ed.), *MEDINFO 2001: Studies in health technology and informatics* (Vol. 84, pp. 338–42). Amsterdam: IOS Press. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/11604759>
- Gorman, P. N., & Helfand, M. (1995). Information seeking in primary care: how physicians choose which clinical questions to pursue and which to leave unanswered. *Medical Decision Making*, 15(2), 113–119. <https://doi.org/10.1177/0272989X9501500203>
- Gosling, S., & Westbrook, J. I. (2004). Allied health professionals' use of online evidence: a survey of 790 staff working in the Australian public hospital system. *International Journal of Medical Informatics*, 73(4), 391–401. <https://doi.org/10.1016/j.ijmedinf.2003.12.017>

- Gosling, S., Westbrook, J. I., & Spencer, R. (2004). Nurses' use of online clinical evidence. *Journal of Advanced Nursing*, 47(2), 201–11. <https://doi.org/10.1111/j.1365-2648.2004.03079.x>
- Grant, H. (2015). Data protection 1998-2008. *Data Protection Summary Information Page*, 25(1), 44–50. <https://doi.org/10.1016/j.clsr.2008.11.005>
- Great White North Technologies. (s.d.). Email attachment safety - Zip files. Retrieved July 25, 2017, from <http://www.novatone.net/mag/mailsec2.htm>
- Greco, P., Laschinger, H. K. S., & Wong, C. (2006). Leader empowering behaviours, staff nurse empowerment and work engagement/burnout. *Nursing Leadership*, 19(4), 41–56.
- Green, A. (2011). Information overload in healthcare management: How the READ Portal is helping healthcare managers. *Journal of the Canadian Health Libraries Association (JCHLA)*, 32(3), 173–176.
- Green, J., Willis, K., Hughes, E., Small, R., Welch, N., Gibbs, L., & Daly, J. (2007). Generating best evidence from qualitative research: the role of data analysis. *Australian and New Zealand Journal of Public Health*, 31(6), 545–550. <https://doi.org/10.1111/j.1753-6405.2007.00141.x>
- Green, T. (1994). Images and perceptions as barriers to the use of library staff and services. *New Library World*, 95(1117), 19–24.
- Greener, I., Harrington, B., Hunter, D., & Powell, M. (2011). *A realistic review of clinico-managerial relationships in the NHS: 1991-2010* (SDO Programme). Southampton: NIHR. Retrieved from http://www.nets.nihr.ac.uk/data/assets/pdf_file/0003/64542/FR-08-1808-245.pdf
- Greenhalgh, T., & Keen, J. (2013). England's national programme for IT: from contested success claims to exaggerated reports of its death. *BMJ British Medical Journal*, 4130(June), 1–2. <https://doi.org/10.1136/bmj.f4130>
- Greenhalgh, T., Robert, G., Bate, P., Macfarlane, F., & Kyriakidou, O. (2008). *Diffusion of innovations in health service organisations: a systematic literature review*. Wiley.
- Greenhalgh, T., & Stones, R. (2010). Theorising big IT programmes in healthcare: Strong structuration theory meets actor-network theory. *Social Science & Medicine*, 70(9), 1285–1294. <https://doi.org/10.1016/j.socscimed.2009.12.034>
- Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Mohammad, Y., & Russell, J. (2008). Introduction of shared electronic records: multi-site case study using diffusion of innovation theory. *BMJ British Medical Journal*, 337(oct23 1). <https://doi.org/10.1136/bmj.a1786>
- Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Russell, J., & Potts, H. W. W. (2010). Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study. *BMJ*, 340(jun16 4), c3111–c3111. <https://doi.org/10.1136/bmj.c3111>
- Griffiths, M. (2010). Internet abuse and internet addiction in the workplace. *Journal of Workplace Learning*, 22(7), 463–472. <https://doi.org/10.1108/13665621011071127>
- Grossman, J. (2012). The web won't be safe or secure until we break it. *Communications of the ACM*, 10(11), 1–6. <https://doi.org/10.1145/2390756.2390758>

- Gualtieri, L., Javetski, G., & Corless, H. (2012). The integration of social media into courses: a literature review and case study from experiences at Tufts University School of Medicine. *Future Learning*, 1(1), 79–102. Retrieved from <http://essential.metapress.com/content/h733482663u035r2/>
- Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough ? An experiment with data saturation and variability. *Family Health International*, 18(1), 59–82. <https://doi.org/10.1177/1525822X05279903>
- Guillemin, M., & Gillam, L. (2004). Ethics, reflexivity, and “ethically important moments” in research. *Qualitative Inquiry*, 10(2), 261–280. <https://doi.org/10.1177/1077800403262360>
- Guttman, B., & Bagwill, R. (2012). *Internet security policy: a technical guide*. Gaithersburg, MD: National Institute of Standards and Technology.
- Guzman, I. R., Joseph, D., West, B. S., & Stanton, J. M. (2007). RIP - beliefs about IT culture : exploring national and gender differences. In *SIGMIS-CPR* (pp. 217–220). St Louis, MO: ACM.
- Guzman, I. R., Stam, K. R., & Stanton, J. M. (2008). The occupational culture of IS/IT personnel within organizations. *ACM SIGMIS Database*, 39(1), 33. <https://doi.org/10.1145/1341971.1341976>
- Guzman, I. R., Stanton, J. M., Stam, K. R., Vijayasri, V., Yamodo, I., Zakaria, N., & Caldera, C. (2004). A qualitative study of the occupational subculture of information systems employees in organizations. In *SIGMIS* (Vol. 1). Tucson, AZ.
- Györy, A., Uebernickel, F., Cleven, A., & Brenner, W. (2013). Exploring the shadows: IT governance approaches to user- driven innovation. In *ECIS 2012 Proceedings* (p. Paper 222). AIS Electronic Library. Retrieved from <http://aisel.aisnet.org/ecis2012/222>
- Hafferty, F. W. (2006). Definitions of professionalism: a search for meaning and identity. *Clinical Orthopaedics and Related Research*, (449), 193–204. Retrieved from http://journals.lww.com/corr/Abstract/2006/08000/Definitions_of_Professionalism_A_Search_For.34.aspx
- Haffey, F., Brady, R. R. W., & Maxwell, S. (2014). Smartphone apps to support hospital prescribing and pharmacology education: a review of current provision. *British Journal of Clinical Pharmacology*, 77(1), 31–8. <https://doi.org/10.1111/bcp.12112>
- Haigh, V. (2006). Clinical effectiveness and allied health professionals: an information needs assessment. *Health Information and Libraries Journal*, 23(1), 41–50. <https://doi.org/10.1111/j.1471-1842.2006.00635.x>
- Halcomb, E. J., & Davidson, P. M. (2006). Is verbatim transcription of interview data always necessary? *Applied Nursing Research : ANR*, 19(1), 38–42. <https://doi.org/10.1016/j.apnr.2005.06.001>
- Hall, M., Hanna, L.-A., & Huey, G. (2013). Use and views on social networking sites of pharmacy students in the United Kingdom. *American Journal of Pharmaceutical Education*, 77(1), 9. <https://doi.org/10.5688/ajpe7719>

- Hall, R. H. (1963). The concept of bureaucracy: an empirical assessment. *American Journal of Sociology*, 69(1), 32–40. <https://doi.org/10.1086/521238>
- Halligan, A., & Donaldson, L. (2001). Implementing clinical governance: turning vision into reality. *BMJ (Clinical Research Ed.)*, 322(7299), 1413–7. Retrieved from <http://www.pubmedcentral.nih.gov>
- Ham, C., Berwick, D., & Dixon, J. (2016). *Improving quality in the English NHS: A strategy for action*. London. Retrieved from http://www.kingsfund.org.uk/sites/files/kf/field/field_publication_file/Improving-quality-Kings-Fund-February-2016.pdf
- Hamblen, M. (2008). “Green” building windows can block cell signals. *Computerworld*. Retrieved from <http://www.computerworld.com/article/2537437/mobile-wireless/-green--building-windows-can-block-cell-signals.html>
- Hamm, M. P., Chisholm, A., Shulhan, J., Milne, A., Scott, S. D., Klassen, T. P., & Hartling, L. (2013). Social media use by health care professionals and trainees: a scoping review. *Academic Medicine : Journal of the Association of American Medical Colleges*, 88(9), 1376–83. <https://doi.org/10.1097/ACM.0b013e31829eb91c>
- Hammond, J., & McDermott, I. (s.d.). Policy document analysis. Retrieved July 11, 2017, from <http://www.methods.manchester.ac.uk/themes/qualitative-methods/policy-document-analysis/>
- Hampton, J. R. (1983). The end of clinical freedom. *British Medical Journal*, 287(6401), 1237–1238. <https://doi.org/10.1093/ije/dyr043>
- Hanna, F. W. (2008). The NHS culture : past, present and future – “reconciling the fighting Titans.” *International Journal of Clinical Leadership*, 16, 203–212.
- Hanson, C., West, J., Neiger, B., Thackeray, R., Barnes, M., & McIntyre, E. (2011). Use and acceptance of social media among health educators. *American Journal of Health Education*, 42(4), 197–204.
- Harbach, M., Fahl, S., & Smith, M. (2014). Who’s afraid of which bad wolf? A survey of IT security risk awareness. *2014 IEEE 27th Computer Security Foundations Symposium*, 97–110. <https://doi.org/10.1109/CSF.2014.15>
- Hardy, C., & Clegg, S. (2007). Relativity without relativism : reflexivity in post-paradigm organization studies. *British Journal of Management*, 8(June 1997), S5–S17.
- Harkins, M. (2013). *Managing risk and information security: protect to enable*. New York: Apress Open. Retrieved from <http://www.apress.com/9781430251132>
- Harris, J. G., Ives, B., & Junglas, I. (2011). *The genie is out of the bottle : managing the infiltration of consumer IT into the workforce*. Dublin. Retrieved from <http://nstore.accenture.com/IM/FinancialServices/AccentureLibrary/data/pdf/genie-out-of-bottle-it-workforce.pdf>

- Harrison, J., Hepworth, M., & de Chazal, P. (2004). NHS and social care interface: a study of social workers' library and information needs. *Journal of Librarianship and Information Science*, 36(1), 27–35. <https://doi.org/10.1177/0961000604042971>
- Harrison, S., & Ahmad, W. I. U. (2000). Medical autonomy and the UK state 1975 to 2025. *Sociology*, 34(1), 129–146. <https://doi.org/10.1177/S0038038500000092>
- Harrison, S., & Checkland, K. (2009). Evidence-based practice in UK health policy. In J. Gabe & M. Calnan (Eds.), *The new sociology of the health service* (pp. 121–142). Abingdon: Routledge.
- Harrison, S., & Lim, J. N. W. (2003). The frontier of control: doctors and managers in the NHS 1966 to 1997. *Clinical Governance: An International Journal*, 8(1), 13–18. <https://doi.org/10.1108/14777270310459922>
- Harrison, S., & Smith, C. (2003). Neo-bureaucracy and public management: the case of medicine in the National Health Service. *Competition & Change*, 7(4), 243–254. <https://doi.org/10.1080/1024529042000197077>
- Harter, J. K., Schmidt, F. L., Kilham, E. A., & Agrawal, S. (2009). *Q12 meta-analysis: the relationship between engagement at work and organizational outcomes*. Washington, DC. <https://doi.org/10.1161/CIRCULATIONAHA.105.579979>
- Hartley, J. (2013). Public and private features of innovation. *Handbook of Innovation in Public Services*, 44–59.
- Harvey, L. (1997). A genealogical exploration of gendered genres in IT cultures. *Information Systems Journal*, 7(2), 153–172. <https://doi.org/10.1046/j.1365-2575.1997.00012.x>
- Harwood, M. (2011). *Security strategies in web applications and social networking*. London: Jones & Bartlett Learning.
- Havelka, S. (2011). Mobile resources for nursing students and nursing faculty. *Journal of Electronic Resources in Medical Libraries*, 8(2), 194–199. <https://doi.org/10.1080/15424065.2011.576623>
- Haw, A., Derry, B., & Gowing, W. (2006). Professionalism and management of health informatics. In *Healthcare Computing Conference* (pp. 1–17). Retrieved from http://www.bcs.org/upload/pdf/professionalism_hc2006_20060905094156.PDF
- Hay-Gibson, N. (2008). A river of risk: a diagram of the history and historiography of risk management. *Interdisciplinary Studies in the Built and Virtual Environment*, 1(2).
- Haynes, D., & Robinson, L. (2015). Defining user risk in social networking services. *Aslib Journal of Information Management*, 67(1), 94–115.
- He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, 14(2), 171–180. <https://doi.org/10.1108/13287261211232180>
- Health and Care Professions Council. (s.d.). Focus on standards – social networking sites. London: Health and Care Professions Council.

- Health and Care Professions Council. (2014). Standards of conduct, performance and ethics. *Health Professions Council Documents*, 1–18. <https://doi.org/http://www.hpc-uk.org/assets/documents/10002367FINALcopyofSCPEJuly2008.pdf>
- Health and Social Care Information Centre. (s.d.). Informatics Capability Maturity Model. Leeds: Health and Social Care Information Centre. Retrieved from <http://www.hscic.gov.uk/media/14897/ICCM-printable-version/pdf/icmm-printable.pdf>
- Health and Social Care Information Centre. (2012). Guidance: social interaction – good practice. Leeds: Health and Social Care Information Centre. Retrieved from <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/socnetworking.pdf>
- Health and Social Care Information Centre. (2015a). *Checklist guidance for reporting, managing and investigating information governance and cyber security serious incidents requiring investigation*. Leeds. Retrieved from https://www.igt.hscic.gov.uk/resources/HSCIC_SIRI_Reporting_and_Checklist_Guidance.pdf
- Health and Social Care Information Centre. (2015b). Information governance - frequently asked questions. Retrieved November 12, 2015, from <http://systems.hscic.gov.uk/infogov/igfaq>
- Health and Social Care Information Centre. (2016). NHS business definitions: NHS allied health professional service. Retrieved March 30, 2016, from <http://www.datadictionary.nhs.uk>
- Health Education England. (2014). *Knowledge for healthcare: a development framework for NHS library and knowledge services in England 2015-2020*. London.
- Health Education England. (2015). About Health Education England. Retrieved February 13, 2015, from <http://hee.nhs.uk/about/>
- Health Protection Agency. (2012). *English national point prevalence survey on healthcare-associated infections and antimicrobial use, 2011*. London. Retrieved from <http://www.hpa.org.uk/Topics/InfectiousDiseases/InfectionsAZ/AntimicrobialResistance/HCAIPointPrevalenceSurvey/>
- Heather, B. (2016a). IG Toolkit to be scrapped as part of security reboot - Shaw. Retrieved November 17, 2016, from <http://www.digitalhealth.net/cybersecurity/48233/ig-toolkit-to-be-scrapped-as-part-of-security-reboot---shaw>
- Heather, B. (2016b). NHS Digital's plans for a digital NHS. Retrieved October 23, 2016, from <http://www.digitalhealth.net/features/48176/nhs-digital's-plans-for-a-digital-nh>
- Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: the importance of user rationale. *Information Management and Computer Security*, 21(4), 266–287. <https://doi.org/10.1108/IMCS-08-2012-0043>
- Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373–384. <https://doi.org/10.1016/j.jsis.2011.06.001>

- Henle, C. A., Kohut, G., & Booth, R. (2009). Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory. *Computers in Human Behavior*, 25(4), 902–910. <https://doi.org/10.1016/j.chb.2009.03.005>
- Henry, R. K., & Webb, C. (2014). A survey of social media policies in U.S. dental schools. *Journal of Dental Education*, 78(6), 850–855.
- Herman, C., & Ward, S. (2004). *The NHS library policy review - developing the strategic roadmap*. London: TFPL.
- Hewitt, J., & Thomas, P. (2007). The impact of clinical governance on the professional autonomy and self-regulation of general practitioners: colonization or appropriation. *Critical Management Studies ...*, 1–33. Retrieved from <http://merlin.mngt.waikato.ac.nz/ejrot/cmsconference/2007/proceedings/newperspectives/thomas.pdf>
- Hickson, D. J., Hinings, C. R., Lee, C., Schneck, R. E., & Pennings, J. M. (1971). A strategic contingencies' theory of intraorganizational power. *Administrative Science Quarterly*, 16(2), 216–229. <https://doi.org/10.2307/2391831>.
- Hider, P. N., Griffin, G., Walker, M., & Coughlan, E. (2009). The information-seeking behavior of clinical staff in a large health care organization. *Journal of the Medical Library Association*, 97(1), 47–50. <https://doi.org/10.3163/1536-5050.97.1.009>
- Hill, P. (2008). *Report of a national review of NHS health library services in England: from knowledge to health in the 21st century*. [S.l.] : National Library for Health. Retrieved from http://www.libraryservices.nhs.uk/document_uploads/NHS_Evidence/national_library_review_final_report_4feb_081.pdf
- Hillman, A., Tadd, W., Calnan, S., Calnan, M., Bayer, A., & Read, S. (2013). Risk, governance and the experience of care. *Sociology of Health and Illness*, 35(6), 939–955. <https://doi.org/10.1111/1467-9566.12017>
- Hirsch, C., & Ezingear, J. (2008). Perceptual and cultural aspects of risk management alignment: a case study. *Journal of Information System Security*, 4(1), 3–19.
- Hirsch, C., & Ezingear, J.-N. (2009). Aligning IT teams' risk management to business requirements. In M. Gupta & R. Sharman (Eds.), *Social and Human Elements of Information Security: Emerging Trends* (pp. 301–315). Hershey, PA: IGI Global.
- Hirsch, E. B., Raux, B. R., Lancaster, J. W., Mann, R. L., & Leonard, S. N. (2014). Surface microbiology of the iPad tablet computer and the potential to serve as a fomite in both inpatient practice settings as well as outside of the hospital environment. *PLoS One*, 9(10), 1–5. <https://doi.org/10.1371/journal.pone.0111250>
- Hirschheim, R. (1985). Information systems epistemology: an historical perspective. In E. Mumford, R. A. Hirschheim, G. Fitzgerald, & T. Wood-Harper (Eds.), *Research methods in information systems* (pp. 13–35). Amsterdam: North-Holland.

- Hirschheim, R., & Klein, H. K. (1989). Four paradigms of information systems development. *Communications of the ACM*, 32(10), 1199–1216.
- Hjørland, B. (2000). Library and information science: practice, theory , and philosophical basis. *Information Processing and Management*, 36(3), 501–531. [https://doi.org/10.1016/S0306-4573\(99\)00038-2](https://doi.org/10.1016/S0306-4573(99)00038-2)
- Hjørland, B. (2005). Empiricism, rationalism and positivism in library and information science. *Journal of Documentation*. <https://doi.org/10.1108/00220410510578050>
- Hoeksma, J. (2015). NHS IT leaders not getting on boards. Retrieved November 9, 2015, from <http://www.digitalhealth.net/cio/46846/nhs-it-leaders-not-getting-on-boards>
- Hoffman, C. (2012). Browser plugins - one of the biggest security problems on the web today. Retrieved May 30, 2013, from <http://www.makeuseof.com/tag/browser-plugins-one-of-the-biggest-security-problems-on-the-web-today-opinion/>
- Holmes, J., Fletcher, L., Buzzeo, J., Robinson, D., Truss, C., & Currie, G. (2014). *NIHR staff engagement in the NHS: review of practitioner studies of engagement*. London.
- Holt, J. (2004). Avoiding employment problems. In J. Newton & J. Holt (Eds.), *A manager's guide to IT law* (Vol. 44, pp. 38–49). Swindon: British Computer Society.
- Honan, B. (s.d.). Tackling the challenges of the next-generation firewall. Retrieved May 22, 2013, from <http://www.computerweekly.com/news/2240159262/Tackling-the-challenges-of-the-next-generation-firewall>
- Honeybourne, C., Sutton, S., & Ward, L. (2006). Knowledge in the Palm of your hands : PDAs in the clinical setting. *Health Information and Libraries Journal*, 23(1), 51–59.
- Hoque, K., Davis, S., & Humphreys, M. (2004). Freedom to do what you are told: senior management team autonomy in an NHS acute trust. *Public Administration*, 82(2), 355–375. <https://doi.org/10.1111/j.0033-3298.2004.00398.x>
- Houghton-Jan, S. (2008). *Internet filtering software tests: Barracuda, CyberPatrol, FilterGate and Websense*. San Jose, CA.
- Houghton-Jan, S. (2010). Internet filtering. *Library Technology Reports - Privacy and Freedom of Information in 21st-Century Libraries*, 46(8), 25–33. <https://doi.org/10.1109/MSP.2010.131>
- How-To Geek. (2015). What is DNS cache poisoning? Retrieved December 3, 2016, from <http://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/>
- Howard, F. (2007). *Modern web attacks*. Oxford.
- Howe, A. E., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012). The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy* (pp. 209–223). IEEE. <https://doi.org/10.1109/SP.2012.23>

- Howell, V., Thoppil, A., Mariyaselvam, M., Jones, R., Young, H., Sharma, S., ... Young, P. (2014). Disinfecting the iPad: evaluating effective methods. *The Journal of Hospital Infection*. <https://doi.org/10.1016/j.jhin.2014.01.012>
- HSCIC. (2013). *Checklist guidance for reporting, managing and investigating information governance and cyber security serious incidents requiring investigation. Version 2.0*. Leeds. Retrieved from [https://www.igt.hscic.gov.uk/resources/HSCIC SIRI Reporting and Checklist Guidance.pdf](https://www.igt.hscic.gov.uk/resources/HSCIC_SIRI_Reporting_and_Checklist_Guidance.pdf)
- Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, 69(12), 870–883. <https://doi.org/10.1016/j.ijhcs.2011.07.007>
- Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In J. Jacko (Ed.), *Human-computer interaction, part IV. Lecture notes in computer science 4553* (Vol. 4553 LNCS, p. 906-). Berlin: Springer-Verlag.
- Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, 29(3), 221–232. <https://doi.org/10.1080/01449290701679361>
- Huang, W. (2011). Newest Adobe Flash zero-day used in new drive-by download variation: drive-by cache, targets human rights website. Retrieved June 8, 2016, from <http://blog.armorize.com/2011/04/newest-adobe-flash-0-day-used-in-new.html>
- Hughes, B. (2010). *The Web 2.0 Internet: democratized internet collaborations in the healthcare sector*. Ramon Lull University.
- Hughes, B., Joshi, I., Lemonde, H., & Wareham, J. (2009). Junior physician's [sic] use of Web 2.0 for information seeking and medical education: a qualitative study. *International Journal of Medical Informatics*, 78(10), 645–55. <https://doi.org/10.1016/j.ijmedinf.2009.04.008>
- Hughes, B., Joshi, I., & Wareham, J. (2008). Health 2.0 and Medicine 2.0: tensions and controversies in the field. *Journal of Medical Internet Research*, 10(3), e23. <https://doi.org/10.2196/jmir.1056>
- Hunter, D. J. (1996). The changing roles of health care personnel in health and health care management. *Social Science & Medicine*, 43(5), 799–808. [https://doi.org/10.1016/0277-9536\(96\)00125-6](https://doi.org/10.1016/0277-9536(96)00125-6)
- Husin, M., & Hanisch, J. (2011). Social media and organisation policy (SOMEOP): Finding the perfect balance. In *ECIS 2011 Proceedings* (p. 253). Retrieved from <http://aisel.aisnet.org/ecis2011/253/>
- Huws, U. (2004). *Socio-economic research in the information society: a user's guide from the RESPECT Project*. Brighton: Institute of Employment Studies / RESPECT.
- Hyde, P., Granter, E., Hassard, J., McCann, L., & Morris, J. (2013). *Roles and behaviours of middle and junior managers: managing new organizational forms of healthcare*. Southampton.
- IFLA, & UNESCO. (2006). *IFLA/UNESCO Internet manifesto guidelines*. The Hague.
- IG Toolkit update from NHS Digital. (2017). Leeds: Information Governance Alliance.

- Igure, V. M., & Williams, R. D. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys and Tutorials*, 10(1), 6–19. <https://doi.org/10.1109/COMST.2008.4483667>
- Iivari, J., Hirschheim, R., & Klein, H. (2008). Challenges of professionalization: bridging research and practice through a body of knowledge for IT specialists. *Advances in Information Systems Research, Education and Practice*, 274, 15–27.
- Imperva. (2013). Search engine poisoning (SEP). Retrieved May 31, 2013, from http://www.imperva.com/resources/glossary/search_engine_poisoning_sep.html
- Information Commissioner's Office. (2005). Data protection: the employment practices code: supplementary guidance. London. Retrieved from http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Detailed_specialist_guides/employment_practice_code_supplementary_guidance.aspx
- Information Commissioner's Office. (2010). Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998. London: Information Commissioner's Office.
- Information Commissioner's Office. (2012, October 12). Information security (Principle 7). Retrieved May 31, 2013, from http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_7
- Information Governance Alliance. (2015). The use of mobile devices in hospitals (e.g. phones, tablets and cameras). Leeds: Information Governance Alliance.
- Inglesant, P., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. *Security*, 1, 383–392. Retrieved from <http://eprints.ucl.ac.uk/102754/>
- Inglesant, P., & Sasse, M. A. (2011a). Information security as organizational power: a framework for re-thinking security policies. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)* (pp. 9–16). IEEE. Retrieved from <http://discovery.ucl.ac.uk/1328206/>
- Inglesant, P., & Sasse, M. A. (2011b). Policy and power: a framework for re-thinking information security. In *Proceedings of 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)* (pp. 9–16).
- ISACA. (2010). *Social media: business benefits and security, governance and assurance perspectives*. Rolling Meadows, IL. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Social-Media_whp_Eng_0510.pdf?regnum=302043
- ISO. (2013). ISO/IEC 27001:2013, Information technology -- security techniques -- information security management systems -- requirements. Geneva: International Organization for Standardization.
- Isetta, M. (2008). Evidence-based practice, healthcare delivery and information management. *Aslib Proceedings*, 60(6), 619–641. <https://doi.org/10.1108/00012530810924302>

- Israel, M., & Hay, I. (2006). *Research ethics for social scientists*. London: Sage.
- Jacks, T. (2012). *An examination of IT occupational culture: interpretations, measurement and impact*. University of North Carolina at Greensboro. Retrieved from http://libres.uncg.edu/ir/uncg/f/Jacks_uncg_0154D_10981.pdf
- Jacks, T., & Palvia, P. (2011). A cultural sociology perspective on IT occupational culture. In *AMCIS 2011 Proceedings - All Submissions*. Retrieved from http://aisel.aisnet.org/amcis2011_submissions/395
- Jackson, R., Baird, W., Davis-Reynolds, L., Smith, C., Blackburn, S., & Allsebrook, J. (2007). The information requirements and information-seeking behaviours of health and social care professionals providing care to children with health care needs: a pilot study. *Health Information and Libraries Journal*, 24(2), 95–102. <https://doi.org/10.1111/j.1471-1842.2007.00700.x>
- Jacobs, A., & Nakata, K. (2012). Organisational semiotics methods to assess organisational readiness for internal use of social media. *AMCIS 2012 Proceedings*, 9.
- Järvelin, K., & Wilson, T. D. (2003). Conceptual models for information seeking and retrieval research. *Information Research*, 9(1).
- Jasanoff, S. (1998). The political science of risk perception. *Reliability Engineering & System Safety*, 59(1), 91–99. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0951832097001294>
- Jasperson, J., Butler, B. S., Carte, T. A., Price, M. F., & Saunders, C. S. (2002). Power and information technology research: a metatriangulation review. *MIS Quarterly*, 26(4), 397–459.
- Jia, R., & Reich, B. H. (2011). IT service climate—an essential managerial tool to improve client satisfaction with IT service quality. *Information Systems Management*, 28(2), 174–179. <https://doi.org/10.1080/10580530.2011.562401>
- Jia, R., & Reich, B. H. (2013). IT service climate, antecedents and IT service quality outcomes: Some initial evidence. *Journal of Strategic Information Systems*, 22(null), 51–69. <https://doi.org/10.1016/j.jsis.2012.10.001>
- Jia, R., Reich, B. H., & Pearson, J. M. (2008). IT service climate: an extension to IT service quality research. *Journal of the Association for Information Systems*, 9(5), 294–320.
- Jiang, H., & Tsohou, A. (2014). Expressive or instrumental: a dual-perspective model of personal web usage at workplace [sic]. In *22nd European Conference on Information Systems* (pp. 1–12). Tel Aviv.
- Joffe, H. (1999). *Risk and “the other.”* Cambridge: Cambridge University Press.
- Joffe, H. (2003). Risk: from perception to social representation. *The British Journal of Social Psychology*, 42(n1), 55–73. <https://doi.org/10.1348/014466603763276126>

- Joffe, H. (2011). Thematic analysis. In *Qualitative research methods in mental health and psychotherapy: a guide for students and practitioners* (pp. 209–223). Chichester: Wiley-Blackwell.
- Johannisson, J., & Sundin, O. (2007). Putting discourse to work: information practices and the professional project of nurses. *Library Quarterly*, 77(2), 199–218.
- Johansson, P., Petersson, G. I., Saveman, B.-I., & Nilsson, G. C. (2012). Experience of mobile devices in nursing practice. *Vård I Norden*. Retrieved from <http://www.diva-portal.org/smash/record.jsf?pid=diva2:600919&dswid=-1700>
- Johnson, J. J., & Ugray, Z. (2007). Employee Internet abuse: policy versus reality. *Information Systems*, VIII(2), 214–219.
- Johnson, M. E., Goetz, E., & Pfleeger, S. L. (2009). Security through information risk management. *IEEE Security & Privacy*, 7(3), 45–52. <https://doi.org/10.1109/MSP.2009.77>
- Johnson, P., & Duberley, J. (2000). *Understanding management research*. London: Sage.
- Johnson, P. T., Chen, J. K., Eng, J., Makary, M. A., & Fishman, E. K. (2008). A comparison of World Wide Web resources for identifying medical information. *Academic Radiology*, 15(9), 1165–1172. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1076633208001426>
- Johnson, R. K., & Luther, J. (2007). *The E-only tipping point for journals: what's ahead in the print-to-electronic transition zone*. Washington, DC. Retrieved from http://eprints.rclis.org/11127/1/Electronic_Transition_final.pdf
- Johnson, S. (2013). Bringing IT out of the shadows. *Network Security*, 2013(12), 5–6. [https://doi.org/10.1016/S1353-4858\(13\)70134-X](https://doi.org/10.1016/S1353-4858(13)70134-X)
- Jones, A. (2007). A framework for the management of information security risks. *BT Technology Journal*, 25(1), 30–36. <https://doi.org/10.1007/s10550-007-0005-9>
- Jones, C., & Hayter, M. (2013). Editorial: Social media use by nurses and midwives: a “recipe for disaster” or a “force for good”? *Journal of Clinical Nursing*, 22, 1495–1496. <https://doi.org/10.1111/jocn.12239>
- Jones, J., Schilling, K., & Pesut, D. (2011). Barriers and benefits associated with nurses [sic] information seeking related to patient education needs on clinical nursing units. *The Open Nursing Journal*, 5, 24–30. <https://doi.org/10.2174/1874434601105010024>
- Joshi, C., Singh, U. K., & Tarey, K. (2015). A Review on Taxonomies of Attacks and Vulnerability in Computer and Network System. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(1).
- Joshi, K. D., & Schmidt, N. L. (2006). Is the information systems profession gendered? Characterization of IS professionals and IS career. *The Data Base for Advances in Information Systems*, 37(4), 26–41.
- Joungtrakul, J., Sheehan, B., & Aticomswan, S. (2013). Qualitative data collection tool: a new approach to developing an interview guide. *AFBE Journal*, 6(2), 140–154.

- Journals and databases. (2008). Retrieved March 2, 2016, from <http://www.library.nhs.uk/CommsPage.aspx>
- Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57(10), 2206–2211. <https://doi.org/10.1016/j.comnet.2012.11.023>
- Juricich, A. L. M. D. (2014). Social media, evidence-based tweeting, and JCEHP. *Journal of Continuing Education in the Health Professions*, 34(4), 202–204. <https://doi.org/10.1002/chp>
- Kaarst-Brown, M. L., & Robey, D. (2006). More on myth, magic and metaphor. *Information Technology and People*, 12(2), 192–218.
- Kaehne, A. (2014). One NHS, or many? The National Health Service under devolution. *Political Insight*, 5(2), 30–33. <https://doi.org/10.1111/2041-9066.12060>
- Kaganer, E., & Vaast, E. (2010). Responding to the (almost) unknown: social representations and corporate policies of social media. In *ICIS 2010 Proceedings* (p. Paper 163). Retrieved from http://aisel.aisnet.org/icis2010_submissions/163
- Kahan, D. M. (2008). Cultural cognition as a conception of the cultural theory of risk. Retrieved from <http://papers.ssrn.com/abstract=1123807>
- Kahan, D. M., Braman, D., Slovic, P., Gastil, J., & Cohen, G. (2009). Cultural cognition of the risks and benefits of nanotechnology. *Nature Nanotechnology*, 4(2), 87–90. <https://doi.org/10.1038/nnano.2008.341>
- Kamath, J.-P. (2008). HMRC left the door open to data loss. Retrieved February 18, 2015, from <http://www.computerweekly.com/news/1280096733/HMRC-left-the-door-open-to-data-loss>
- Kanter, R. M. (1979). Power failure in management circuits. *Harvard Business Review*, 57(4), 65–75.
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68. <https://doi.org/10.1016/j.bushor.2009.09.003>
- Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, 9(3), 163–175.
- Kearney, W. D. (2016). *Risk homeostasis as a factor in information security*. North-West University.
- Keats, S., & Koshy, E. (2009). *The Web's most dangerous search terms*. McAfee Reports. Santa Clara, CA. Retrieved from https://promos.mcafee.com/en-us/pdf/most_dangerous_searchterm_us.pdf
- Kelly, W. (2014). How a UK hospital mobilized its board with Huddle for iPad. Retrieved July 27, 2015, from <http://www.techrepublic.com/article/how-a-uk-non-profit-mobilized-board-with-huddle-for-ipad/>
- Kent, A. D., Liebrock, L. M., & Neil, J. (2013). Web adoption: an attempt toward classifying risky Internet web browsing behavior. In *Proceedings of the LASER 2013* (pp. 25–36). USENIX Association. Retrieved from <https://www.usenix.org/laser2013/program/kent>

- Kent, P. (2006). Search engine optimization. *Journal of Visual Communication in Medicine*, 29(1), 39–40. <https://doi.org/10.1080/01405110600652297>
- Keogh, B. (2013). *Review into the quality of care and treatment provided by 14 hospital trusts in England*. s.l.
- Kerr, S. (2009). Using medicines wisely: the medicines information pharmacist's role. *Pharmaceutical Journal*, (August). Retrieved from <http://www.pharmaceutical-journal.com/learning/learning-article/using-medicines-wisely-the-medicines-information-pharmacists-role/10976343.article>
- Kettinger, W. J., & Lee, C. C. (2002). Understanding the IS-user divide in IT innovation. *Communications of the ACM*, 45(2), 79–84. <https://doi.org/10.1145/503124.503127>
- Khidzir, N. Z. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. *Lecture Notes on Information Theory*, 4(1), 18–24. <https://doi.org/10.18178/lnit.4.1.18-24>
- Kiedrowski, L. M., Perisetti, A., Loock, M. H., Khaitza, M. L., & Guerrero, D. M. (2013). Disinfection of iPad to reduce contamination with *Clostridium difficile* and methicillin-resistant *Staphylococcus aureus*. *American Journal of Infection Control*, 41(11), 1136–1146. <https://doi.org/10.1016/j.ajic.2013.01.030>
- Killoran, J. B. (2013). How to use search engine optimization techniques to increase website visibility. *IEEE Transactions on Professional Communication*, 56(1), 50–66. <https://doi.org/10.1109/TPC.2012.2237255>
- Kim, S. J., & Byrne, S. (2011). Conceptualizing personal web usage in work contexts: a preliminary framework. *Computers in Human Behavior*, 27(6), 2271–2283. <https://doi.org/10.1016/j.chb.2011.07.006>
- Kirk, M. (2009). Language as social institution: the male-centered IT culture. In *Gender and information technology* (pp. 119–142). Hershey, PA: IGI Global. <https://doi.org/10.4018/978-1-59904-786-7>
- Kirkpatrick, I., Ackroyd, S., & Walker, R. (2007). Public management reform in the UK and its consequences for professional organisation: a comparative analysis. *Public Administration*, 85(1), 9–26. Retrieved from <http://eprints.lancs.ac.uk/27436/>
- Kirlappos, I., & Sasse, M. A. (2014). What usable security really means: trusting and engaging users. In *Human aspects of informatoin security, privacy and trust: Second International Conference, HAS 2014 Held as Part of HCI International 2014 ... Proceedings* (pp. 69–78). Heraklion, Crete, Greece.
- Kirlappos, I., & Sasse, M. A. (2015). Fixing security together: leveraging trust relationships to improve security in organizations. In *USEC '15*. San Diego, CA. <https://doi.org/10.14722/usec.2015.23013>
- Kirshbaum, M. N. (2004). Are we ready for the Electronic Patient Record? Attitudes and perceptions of staff from two NHS trust hospitals. *Health Informatics Journal*, 10(4), 265–276. <https://doi.org/10.1177/1460458204048509>

- Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies of information systems. *Management Information Systems Quarterly*, 23(1), 67–93.
- Klein, H. K., & Myers, M. D. (2001). A classification scheme for interpretive research in information systems. In E. M. Trauth (Ed.), *Qualitative research in IS: issues and trends* (pp. 218–239). Hershey, PA: Idea Group Publishing.
- Kloda, L. A., & Bartlett, J. C. (2009). Clinical information behavior of rehabilitation therapists: a review of the research on occupational therapists, physical therapists, and speech-language pathologists. *Journal of the Medical Library Association*, 97(3), 194–202.
<https://doi.org/10.3163/1536-5050.97.3.008>
- Koçak, N. G., Kaya, S., & Erol, E. (2013). Social media from the perspective of diffusion of innovation approach. *The Macrotheme Review: A Multidisciplinary Journal of Global Macro Trends*, 2(3), 144–160.
- Koch, H., Gonzalez, E., & Leidner, D. Resolving IT-culture conflict in enterprise 2.0 implementations, AMCIS 2011 Proceedings - All Submissions § (2011). Retrieved from http://aisel.aisnet.org/amcis2011_submissions/279
- Koch, H., Leidner, D. E., & Gonzalez, E. S. (2013). Digitally enabling social networks: resolving IT-culture conflict. *Information Systems Journal*, 23(6), 201–523.
<https://doi.org/10.1111/isj.12020>
- Koehler, W. C. (2003). Professional values and ethics as defined by “The LIS Discipline.” *Journal of Education for Library and Information Science*, 44(2), 99–119. Retrieved from http://www.jstor.org/stable/40323926?seq=1#page_scan_tab_contents
- Koh, S., Cattell, G. M., Cochran, D. M., Krasner, A., Langheim, F. J. P., & Sasso, D. (2013). Psychiatrists’ use of electronic communication and social media and a proposed framework for future guidelines. *Journal of Psychiatric Practice*, 19(3), 254–63.
<https://doi.org/10.1097/01.pra.0000430511.90509.e2>
- Kolkowska, E. (2006). Values for information system security in an academic environment: a pilot study.
- Kolkowska, E. (2011). Security subcultures in an organization - exploring value conflicts. In *ECIS 2011 Proceedings*. Retrieved from <http://aisel.aisnet.org/ecis2011/237>
- Kolkowska, E., Hedström, K., & Karlsson, F. (2009). Information security goals in a Swedish hospital. In G. Dhillon (Ed.), *Security, Assurance and Privacy: Organisational Challenges. Proceedings of the 8th Annual Security Conference* (pp. 1–11). Las Vegas, NV. Retrieved from www.security-conference.org
- Koskosas, I. (2013). A short literature review in information systems security approaches. *Business Excellence and Management*, 3(2), 5–15.
- Koskosas, I., & Siomos, C. (2011). Information security : corporate culture and organizational commitment. *International Journal of Humanities and Social Science*, 1(3), 192–198.

- Kostagiolas, P. A., Ziavrou, K., Alexias, G., & Niakas, D. (2012). Studying the information-seeking behavior of hospital professionals: the case of METAXA cancer hospital in Greece. *Journal of Hospital Librarianship*, 12(1), 33–45. <https://doi.org/10.1080/15323269.2012.637871>
- Kostera, M., & Postuła, A. (2011). Holding up the aegis: on the construction of social roles by Polish IT professionals and the change in agency. *Tamara: Journal for Critical Organizational Inquiry*, 9(1), 83–92.
- Kotb, A., Roberts, C., & Sian, S. (2012). E-business audit: Advisory jurisdiction or occupational invasion? *Critical Perspectives on Accounting*, 23(6), 468–482. <https://doi.org/10.1016/j.cpa.2012.03.003>
- Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies? *Information & Management*, 41(2), 597–607. <https://doi.org/10.1016/j.im.2003.08.001>
- Kowal, S., & O'Connell, D. C. (2014). Transcription as a crucial step of data analysis. In U. Flick (Ed.), *The Sage handbook of qualitative data analysis* (pp. 64–79). London: Sage.
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2016). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 1, 1–10. <https://doi.org/10.3233/THC-161263>
- Kshetri, N. (2012). Privacy and security aspects of social media: institutional and technological environment. *Pacific Asia Journal of the Association for Information Systems*, 3(3), article 2.
- Kummerow, E. H., & Innes, J. M. (1994). Social representations and the concept of organizational culture. *Social Science Information*, 33(2), 255–271. <https://doi.org/10.1177/053901894033002007>
- Lacey, A. R. (1976). *A dictionary of philosophy*. London: Routledge and Kegan Paul.
- Lacey Bryant, S. (2016). LKS for different generations: mind the gap (July 28) [Electronic mailing list message]. Retrieved from <https://www.jiscmail.ac.uk/cgi-bin/webadmin?A2=ind1607&L=lis-medical&F=&S=&P=76201>
- Lafferty, N. (2013). *NHS-HE connectivity project: Web 2.0 and social media in education and research*. Retrieved from <https://community.ja.net/groups/nhs-he-forum-connectivity-project/document/web-20-and-social-media-education-and-research>
- Lafferty, N. (2015). *Barriers to access for technology enhanced learning (TEL)*. London: Health Education England.
- Lafferty, N. (2017). *Barriers to access for technology enhanced learning (TEL) v. 2.8*. London. Retrieved from <https://www.hee.nhs.uk>
- Lalonde Lévesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013). A clinical study of risk factors related to malware infections. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13*, 97–108. <https://doi.org/10.1145/2508859.2516747>

- Lam, A. (2000). Tacit knowledge, organizational learning and societal institutions: an integrated framework. *Organization Studies*, 21(3), 487–513. <https://doi.org/10.1177/0170840600213001>
- Lambert, P. (2013). How to check and configure your browser plugins. Retrieved May 30, 2013, from <http://www.techrepublic.com/blog/security/how-to-check-and-configure-your-browser-plugins/9156>
- Lambert, S., Herbert, I., & Rothwell, A. (2013). Understanding and navigating new professional ways of working: an analysis of the literature. Loughborough.
- Lampard, K., & Marsden, E. (2015). *Themes and lessons learnt from NHS investigations into matters relating to Jimmy Savile*. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/407209/KL_1_lessons_learned_report_FINAL.pdf
- Landry, C. F. (2006). Work roles, tasks, and the information behavior of dentists. *Journal of the American Society for Information Science and Technology*, 57(14), 1896–1908. <https://doi.org/10.1002/asi>
- Lapke, M., & Dhillon, G. (2008). Power relationships in information systems security policy formulation and implementation. In *ECIS 2008 Proceedings* (Paper 119).
- Larsen, C. (2015). Search engine poisoning (SEP) update: dangerous searches. Retrieved from <https://www.bluecoat.com/security-blog/2015-01-07/search-engine-poisoning-sep-update-dangerous-searches>
- Larson, M. S. (1977). *The rise of professionalism: a sociological analysis*. Berkeley, CA: University of California Press.
- Laschinger, H. K. S. (2008). Effect of empowerment on professional practice environments, work satisfaction, and patient care quality: further testing the nursing worklife model. *Journal of Nursing Care Quality*, 3(4), 322–330. Retrieved from http://journals.lww.com/jncqjournal/Abstract/2008/10000/Effect_of_Empowerment_on_Professional_Practice.7.aspx
- Laschinger, H. K. S., & Finegan, J. E. (2004). Empowerment, interactional justice, trust and respect: a nursing recruitment and retention strategy. In *Academy of Management Proceedings* (pp. C1–C6).
- Laschinger, H. K. S., Finegan, J., & Shamian, J. (2001). The impact of workplace empowerment, organizational trust on staff nurses' work satisfaction and organizational commitment. *Health Care Management Review*, 26(3), 7–23. Retrieved from <http://ovidsp.tx.ovid.com.eresources.shef.ac.uk/sp-3.15.1b/ovidweb.cgi>
- Laschinger, H. K. S., Gilbert, S., Smith, L. M., & Leslie, K. (2010). Towards a comprehensive theory of nurse/patient empowerment: Applying Kanter's empowerment theory to patient care. *Journal of Nursing Management*, 18(1), 4–13. <https://doi.org/10.1111/j.1365-2834.2009.01046.x>

- Laschinger, H. K. S., Wilk, P., Cho, J., & Greco, P. (2009). Empowerment, engagement and perceived effectiveness in nursing work environments: Does experience matter? *Journal of Nursing Management*, 17(5), 636–646. <https://doi.org/10.1111/j.1365-2834.2008.00907.x>
- Law, J., & Hassard, J. (1999). *Actor network theory and after*. Oxford: Blackwell Publishing.
- Lawton, S. (2015). A guide to security information and event management. Retrieved March 17, 2017, from <http://www.tomsitpro.com/articles/siem-solutions-guide,2-864.html>
- Le, N. T., & Hoang, D. B. (2016). Can maturity models support cyber security? In *Performance Computing and Communications Conference (IPCCC)* (pp. 1–7). IEEE.
- Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, 37(12), 1049–1092. <https://doi.org/10.1108/MRR-04-2013-0085>
- LeBlanc, D., & Biddle, R. (2012). Risk perception of internet-related activities. *2012 10th Annual International Conference on Privacy, Security and Trust, PST 2012*, 88–95. <https://doi.org/10.1109/PST.2012.6297924>
- Leclercq-Vandelannoitte, A. (2015). Managing BYOD: how do organizations incorporate user-driven IT innovations? *Information Technology & People*, 28(1), 2–33. <https://doi.org/10.1108/ITP-11-2012-0129>
- Lee, A. S. (1991). Integrating positivist and interpretive approaches to organizational research. *Organization Science*, 2(4), 342–365. <https://doi.org/10.1287/orsc.2.4.342>
- Lehmann, C. U., Cohen, B. A., & Kim, G. R. (2005). Blocking of pornography-seeking behavior in digital image libraries: adventures in the skin trade. *AMIA 2005 Annual Symposium Proceedings*, 435–9. Retrieved from <http://europepmc.org/articles/PMC1560843/?report=abstract>
- Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: towards a theory of information technology culture conflict. *MIS Quarterly*, 30(2), 357–399.
- Leiter, M. P., & Maslach, C. (2003). Areas of worklife: a structured approach to organizational predictors of job burnout. *Research in Occupational Stress and Well Being*, 3, 91–134. [https://doi.org/10.1016/S1479-3555\(03\)03003-8](https://doi.org/10.1016/S1479-3555(03)03003-8)
- Leitold, F. (2016). *Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility*. Veszprém. Retrieved from <http://www.secudit.com/assets/images/VB2016-paper.pdf>
- Lemos, R. (2015, March). The hunt for data analytics: Is your SIEM on the endangered list? *Information Security*, 4–9.
- Levy, D. M. (2003). Documents and libraries: A sociotechnical perspective. In A. P. Bishop, N. A. Van House, & B. P. Battenfield (Eds.), *Digital library use: Social practice in design and evaluation* (pp. 25–42). Cambridge, MA: MIT Press.

- Li, Y., & Belkin, N. J. (2010). An exploration of the relationships between work task and interactive information search behavior. *Journal of the American Society for Information Science and Technology*, 61(9), 1771–1789. <https://doi.org/10.1002/asi.21359>
- Liddell, A., Adshead, S., & Burgess, E. (2008). *Technology in the NHS: transforming the patient's experience of care*. London.
- Lilo, E., & Vose, C. (2016). *Mental health integration past, present and future: A report of national survey into mental health integration in England*. Retrieved from <https://www.basw.co.uk/resource/?id=4999>
- Lim, V. K. G. G., & Chen, D. J. Q. Q. (2012). Cyberloafing at the workplace: gain or drain on work? *Behaviour and Information Technology*, 31(4), 343–353. <https://doi.org/10.1080/01449290903353054>
- Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2011). Paradigmatic controversies, contradictions and emerging confluences, revisited. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research* (4th ed., pp. 97–128). Thousand Oaks, CA: Sage.
- Lingard, L., Albert, M., & Levinson, W. (2008). Grounded theory, mixed methods, and action research. *BMJ*, 337. Retrieved from <http://www.bmj.com/content/337/bmj.39602.690162.47>
- Linsley, P., Kane, R., & Owen, S. (2011). *Nursing for public health: promotion, principles and practice*. Oxford: Oxford University Press.
- Lippert, S. K. (2004). The effect of trust on personal web usage in the workplace. In M. Anandarajan & C. A. Simmers (Eds.), *Personal web usage in the workplace: a guide to effective human resources management* (pp. 80–110). Hershey, PA: Information Science Publishing.
- Lloyd, A. (2009). Informing practice: information experiences of ambulance officers in training and on-road practice. *Journal of Documentation*, 65(3), 396–419.
- Locke, K. (2008). *The practice of member review in qualitative research: what happens when they read what we write*. Williamsburg, VA: College of William and Mary.
- Locke, K., & Velamuri, S. R. (2008). The design of member review: showing what to organization members and why. *Organizational Research Methods*, 12(3), 488–509. <https://doi.org/10.1177/1094428108320235>
- Logan, D. (2010). What is information governance? And why is it so hard? Retrieved October 10, 2012, from http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/
- Lomas, E. (2010). Information governance: information security and access within a UK context. *Records Management Journal*, 20(2), 182–198. <https://doi.org/10.1108/09565691011064322>
- Lomas, J. (2007). The in-between world of knowledge brokering. *British Medical Journal*, 334(7585), 129–132.
- Lord, N. (2012). Common malware types: cybersecurity 101. Retrieved May 17, 2013, from <http://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101/>

- Lord, N. (2017). Communicating the data security risks of file sharing and cloud storage. Retrieved March 4, 2017, from <https://digitalguardian.com/blog/communicating-data-security-risks-file-sharing-cloud-storage>
- Lovaas, S. (2015). Web monitoring and content filtering. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (p. 31.1-31.15). Hoboken, NJ: Wiley. <https://doi.org/10.1002/9781118851678.ch31>
- Lowes, R. (2007). Can Google make you a better doctor? *Medical Economics*, 84(5), 24–5. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/17425271>
- Lui, K. (2013). The health informatics professional. In I. R. M. Association (Ed.), *User-driven healthcare: concepts, methodologies, tools, and applications (3 Volumes)* (pp. 120–141). Hershey, PA: IGI Global. Retrieved from <http://www.igi-global.com/book/user-driven-healthcare/69668>
- Lukes, S. (1974). *Power: a radical view*. Basingstoke: Macmillan. Retrieved from <http://www.myilibrary.com?id=85996>
- Lumsden, C. J., Byrne-Davis, L. M. T., Mooney, J. S., & Sandars, J. (2015). Using mobile devices for teaching and learning in clinical medicine. *Archives of Disease in Childhood. Education and Practice Edition*, 100(5), 244–251. <https://doi.org/10.1136/archdischild-2014-306620>
- Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, 24(1), 1–9. <https://doi.org/10.3233/THC-151102>
- Lupton, D. (2009). *Risk* (2nd ed.). Abingdon: Abingdon.
- Lutz, C. A. (2005). *From old maids to action heroes: librarians and the meanings of librarian stereotypes*. University of Maryland. Retrieved from <http://drum.lib.umd.edu/bitstream/1903/2670/1/umi-umd-2587.pdf>
- MacDonald, J. M. (2011). *The information sharing behaviour of health service managers: a three-part study*. University of Sheffield.
- MacDonald, J. M., Bath, P. A., & Booth, A. (2008). Healthcare managers' decision making: findings of a small scale exploratory study. *Health Informatics Journal*, 14(4), 247–58. <https://doi.org/10.1177/1460458208096554>
- MacDonald, J. M., Bath, P. A., & Booth, A. (2011). Information overload and information poverty: challenges for healthcare services managers? *Journal of Documentation*, 67(2), 238–263. <https://doi.org/10.1108/00220411111109458>
- MacIntosh-Murray, A., & Choo, C. W. (2005). Information behavior in the context of improving patient safety. *Journal of the American Society for Information Science and Technology*, 56(12), 1332–1345. <https://doi.org/10.1002/asi.20228>

- Maddock, S. (2002). Making modernisation work: new narratives, change strategies and people management in the public sector. *International Journal of Public Sector Management*, 15(1), 13–43.
- Mailley, J. (2011). *Engagement: the grey literature: what's known about engagement in the NHS, and what do we still need to find out?* Birmingham.
- Malaga, R. A. (2008). Worst practices in search engine optimization. *Communications of the ACM*, 51(12), 147–150.
- Malaga, R. A. (2010). Search engine optimization—black and white hat approaches. *Advances in Computers*, 78, 1–39. [https://doi.org/10.1016/S0065-2458\(10\)78001-3](https://doi.org/10.1016/S0065-2458(10)78001-3)
- Manning, M. Lou, Davis, J., Sparnon, E., & Ballard, R. M. (2013). iPads, droids, and bugs: Infection prevention for mobile handheld devices at the point of care. *American Journal of Infection Control*, 41(11), 1073–1076. <https://doi.org/10.1016/j.ajic.2013.03.304>
- Manojlovich, M. (2007). Power and empowerment in nursing: looking backward to inform the future. *Online Journal of Issues in Nursing*, 12(1), article 1. Retrieved from <http://www.nursingworld.org>
- Mansourian, Y. (2006). Adoption of grounded theory in LIS research. *New Library World*, 107(9/10), 386–402. <https://doi.org/10.1108/03074800610702589>
- Mansourian, Y., & Ford, N. (2007). Search persistence and failure on the web: a “bounded rationality” and “satisficing” analysis. *Journal of Documentation*, 63(5), 680–701. <https://doi.org/10.1108/00220410710827754>
- Marinos, L., & Sfakianakis, A. (2012). *ENISA threat landscape: responding to the evolving threat environment*. Heraklion, Greece.
- Mark, A. L. (2007). Modernising healthcare – is the NPfIT for purpose? *Journal of Information Technology*, 22(3), 248–256. <https://doi.org/10.1057/palgrave.jit.2000100>
- Markus, M. L. (1983). Power, politics, and MIS implementation. *Communications of the ACM*, 26(6), 430–444. Retrieved from <http://dl.acm.org/citation.cfm?id=358141.358148>
- Markus, M. L. (1987). Toward a “critical mass” theory of interactive media. *Communication Research*, 14(5), 191–511.
- Markus, M. L., & Bjørn-Andersen, N. (1987). Power over users: its exercise by system professionals. *Communications of the ACM*, 30(6), 498–504.
- Marshall, A. P., West, S. H., & Aitken, L. M. (2011). Preferred information sources for clinical decision making: critical care nurses’ perceptions of information accessibility and usefulness. *Worldviews on Evidence-Based Nursing / Sigma Theta Tau International, Honor Society of Nursing*, 8(4), 224–35. <https://doi.org/10.1111/j.1741-6787.2011.00221.x>
- Martin, J., Frost, P. J., & O’Neill, O. A. (2006). Organizational culture: beyond struggles for intellectual dominance. In S. R. Clegg, C. Hardy, T. B. Lawrence, & W. R. Nord (Eds.), *The Sage handbook of organization studies* (2nd ed., pp. 725–753). London: Sage.

- Mason, J. (2002). *Qualitative researching* (2nd ed.). London: Sage.
- Mason, J. (2003). Interview guide. In A. E. Bryman, T. F. Liao, & M. Lewis-Beck (Eds.), *The Sage encyclopedia of social science research methods* (pp. 518–519). Thousand Oaks, CA: Sage. Retrieved from http://books.google.co.uk/books?id=AB_JIZN-3j0C
- Matthews, J. I. (2009). *Power, management and complexity in the NHS: a Foucauldian perspective*. University of Glamorgan. Retrieved from [http://dspace1.isd.glam.ac.uk/dspace/bitstream/10265/435/3/Jean Matthews PhD Thesis Completed.pdf.txt](http://dspace1.isd.glam.ac.uk/dspace/bitstream/10265/435/3/Jean_Matthews_PhD_Thesis_Completed.pdf.txt)
- Maule, A. J. (2004). Translating management knowledge: the lessons to be learned from research on the perception and communication of risk. *Risk Management*, 6(2), 17–29. Retrieved from <http://www.jstor.org/discover/10.2307/3867694?uid=3738032&uid=2&uid=4&sid=21101304126907>
- Maurer, T. I. M., & Morgus, R. (2014). *Compilation of existing cybersecurity and information security related definitions*.
- May, E. (2014, December). Computer says no: NHS IT was not designed to operate at this level. *Healthcare Professionals Network | The Guardian*. Retrieved from <http://www.theguardian.com/healthcare-network/views-from-the-nhs-frontline/2014/dec/08/nhs-computer-technology-investment-operate#comment-44768551>
- May, V. (2010). *What to do with contradictory data?* (Realities toolkit No. 10). Southampton: ESRC National Centre for Research Methods. Retrieved from <http://eprints.ncrm.ac.uk/1322/1/12-toolkit-contradictory-data.pdf>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. Retrieved from <http://www.jstor.org/stable/258792>
- Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). Stakeholders in security policy development. In *Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, 5th - 7th December, 2011* (pp. 183–187). Perth. Retrieved from <http://ro.ecu.edu.au/ism/125>
- McAfee, A. P. (2006). Enterprise 2.0: the dawn of emergent collaboration. *MIT Sloan Management Review*, 47(3), 21–28. <https://doi.org/10.1109/EMR.2006.261380>
- McAfee, A. P. (2009). *Enterprise 2.0: new collaborative tools for your organization's toughest challenges*. Boston, MA: Harvard Business Press. Retrieved from <https://books.google.com/books?hl=en&lr=&id=Gqz3UF5FbI0C&pgis=1>
- McBeth, R. (2016a). HSCN connections available this summer. Retrieved February 18, 2016, from <http://www.digitalhealth.net/infrastructure/47163/hscn-connections-available-this-summer>
- McBeth, R. (2016b). John Newton: interview. Retrieved February 10, 2016, from <http://www.digitalhealth.net/features/47140/john-newton:-interview>

- McCarthy, P. (2013). Internet Explorer and CSS issues. Retrieved December 9, 2014, from <http://www.webcredible.com/blog-reports/css/internet-explorer.shtml>
- McClure, T. (2013). Security top concern in online file sharing and collaboration. Retrieved March 4, 2017, from <http://searchcloudstorage.techtarget.com/opinion/Security-top-concern-in-online-file-sharing-and-collaboration>
- McCormack, C. (2016). *Five stages of a web malware attack*. Abingdon. Retrieved from [https://www.sophos.com/en-us/medialibrary/Gated Assets/white papers/sophos-five-stages-of-a-web-malware-attack.pdf](https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophos-five-stages-of-a-web-malware-attack.pdf)
- McCreadie, M., & Rice, R. E. (1999a). Trends in analyzing access to information. Part I: cross-disciplinary conceptualizations of access. *Information Processing & Management*, 35(1), 45–76. [https://doi.org/10.1016/S0306-4573\(98\)00037-5](https://doi.org/10.1016/S0306-4573(98)00037-5)
- McCreadie, M., & Rice, R. E. (1999b). Trends in analyzing access to information. Part II. Unique and integrating conceptualizations. *Information Processing & Management*, 35(1), 77–99. [https://doi.org/10.1016/S0306-4573\(98\)00038-7](https://doi.org/10.1016/S0306-4573(98)00038-7)
- McDiarmid, M., Kendall, S., & Binns, M. (2007). Evidence-based administrative decision making and the Ontario hospital CEO: information needs, seeking behaviour, and access to sources. *Journal of the Canadian Health Libraries Association*, 28(2), 63–72. <https://doi.org/10.5596/c07-019>
- McElroy, L., & Weakland, E. (2013). *Measuring the effectiveness of security awareness programs*.
- McEvoy, P., & Richards, D. (2003). Critical realism: a way forward for evaluation research in nursing? *Journal of Advanced Nursing*, 43(4), 411–420. <https://doi.org/10.1046/j.1365-2648.2003.02730.x>
- McFadzean, E., Ezingard, J.-N., & Birchall, D. (2006). Anchoring information security governance research: sociological groundings and future directions. *Journal of Information System Security*, 2(3), 3–48.
- McGee, J. B., & Begg, M. (2008). What medical educators need to know about “Web 2.0”. *Medical Teacher*, 30(2), 164–9. <https://doi.org/10.1080/01421590701881673>
- McKenna, L., & McLelland, G. (2011). Midwives’ use of the Internet: an Australian study. *Midwifery*, 27(1), 74–9. <https://doi.org/10.1016/j.midw.2009.07.007>
- McLaughlin, J. (2001). EBM and risk: rhetorical resources in the articulation of professional identity. *Journal of Management in Medicine*, 15(5), 352–363.
- McMenemy, D. (2008). Internet access in UK public libraries: notes and queries from a small scale study. *Library Review*, 57(7), 485–489. <https://doi.org/10.1108/00242530810894004>
- McSherry, R., & Haddock, J. (1999). Evidence-based health care: its place within clinical governance. *British Journal of Nursing (Mark Allen Publishing)*, 8(2), 113–7. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/10214142>
- Meek, T. (2015a). Hunt approves HSCN: N3 replacement. Retrieved February 15, 2016, from <http://www.digitalhealth.net/infrastructure/46861/hunt-approves-hscn-n3-replacement>

- Meek, T. (2015b). Kelsey pushes for free NHS wi-fi. Retrieved April 9, 2015, from <http://www.ehi.co.uk/news/EHI/9930/kelsey-pushes-for-free-nhs-wi-fi>
- Meek, T. (2015c). NHS to switch ESR to IBM in June. Retrieved April 22, 2015, from <http://www.ehi.co.uk/news/industry/9965/nhs-to-switch-esr-to-ibm-in-june>
- Merrifield, N. (2015, October). Digital expert warns district nurses not to ignore technology skills. *Nursing Times*. Retrieved from <http://www.nursingtimes.net/roles/district-and-community-nurses/digital-expert-warns-district-nurses-not-to-ignore-technology-skills/5082508.article>
- Meyer, C. B. (2001). A case in case study methodology. *Field Methods*, 13(4), 329–352.
- Mickan, S., Atherton, H., Roberts, N. W., Heneghan, C., & Tilson, J. K. (2014). Use of handheld computers in clinical practice: a systematic review. *BMC Medical Informatics and Decision Making*, 14(1), 56. <https://doi.org/10.1186/1472-6947-14-56>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: a methods sourcebook* (3rd ed.). Thousand Oaks, CA: Sage. Retrieved from <http://www.amazon.com/Qualitative-Data-Analysis-Methods-Sourcebook/dp/1452257876>
- Millar, S. (2016). *A cyber security risk assessment of hospital infrastructure including TLS / SSL and other threats*. Belfast. Retrieved from http://pure.qub.ac.uk/portal/files/125120790/StuartMillar13616005_ACyberSecurityRiskAssesmentOfHospitalInfrastructure_TLS.pdf
- Mingers, J. (2000). The contribution of critical realism as an underpinning philosophy for OR/MS and systems. *Journal of the Operational Research Society*, 51(11), 1256–1270. <https://doi.org/10.1057/palgrave.jors.2601033>
- Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. *Information Systems Research*, 23(3), 240–259.
- Mingers, J. (2003). The paucity of multimethod research: a review of the information systems literature. *Information Systems Journal*, 13, 233–249.
- Mingers, J. (2004a). Paradigm wars: ceasefire announced who will set up the new administration? *Journal of Information Technology*, 19(3), 165–171. <https://doi.org/10.1057/palgrave.jit.2000021>
- Mingers, J. (2004b). Re-establishing the real: critical realism and information systems. In J. Mingers & L. Willcocks (Eds.), *Social theory and philosophy for information systems* (p. 455). Chichester: Wiley.
- Mingers, J. (2004c). Real-izing information systems: critical realism as an underpinning philosophy for information systems. *Information and Organization*, 14(2), paper 27. <https://doi.org/10.1016/j.infoandorg.2003.06.001>
- Mingers, J., Mutch, A., & Willcocks, L. (2013). Critical realism in information systems research: basic concepts. *MIS*, 37(3), 795–802.

- Mirchandani, D., & Motwani, J. (2003). Reducing internet abuse in the workplace. *SAM Advanced Management Journal*, 68(1). Retrieved from <http://www.freepatentsonline.com/article/SAM-Advanced-Management-Journal/98831088.html>
- Monitor. (2014). *Detailed requirements for quality reports*. London. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/406537/Detailed_req_for_qual_repts_update24feb.pdf
- Moore-Colyer, R. (2016). Health secretary Jeremy Hunt commits £4bn to NHS tech investment. Retrieved February 8, 2016, from <http://www.computing.co.uk>
- Moore, S., & Jayewardene, D. (2014). The use of smartphones in clinical practice. *Nursing Management*, 21(4), 18–22. Retrieved from <http://journals.rcni.com/doi/abs/10.7748/nm.21.4.18.e1225>
- Moorhead, S. A., Hazlett, D. E., Harrison, L., Carroll, J. K., Irwin, A., & Hoving, C. (2013). A new dimension of health care: systematic review of the uses, benefits, and limitations of social media for health communication. *Journal of Medical Internet Research*, 15(4), e85. <https://doi.org/10.2196/jmir.1933>
- Moorley, C., & Chinn, T. (2014). Using social media for continuous professional development. *Journal of Advanced Nursing*. <https://doi.org/10.1111/jan.12504>
- Morey, N. C., & Luthans, F. (1984). Emic perspective and ethnoscience methods for organizational research. *Academy of Management Review*, 9(1), 27–36.
- Mort, D. (2006). Online passes print in STM publishing. *Research Information*, (August-September). Retrieved from <http://www.researchinformation.info/riaugsep06analysis.html>
- Moscovici, S. (1988). Notes towards a description of social representations. *European Journal of Social Psychology*, 18(January), 211–250. <https://doi.org/10.1002/ejsp.2420180303>
- Moule, P., Ward, R., & Lockyer, L. (2010). Issues with e-learning in nursing and health education in the UK: are new technologies being embraced in the teaching and learning environments? *Journal of Research in Nursing*, 16(1), 77–90. <https://doi.org/10.1177/1744987110370940>
- Mulgan, G., & Albury, D. (2003). *Innovation in the public sector* (No. version 1.9). Strategy Unit, Cabinet Office. London. <https://doi.org/10.1057/9780230307520>
- Munn, M. (2011). *Unlocking potential - perspectives on women in science, engineering and technology*. London.
- Munson, S. A., Cavusoglu, H., Frisch, L., & Fels, S. (2013). Sociotechnical challenges and progress in using social media for health. *Journal of Medical Internet Research*, 15(10), e226. <https://doi.org/10.2196/jmir.2792>
- Murdoch, S. J., & Anderson, R. (2008). Tools and technology of internet filtering. In R. R. and J. Z. Ronald Deibert, John Palfrey (Ed.), *Access denied: the practice and policy of global internet filtering* (pp. 57–72). Boston, MA: MIT Press.

- Murray, I., & Savin-Baden, M. (2000). Staff development in problem-based learning. *Teaching in Higher Education*, 5(1), 107–126. <https://doi.org/10.1080/135625100114993>
- Mutch, A. (2002). Actors and networks or agents and structures: towards a realist view of information systems. *Organization*, 9(3), 477–496.
- Mutch, A. (2010). Technology, organization, and structure--a morphogenetic approach. *Organization Science*, 21(2), 507–520. Retrieved from <https://doi.org/10.1287/orsc.1090.0441>
- Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly*, 21(2), 241–242.
- Myers, M. D., & Klein, H. K. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly*, 35(1), 17–36.
- Nail-Chiwetalu, B., & Ratner, N. B. (2007). An assessment of the information-seeking abilities and needs of practicing speech-language pathologists. *Journal of the Medical Library Association*, 95(2), 182.
- National Advisory Group on the Safety of Patients in England. (2013). *A promise to learn - a commitment to act: improving the safety of patients in England*. London.
- National Information Board. (2014a). National Information Board Terms of Reference November 2014. London: National Information Board.
- National Information Board. (2014b). *Personalised health and care 2020: using data and technology to transform outcomes for patients and citizens*. London.
- National Information Board. (2016). *Annual report*. London. <https://doi.org/10.1039/C1DT90165F>
- National Library for Health. (2009, March). Celebrating 10 years of National Library for Health. *National Library for Health News*, 1(10), 1–11. Retrieved from http://web.archive.org/web/20101126073557/http://library.nhs.uk/nlhdocs/nlh_newsletter_march_09_vol1_iss_10_v2.pdf
- National Pharmacy Association. (2016). Patient safety incidents. Retrieved March 2, 2017, from <https://www.npa.co.uk/news-and-events/news-item/patient-safety-incident-mso-report-january-march-2016/>
- National Quality Board. (2011). *Quality governance in the NHS*. London.
- Neergaard, H. (2006). Sampling in entrepreneurial settings. In H. Neergaard & J. P. Ulhøi (Eds.), *Handbook of qualitative research methods in entrepreneurship* (pp. 314–337). Cheltenham: Edward Elgar. <https://doi.org/10.4337/9781847204387>
- Ngwenyama, O. K. (1991). The critical social theory approach to information systems: problems and challenges. In H.-E. Nissen, H. K. Klein, & R. Hirschheim (Eds.), *Information systems research: contemporary approaches and emergent traditions: proceedings of the IFIP TC8/WG 8.2 working conference on the information systems research arena of the 90's: challenges, perceptions, and alternative approaches* (pp. 267–280). Copenhagen: North-Holland.

- NHS Choices. (2012). MRSA rates fall, but other infections emerge. Retrieved March 12, 2015, from <http://www.nhs.uk/news/2012/05may/Pages/mrsa-hospital-acquired-infection-rates.aspx>
- NHS Choices (2016). The structure of the NHS in England.
- NHS Commissioning Board. (2011). Commissioning support: key facts. London: NHS Commissioning Board.
- NHS Confederation. (2014). Framework for action published by the National Information Board. Retrieved January 24, 2017, from <http://www.nhsconfed.org/resources/2014/12/framework-for-action-published-by-the-national-information-board>
- NHS Confederation. (2016). Key statistics on the NHS. Retrieved January 24, 2017, from <http://www.nhsconfed.org/resources/key-statistics-on-the-nhs>
- NHS Connecting for Health. (2007). *NHS information security management: code of practice*. Leeds. Retrieved from <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/securitycode.pdf>
- NHS East of England. (2009). East of England e-learning strategy. Cambridge: NHS East of England.
- NHS Electronic Staff Record Programme. (2014). Future development of ESR. Retrieved April 22, 2015, from <http://www.esrnews.nhs.uk/spring-2014/latest-news/future-development-of-esr>
- NHS Employers. (2013a). HR and social media in the NHS: an essential guide for HR directors and managers. London: NHS Employers.
- NHS Employers. (2013b). Increasing staff engagement with social media. London: NHS Employers. Retrieved from <http://www.nhsemployers.org>
- NHS Employers. (2013c). Social media for chief executives : the essential guide. London: NHS Employers. Retrieved from <http://www.nhsemployers.org>
- NHS Employers. (2013d). Social media guidelines. Retrieved February 13, 2014, from <http://www.nhsemployers.org>
- NHS Employers. (2014). *A social media toolkit for the NHS*. London.
- NHS Employers. (2017). Making best use of your survey data - a quick guide. Retrieved February 6, 2017, from <http://www.nhsemployers.org/your-workforce/retain-and-improve/staff-experience/staff-engagement/the-nhs-staff-survey/making-best-use-of-your-staff-survey-data-a-quick-guide>
- NHS England. (s.d.). Academic Health Science Networks. Retrieved January 7, 2017, from <https://www.england.nhs.uk/ourwork/part-rel/ahsn/>
- NHS England. (2013a). *Safer hospitals safer wards: achieving an integrated digital care record*. London.
- NHS England. (2013b). *Social media and attributed digital media policy and corporate procedures*. Leeds. Retrieved from <http://www.england.nhs.uk/wp-content/uploads/2013/09/pat-1001-social-media-policy.pdf>

- NHS England. (2014a). *Five year forward view*. Redditch: NHS England. Retrieved from <http://www.england.nhs.uk/ourwork/futurenhs/>
- NHS England. (2014b). *Information governance policy*. London. Retrieved from <http://www.england.nhs.uk/wp-content/uploads/2013/06/ig-policy-1.1.pdf>
- NHS England. (2015). Martha Lane Fox sets out key digital proposals for the NHS. Retrieved January 29, 2016, from <https://www.england.nhs.uk/2015/12/martha-lane-fox/>
- NHS Executive. (1998). *Information for health: an information strategy for the modern NHS 1998-2005*. Retrieved January 21, 2013, from http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4014469.pdf
- NHS Executive. (1999). *Governance in the New NHS: Background Information and Guidance on the Development and Implementation of Controls Assurance for 1999/2000*. Leeds.
- NHS Litigation Authority. (2013). *NHSLA risk management standards 2013-14*. London: NHS Litigation Authority.
- NHS National Workforce Group. (2005). *Supporting best practice in e-learning across the NHS: a strategic framework*. Preston.
- NHS Networks. (2013). *Obsolete browsers - how to get action?* Retrieved May 30, 2013, from http://www.networks.nhs.uk/discussion/a-lifeboat-for-nhs-managers/228746657?b_start=0#357896610
- NHS Staff Council. (s.d.). *Simplified knowledge and skills framework (KSF)*. Retrieved September 8, 2015, from <http://www.nhsemployers.org/your-workforce/retain-and-improve/managing-your-workforce/appraisals/simplified-ksf>
- Nicoletti, P. (2009). Content filtering. In J. Vacca (Ed.), *Computer and information security handbook* (pp. 723–744). Burlington, MA: Elsevier. <https://doi.org/10.1016/B978-0-12-374354-1.00042-X>
- Niedźwiedzka, B. (2003). Barriers to evidence-based decision making among Polish healthcare managers. *Health Services Management Research : An Official Journal of the Association of University Programs in Health Administration / HSMC, AUPHA*, 16(2), 106.
- Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. *European Journal of Information Systems*, 21(6), 592–607. Retrieved from <http://dx.doi.org/10.1057/ejis.2012.3>
- Noordegraaf, M. (2007). From “pure” to “hybrid” professionalism. *Administration and Society*, 39(6), 761–785.
- Noordegraaf, M. (2013). Reconfiguring professional work: changing forms of professionalism in public services. *Administration & Society*, 95399713509242. <https://doi.org/10.1177/0095399713509242>
- Nord, J., & Nord, G. (2007). IT culture: its impact on communication and work relationships in business. *International Journal of Intercultural Information Management*, 1(1), 85–107.

- Nurse, J. R. C. (2013). Effective communication of cyber security risks. In *Security and Protection of Information 2013* (pp. 75–82).
- Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011*, 60–68.
<https://doi.org/10.1109/STAST.2011.6059257>
- Nursing and Midwifery Council. (s.d.). Social networking sites. Retrieved April 1, 2013, from <http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Social-networking-sites/>
- Nursing and Midwifery Council. (2008). The code: standards of conduct, performance and ethics for nurses and midwives. London: Nursing and Midwifery Council.
- Nursing and Midwifery Council. (2011). The PREP handbook. London: Nursing and Midwifery Council.
- Nursing and Midwifery Council. (2015a). Guidance on using social media responsibly. London: Nursing and Midwifery Council.
- Nursing and Midwifery Council. (2015b). The code: professional standards of practice and behaviour for nurses and midwives. London: Nursing and Midwifery Council.
- O’Reilly, T. (2005). *What is Web 2.0: design patterns and business models for the next generation of software* (No. 4578). O’Reilly Network. Munich. Retrieved from http://mpira.ub.uni-muenchen.de/4578/1/MPRA_paper_4578.pdf
- O’Carroll, A. M., Westby, E. P., Dooley, J., & Gordon, K. E. (2015). Information-seeking behaviors of medical students: A cross-sectional web-based survey. *JMIR Medical Education*, 1(1), e4.
<https://doi.org/10.2196/mededu.4267>
- O’Connell, B. M. (2005). Electronic monitoring in the American academy. In J. Weckert (Ed.), *Electronic monitoring in the workplace: controversies and solutions* (pp. 171–207). Hershey, PA: IGI Global.
- O’Connor, L. (2009). Information literacy as professional legitimation: the quest for a new jurisdiction. *Library Review*, 58(7), 493–508. <https://doi.org/10.1108/00242530910978190>
- O’Leary, D. F., & Ni Mhaolrúnaigh, S. (2012). Information-seeking behaviour of nurses: where is information sought and what processes are followed? *Journal of Advanced Nursing*, 68(2), 379–90. <https://doi.org/10.1111/j.1365-2648.2011.05750.x>
- Oakley, M., & Spallek, H. (2012). Social media in dental education: a call for research and action. *Journal of Dental Education*, 76(3), 279–87. Retrieved from <http://www.pubmedcentral.nih.gov>
- Ofcom. (2014). *Building materials and propagation*. London. Retrieved from <http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2014/buildingmaterials/>

- Ofsted. (2010). Students safest using the internet when they are trusted to manage their own risk. Retrieved July 17, 2014, from <http://www.ofsted.gov.uk/news/students-safest-using-internet-when-they-are-trusted-manage-their-own-risk>
- Olijnyk, N. V. (2015). A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. *Scientometrics*, *105*(2), 883–904. <https://doi.org/10.1007/s11192-015-1708-1>
- Oliveira, J. P. F. F. C. (2010). *Power and organisational change: a case study*. University of Dundee.
- Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, *14*(1), 110–121.
- Oliver, G. (2006). Investigating information culture: a comparative case study research design and methods. *Archival Science*, *4*(3–4), 287–314. <https://doi.org/10.1007/s10502-005-2596-6>
- Oltsik, J. (2013). *Endpoint security demands defense-in-depth and advanced analytics*. Milford, MA. Retrieved from www.esg-global.com
- Oost, D. (2010). A potential loss of trust as a result of the conflicting messages within information security research. In *2010 IEEE International Symposium on Technology and Society* (pp. 213–219). IEEE. <https://doi.org/10.1109/ISTAS.2010.5514635>
- Oppliger, R. (2015). Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale. *IEEE Security & Privacy*, *13*(6), 18–21. <https://doi.org/10.1109/MSP.2015.118>
- Oravec, J. A. (2002). Constructive approaches to internet recreation in the workplace. *Communications of the ACM*, *45*(1), 60–63. <https://doi.org/10.1145/502269.502298>
- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: research approaches and assumptions. *Information Systems Research*, *2*(1), 1–28. <https://doi.org/10.1287/isre.2.1.1>
- Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems*, *12*(2), 174–207. <https://doi.org/10.1145/196734.196745>
- Osch, W. van, & Coursaris, C. K. (2013). Organizational social media: a comprehensive framework and research agenda. In *2013 46th Hawaii International Conference on System Sciences* (pp. 700–707). Kauai, HI: IEEE. <https://doi.org/10.1109/HICSS.2013.439>
- Osch, W. van, & Coursaris, C. K. (2015). A meta-analysis of theories and topics in social media research. In *2015 48th Hawaii International Conference on System Sciences* (pp. 1668–1675). Kauai, HI: IEEE. <https://doi.org/10.1109/HICSS.2015.201>
- Ozdalga, E., Ozdalga, A., & Ahuja, N. (2012). The smartphone in medicine: a review of current and potential use among physicians and students. *Journal of Medical Internet Research*, *14*(5), e128. <https://doi.org/10.2196/jmir.1994>

- Özel, H. (2002). Closing the open systems: the “double hermeneutics” in economics. In *International Congress in Economics VI* (Vol. 1, pp. 1–32). Ankara.
<https://doi.org/10.1017/CBO9781107415324.004>
- Palo Alto Networks. (2009). *To block or not. Is that the question?* Sunnyvale, CA.
- Parker, M. (2005). False dichotomies: EBM, clinical freedom, and the art of medicine. *Medical Humanities*, 31(1), 23–30. <https://doi.org/10.1136/jmh.2004.000195>
- Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human factors and information security: individual, culture and security environment*. Edinburgh, South Australia.
- Patel, R. K., Sayers, A. E., Patrick, N. L., Hughes, K., Armitage, J., & Hunter, I. A. (2015). A UK perspective on smartphone use amongst doctors within the surgical profession. *Annals of Medicine and Surgery*, 4(2), 107–112. <https://doi.org/10.1016/j.amsu.2015.03.004>
- Pather, S., & Remenyi, D. (2004). Some of the philosophical issues underpinning research in information systems: from positivism to critical realism. In *SAICSIT* (pp. 141–146). South African Institute for Computer Scientists and Information Technologists. Retrieved from <http://dl.acm.org/citation.cfm?id=1035053.1035070>
- Paton, C., Bamidis, P. D., Eysenbach, G., Hansen, M., & Cabrer, M. (2011). Experience in the use of social media in medical and health education. Contribution of the IMIA Social Media Working Group. *Yearbook of Medical Informatics*, 6(1), 21–9. Retrieved from <http://europepmc.org/abstract/MED/21938320>
- Paton, S., Hodgson, D., & Muzio, D. (2013). The price of corporate professionalisation: analysing the corporate capture of professions in the UK. *New Technology, Work and Employment*, 28, 227–240. <https://doi.org/10.1111/ntwe.12014>
- Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: Sage. Retrieved from <http://books.google.com/books?id=FjBw2oi8E14C&pgis=1>
- Payne, D., Arkle, S., Gallagher, J., Lawson, S., Richardson, J., Smith, L., & Stephan, K. (2016). *Content filtering in UK public libraries*. s.l.: Figshare. <https://doi.org/10.6084/M9.FIGSHARE.2059998.V2>
- Payne, K. F. B., Wharrad, H., & Watts, K. (2012). Smartphone and medical related app use among medical students and junior doctors in the United Kingdom (UK): a regional survey. *BMC Medical Informatics and Decision Making*, 12(1), 121. <https://doi.org/10.1186/1472-6947-12-121>
- Pettigrew, K. E., Fidel, R., & Bruce, H. (2001). Conceptual frameworks in information behavior. *Annual Review of Information Science and Technology*, 35, 43–78.
- Pfleeger, S. L., & Caputo, D. D. (2012). *Leveraging behavioral science to mitigate cyber security risk*. McLean, VA. Retrieved from https://www.mitre.org/sites/default/files/pdf/12_0499.pdf
- Phillips, R. (2013). Beyond connected healthcare: BYOD and the NHS. Retrieved November 10, 2014, from <http://letstalk.globalservices.bt.com/en/2013/07/beyond-connected-healthcare-byod-and-the-nhs/>

- Pickard, A. J. (2007). *Research methods in information*. London: Facet Publishing.
- Pidgeon, N. (1998). Risk assessment, risk values and the social science programme: why we do need risk perception research. *Reliability Engineering and System Safety*, 59, 5–15.
- Pitt, L. F., Watson, R. T., & Kavan, C. B. (1995). Service quality: a measure of information systems effectiveness. *MIS Quarterly*, 19(2), 173. <https://doi.org/10.2307/249687>
- Ploeg, J. (1999). Identifying the best research design to fit the question. Part 2: qualitative designs. *Evidence-Based Nursing*, 2(2), 36–37. <https://doi.org/10.1136/ebn.2.2.36>
- Podichetty, V. K., Booher, J., Whitfield, M., & Biscup, R. S. (2006). Assessment of internet use and effects among healthcare professionals: a cross sectional survey. *Postgraduate Medical Journal*, 82, 274–279.
- Pomerantz, J., Hank, C., & Sugimoto, C. R. (2015). The state of social media policies in higher education. *PloS One*, 10(5), 1–18. <https://doi.org/10.7290/V70Z7156.Funding>
- Pomerol, J.-C., & Adam, F. (2008). Understanding the legacy of Herbert Simon to decision support systems. In *Encyclopedia of Decision Making and Decision Support Technologies* (pp. 930–938). Hershey, PA: IGI Global. <https://doi.org/10.4018/978-1-59904-843-7.ch105>
- Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers and Security*, 30(6–7), 486–497. <https://doi.org/10.1016/j.cose.2011.05.002>
- Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: restricting access can interfere with user tasks. *Computers and Security*, 26(3), 229–237. <https://doi.org/10.1016/j.cose.2006.10.004>
- Potter, L. E. (2007). *The information technology gap: exploring the factors that potentially separate and differentiate IT professionals and users*. Griffith University.
- Poulter, T., & Bath, P. A. (2012). The use and usability of EPR systems in oncology. *Studies in Health Technology and Informatics*, 180(August), 398–402. <https://doi.org/10.3233/978-1-61499-101-4-398>
- Powell, M. (2016). *Leadership in the NHS: thoughts of a newcomer*. London. Retrieved from http://www.kingsfund.org.uk/sites/files/kf/field/field_publication_file/Thoughts_of_a_Newcomer.pdf
- Prabha, C., Connaway, L. S., Olszewski, L., Jenkins, L. R., Silipigni Connaway, L., Olszewski, L., & Jenkins, L. R. (2007). What is enough? Satisficing information needs. *Journal of Documentation*, 63(1), 74–89. <https://doi.org/10.1108/00220410710723894>
- Price, R., & Cook, J. (2015). Europe's highest court just rejected the "safe harbor" agreement used by American tech companies. Retrieved October 7, 2015, from <http://uk.businessinsider.com/european-court-of-justice-safe-harbor-ruling-2015-10>
- Prince, N. J., Cass, H. D., & Klaber, R. E. (2010). Accessing e-learning and e-resources. *Medical Education*, 44(436–437).

- Prior, L. (2003). *Using documents in social research*. London: Sage.
- Prior, L. (2008). Repositioning documents in social research. *Sociology*, 42(5), 821–836. <https://doi.org/10.1177/0038038508094564>
- Prior, L. (2010). Documents in health research. In Ivy Bourgeault, R. Dingwall, & R. de Vries (Eds.), *The Sage handbook of qualitative methods in health research* (pp. 417–433). London: Sage.
- Proctor, W. R. (2016). *Investigating the efficacy of cybersecurity awareness training programs*. Utica College. Retrieved from <http://gradworks.umi.com/10/10/10103886.html>
- Provos, N., Mavrommatis, P., Rajab, M. A., & Monrose, F. (2008). All your iFRAMEs point to us. In *17th USENIX Security Symposium*. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/summary;jsessionid=D8E4407A21C1DE270A6FAB15106FFBF3?doi=10.1.1.117.2290>
- Provos, N., McNamee, D., Mavrommatis, P., Wang, K., & Modadugu, N. (2007). The ghost in the browser: analysis of web-based malware. In *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets* (p. 9pp.).
- Provos, N., Rajab, M. A., & Mavromattis, P. (2009). Cybercrime 2.0: when the cloud turns dark. *ACM Queue*, 46–53. <https://doi.org/10.1145/950566.950578>
- Publish. (2016). Retrieved May 10, 2016, from <http://www.businessdictionary.com/definition/publish.html>
- Puhakainen, P., & Siponen, M. T. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly: Management Information Systems*, 34(4), 757–778. <https://doi.org/Article>
- Purcell, J. (2014). Disengaging from engagement. *Human Resource Management Journal*, 24(3), 241–254. <https://doi.org/10.1111/1748-8583.12046>
- Pye, J., & Ball, D. (1999). *Library purchasing consortia in the UK: activity, benefits and good practice. Final Report of BLRIC Research Project RIC/G/403*. Bournemouth.
- Quam, L., & Smith, R. (2005). What can the UK and US health systems learn from each other? *BMJ (Clinical Research Ed.)*, 330(7490), 530–3. <https://doi.org/10.1136/bmj.330.7490.530>
- Quigley, K., Burns, C., & Stallard, K. (2015). “Cyber gurus”: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, 32(2), 108–117. <https://doi.org/10.1016/j.giq.2015.02.001>
- Radicati Group. (2012). *Corporate web security - market quadrant 2012: an analysis of the market for corporate web security solutions, revealing top players, mature players, specialists and trail blazers*. Palo Alto, CA. Retrieved from <http://www.websense.com/assets/white-papers/corporate-Web-Security-Market-Quadrant-2012.pdf>

- Radulescu, C., & Vessey, I. (2009). Methodology in critical realist research: the mediating role of domain specific theory. In *AMCIS 2009 Proceedings*. AIS Electronic Library. Retrieved from <http://aisel.aisnet.org/amcis2009/433>
- Rains, T. (2011). What you should know about drive-by download attacks – Part 1. Retrieved March 6, 2017, from <https://blogs.microsoft.com/microsoftsecure/2011/12/08/what-you-should-know-about-drive-by-download-attacks-part-1/>
- Ramachandran, S., & Rao, S. V. (2006). An effort towards identifying occupational culture among information systems professionals. In *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research: forty four years of computer personnel research: achievements, challenges & the future* (p. 198). New York: ACM Press.
<https://doi.org/10.1145/1125170.1125221>
- Ramos, K., Linscheid, R., & Schafer, S. (2003). Real-time information-seeking behavior of residency physicians. *Family Medicine*, 35(4), 257–260.
- Ranadive, A., Demir, T., Rizvi, S., & Daswani, N. (2010). Malware distribution via widgetization of the web. In *Blackhat*. San Francisco, CA: Black Hat. Retrieved from http://media.blackhat.com/bh-dc-11/Daswani/BlackHat_DC_2011_Daswani_Malware_Dist-wp.pdf
- Randell, R., Mitchell, N., Thompson, C., McCaughan, D., & Dowding, D. (2009). From pull to push: understanding nurses' information needs. *Health Informatics Journal*, 15(2), 75–85.
<https://doi.org/10.1177/1460458209102969>
- Rao, V., & Ramachandran, S. (2011). Occupational cultures of information systems personnel and managerial personnel: potential conflicts. In *Communications of the Association for Information Systems* (Vol. 29). Retrieved from <http://aisel.aisnet.org/cais/vol29/iss1/31>
- Rastogi, R., & von Solms, R. (2012). Information security service culture – information security for end-users. *Journal of Universal Computer Science*, 18(12), 1628–1642.
- Raynor, M. (2009). Access all areas: exploring the use of library and IT facilities by University of Salford pre-registration diploma nurses during periods of clinical practice placement. *Evidence Based Library and Information Practice*, 4(3), 4–18.
- Read, I. (2010). N3 network user guide version 1.3. London: British Telecommunications plc.
- Reddy, M. C., & Dourish, P. (2002). A finger on the pulse: temporal rhythms and information seeking in medical work. In *Proceedings of the ACM Conference on Computer Supported Collaborative Work CSCW* (Vol. Proceeding, pp. 344–353). New Orleans, LA: ACM.
<https://doi.org/10.1145/587078.587126>
- Reece, R. P., & Stahl, B. C. (2015). The professionalisation of information security: perspectives of UK practitioners. *Computers & Security*, 48, 182–195. <https://doi.org/10.1016/j.cose.2014.10.007>
- Reed, J., & Procter, S. (Eds.). (1995). *Practitioner research in health care*. London: London : Chapman & Hall, 1995.

- Reed, M. (2005). Reflections on the “realist turn” in organization and management studies. *Journal of Management Studies*, 42(8), 1921–1644.
- Reeves, S., Kuper, A., & Hodges, B. D. (2008). Qualitative research methodologies: ethnography. *BMJ*, 337. Retrieved from <http://www.bmj.com/content/337/bmj.a1020>
- Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cybersecurity. In *Cyber-risk management* (pp. 29–32). Springer International Publishing. <https://doi.org/10.1007/978-3-319-23570-7>
- Reid, M. F., Allen, M. W., Armstrong, D. J., & Riemenschneider, C. K. (2010). Perspectives on challenges facing women in IS: the cognitive gender gap. *European Journal of Information Systems*, 19(5), 526–539. <https://doi.org/10.1057/ejis.2010.30>
- Reisinger, D. (2011). Internet Explorer 6 must die quickly: 10 reasons why. Retrieved May 30, 2013, from <http://www.eweek.com/c/a/Security/Internet-Explorer-6-Must-Die-Quickly-10-Reasons-Why-472583/>
- Renaud, K. (2012). Blaming noncompliance is too convenient: what really causes information breaches? Why people don’t comply. *IEEE Security and Privacy*, (June), 57–63.
- Renaud, K., & Goucher, W. (2012). Health service employees and information security policies : an uneasy partnership? *Information Management and Computer Security*, 20(4), 296–311. <https://doi.org/10.1108/09685221211267666>
- Renn, O. (2008). Concepts of risk: an interdisciplinary review. Part 2: integrative approaches. *Gaia*, 17(2), 196–204.
- Rensleigh, C. W. (2002). Controlling Internet abuse through effective content filtering: a higher education implementation. *South African Journal of Information Management*, 4(4).
- Rentrop, C., & Zimmermann, S. (2012). Shadow IT-management and control of unofficial IT. *ICDS 2012, The Sixth International Conference on Digital Society*, (October 2015), 98–102. Retrieved from <http://www.thinkmind.org>
- Resnick, P. J., Hansen, D. L., & Richardson, C. R. (2004). Calculating error rates for filtering software. *Communications of the ACM*, 47(9), 67–71. Retrieved from <http://presnick.people.si.umich.edu/healthfiltering/CACM.pdf>
- Rey, T. (2016). Digital communications policies (July 28) [Electronic mailing list message]. Retrieved from <http://www.jiscmail.ac.uk/lis-medical>
- Richardson, C. R., Resnick, P. J., Hansen, D. L., Derry, H. A., & Rideout, V. J. (2002). Does pornography-blocking software block access to health information on the Internet? *JAMA*, 288(22), 2887–2894.
- Rideout, V., Richardson, C., & Resnick, P. (2002). *See no evil: how Internet filters affect the search for online health information*. Menlo Park, CA. Retrieved from http://www.kff.org/content/2002/3294/Internet_Filtering_exec_summ.pdf
- Rippl, S. (2002). Cultural theory and risk perception: a proposal for a better measurement. *Journal of Risk Research*, 5(2), 147–165. <https://doi.org/10.1080/1366987011004259>

- Ritchie, J., Lewis, J., Elam, G., Tennant, R., & Rahim, N. (2014). Designing and selecting samples. In J. Ritchie, J. Lewis, C. McNaughton Nicholls, & R. Ormston (Eds.), *Qualitative research practice: a guide for social science students and researchers* (2nd ed., pp. 111–145). London: Sage.
- Ritchie, J., & Spencer, L. (1994). Qualitative data analysis for applied policy research. In *Analysing qualitative data* (pp. 173–194). London: Routledge.
- Roberts, P. M., & Priest, H. (2010). *Healthcare research: a handbook for students and practitioners*. Chichester: Wiley.
- Robertson, A., Cresswell, K., Takian, A., Petrakaki, D., Crowe, S., Cornford, T., ... Sheikh, A. (2010). Implementation and adoption of nationwide electronic health records in secondary care in England: qualitative analysis of interim results from a prospective national evaluation. *BMJ (Clinical Research Ed.)*, *341*(sep01_3), c4564. <https://doi.org/10.1136/bmj.c4564>
- Robey, D., & Markus, M. L. (1984). Rituals in information system design. *MIS Quarterly*, *8*(1), 5–15.
- Robinson, D., Perryman, S., & Hayday, S. (2004). *The drivers of employee engagement*. North (Vol. 408). London. Retrieved from http://www.managingpeople4profit.com/uploads/2/8/1/6/2816853/www-employment-studies-co-uk_drivers_of_engagement.pdf
- Rodrigues, R., & Druschel, P. (2010). Peer-to-peer systems. *Communications of the ACM*, *53*(10), 72. <https://doi.org/10.1145/1831407.1831427>
- Rogers, E. M. (2003). *Diffusion of Innovations Theory* (5th ed.). New York: Free Press. Retrieved from https://www.utwente.nl/cw/theorieenoverzicht/theory_clusters/communication_and_information_technology/diffusion_of_innovations_theory/
- Roiter, N. (2007). Web security gateways meet rising malware threats. Retrieved June 5, 2013, from <http://searchsecurity.techtarget.com/news/1263882/Web-security-gateways-meet-rising-malware-threats#.Ua9EZjvdwLY.mendeley>
- Rose, J. D. (2011). Diverse perspectives on the groupthink theory – a literary review. *Emerging Leadership Journeys*, *4*(1), 37–57. Retrieved from http://www.regent.edu/acad/global/publications/elj/vol4iss1/Rose_V4i1_pp37-57.pdf
- Roulston, K. (2010). Considering quality in qualitative interviewing. *Qualitative Research*, *10*(2), 199–228. <https://doi.org/10.1177/1468794109356739>
- Rouse, M. (2006). What is social engineering? - definition from WhatIs.com. Retrieved May 31, 2013, from <http://searchsecurity.techtarget.com/definition/social-engineering#.Uahk5ASHjBs.mendeley>
- Rouse, M. (2007). Pharming. Retrieved June 4, 2013, from <http://searchsecurity.techtarget.com/definition/pharming>
- Rowlands, I., Nicholas, D., Brown, D., & Williams, P. (2011). Access to scholarly content: gaps and barriers to access. *Serials*, *24*2(December), 123–136.

- Royal Berkshire NHS Foundation Trust. (2014). Trust library and e-learning hub key performance indicators briefing. Reading: Royal Berkshire NHS Foundation Trust. Retrieved from http://wessex.hee.nhs.uk/files/2014/11/7_KPIs_used_by_Royal_Berkshire_Hospital_NHS_Library_Service.doc
- Royal College of General Practitioners. (2013). Social media highway code. London: Royal College of General Practitioners. Retrieved from http://www.rcgp.org.uk/~media/Files/Policy/A-Z_policy/RCGP-Social-Media-Highway-Code.ashx
- Royal College of Nursing. (2006). *Nurses and NHS IT developments. Results of an online survey by Nursix.com on behalf of the Royal College of Nursing*. London.
- Royal College of Nursing. (2009). Legal advice for RCN members using the internet. London: Royal College of Nursing. Retrieved from http://www.rcn.org.uk/_data/assets/pdf_file/0008/272195/003557.pdf
- Royal College of Nursing. (2012a). *Quality innovation productivity and prevention in England*. London. Retrieved from https://www2.rcn.org.uk/_data/assets/pdf_file/0007/457900/13.12_QIPP_in_England.pdf
- Royal College of Nursing. (2012b). *RCN guidance: nursing staff using personal mobile phones for work purposes*. London.
- Royal College of Radiologists. (s.d.). Social media policy.
- Royal Pharmaceutical Society. (s.d.). Social media guidance for pharmacists. Retrieved May 28, 2013, from <http://www.rpharms.com/unsecure-support-resources/social-media-guidance.asp?>
- Royal Pharmaceutical Society. (2014). Professional standards for hospital pharmacy services: optimising patient outcomes from medicines. *Royal Pharmaceutical Society*. London: Royal Pharmaceutical Society.
- Rutland, J. D., & Smith, A. M. (2010). Information needs of the “frontline” public health workforce. *Public Health*, 124(11), 659–663. <https://doi.org/10.1016/j.puhe.2010.06.002>
- Rycroft-Malone, J. (2005). The politics of evidence-based practice. *Worldviews on Evidence-Based Nursing*, 2(4), 169–171.
- Rycroft-Malone, J. (2006). The politics of the evidence-based practice movements: legacies and current challenges. *Journal of Research in Nursing*, 11(2), 95–108. <https://doi.org/10.1177/1744987106059793>
- Rycroft-Malone, J. (2008). Evidence-informed practice: from individual to context. *Journal of Nursing Management*, 16(4), 404–8. <https://doi.org/10.1111/j.1365-2834.2008.00859.x>
- Sachdeva, S. (2014). NHS wi-fi access “up, but not by enough.” *E-Health Insider*. Retrieved from <http://www.ehi.co.uk/news/EHI/9743/nhs-wi-fi-access-'up-but-not-b'>
- Salazar, J. (2015). Edward Snowden, SharePoint, and security. Retrieved March 4, 2017, from <https://www.credera.com/blog/technology-insights/microsoft-solutions/edward-snowden-sharepoint-security/>

- Saldanha, T. J. V., & Krishnan, M. S. (2012). Organizational adoption of web 2.0 technologies: An Empirical Analysis. *Journal of Organizational Computing and Electronic Commerce*, 22(4), 301–333. <https://doi.org/10.1080/10919392.2012.723585>
- Sandars, J., & Schroter, S. (2007). Web 2.0 technologies for undergraduate and postgraduate medical education: an online survey. *Postgraduate Medical Journal*, 83(986), 759–62. <https://doi.org/10.1136/pgmj.2007.063123>
- Sandbox. (2005). Retrieved June 24, 2016, from <http://searchsecurity.techtarget.com/definition/sandbox>
- Sapsford, R. (2006). Methodology. In V. Jupp (Ed.), *The Sage dictionary of social research methods* (pp. 176–178). London: Sage. Retrieved from <http://srmo.sagepub.com.eresources.shef.ac.uk/view/the-sage-dictionary-of-social-research-methods/n118.xml>
- Sasse, M. A. (2015). Scaring and bullying people into security won't work. *IEEE Security and Privacy*, (June), 80–83.
- Sauer, C., & Willcocks, L. (2007). Unreasonable expectations – NHS IT, Greek choruses and the games institutions play around mega-programmes. *Journal of Information Technology*, 22(3), 195–201. <https://doi.org/10.1057/palgrave.jit.2000108>
- Savin-Baden, M., & Major, C. H. (2013). *Qualitative research: the essential guide to theory and practice*. London: Routledge.
- Savolainen, R., & Kari, J. (2004). Placing the Internet in information source horizons. A study of information seeking by Internet users in the context of self-development. *Library and Information Science Research*, 26(4), 415–433. <https://doi.org/10.1016/j.lisr.2004.04.004>
- Sawyer, S., & Jarrahi, M. H. (2014). Sociotechnical approaches to the study of information systems. In A. Tucker, T. Gonzalez, H. Topi, & J. Diaz-Herrera (Eds.), *CRC computing handbook* (3rd ed., pp. 5-1 – 5-19). London: Chapman and Hall. <https://doi.org/DOI:10.1201/b16768-7>
- Sayer, A. (1992). *Method in social science: a realist approach* (2nd ed.). London: London.
- Sayer, A. (2000). *Realism and social science*. London: Sage.
- Sayer, A. (2004). Foreword: why critical realism? In S. Fleetwood & S. Ackroyd (Eds.), *Critical realist applications in organisation and management studies* (pp. 6–20). London: Routledge.
- Scally, G., & Donaldson, L. J. (1998). The NHS's 50th anniversary. Clinical governance and the drive for quality improvement in the new NHS in England. *BMJ British Medical Journal*, 317, 61–65.
- Schalow, P. S. R. R., Winkler, T. J., Repschläger, J., Zarnekow, R. R., Repschlaeger, J., & Zarnekow, R. R. (2013). The blurring boundaries of work-related and personal media use : a grounded theory study on the employee's perspective. *Proceedings of the 21st European Conference on Information Systems*, 1–12. Retrieved from http://aisel.aisnet.org/ecis2013_cr
- Schein, E. H. (1996). Three cultures of management: the key to organizational learning. *Sloan Management Review*, 38(1), 9–20.

- Schilling, L. M., Steiner, J. F., Lundahl, K., & Anderson, R. J. (2005). Residents' patient-specific clinical questions: opportunities for evidence-based learning. *Academic Medicine : Journal of the Association of American Medical Colleges*, *80*(1), 51–6. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/15618093>
- Schneier, B. (2000). *Secrets and lies: digital security in a networked world*. Indianapolis, IN: Wiley.
- Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: past, present and future. *Academy of Management Review*, *32*(2), 344–354. <https://doi.org/10.5465/AMR.2007.24348410>
- Scott-Findlay, S., & Golden-Biddle, K. (2005). Understanding how organizational culture shapes research use. *JONA*, *35*(7), 359–365.
- Scott, S. D., Estabrooks, C., Allen, M., & Pollock, C. (2008). A context of uncertainty: how context shapes nurses' research utilization behaviors. *Qualitative Health Research*, *18*(3), 347–57. <https://doi.org/10.1177/1049732307313354>
- Scragg, B., Shaikh, S., Robinson, L., & Mercer, C. (2017). Mixed messages: An evaluation of NHS Trust social media policies in the north west of England. *Radiography*. <https://doi.org/10.1016/j.radi.2017.03.018>
- Scragg, B., Shaikh, S., Shires, G., Stein Hodgins, J., Mercer, C., Robinson, L., & Wray, J. (2017). An exploration of mammographers' attitudes towards the use of social media for providing breast screening information to clients. *Radiography*. <https://doi.org/10.1016/j.radi.2017.04.004>
- Scully, T. (2011). The cyber threat, trophy information and the fortress mentality. *Journal of Business Continuity & Emergency Planning*, *5*(3), 195–207.
- Sedghi, S., Sanderson, M., & Clough, P. (2012). How do health care professionals select medical images they need? *Aslib Proceedings*, *64*(4), 437–456.
- Sedlack, D. J., & Tejay, G. P. S. (2011). Improving information security through technological frames of reference. In *Southern Association for Information Systems* (pp. 153–157). Atlanta, GA. Retrieved from <http://sais.aisnet.org/2011/SedlackTejay.pdf>
- Segers, J., El Ouiridi, A., El Ouiridi, M., & Hendrickx, E. (2014). Social media guidelines and policies: an exploratory study. In A. Rospigliosi & S. Greener (Eds.), *Proceedings of the European Conference on Social Media* (pp. 737–739). Brighton: University of Brighton.
- Sen, B. A., & Spring, H. (2013). Mapping the information-coping trajectory of young people with long-term illness: an evidence-based approach. *Journal of Documentation*, *69*(5), 638–666.
- Setterstrom, A. J., & Pearson, J. M. (2013). Bases of intra-organizational power: an analysis of the information technology department. *Electronic Journal of Information Systems Evaluation*, *16*(2), 88–102.
- Shanahan, M. (2009). Using e-resources and tools to update professional knowledge in the workplace. In *Ascilite 2009* (pp. 945–954). Auckland. Retrieved from <http://www.ascilite.org.au/conferences/auckland09/procs/shanahan.pdf>

- Shanahan, M. (2012). Professional learning in sonography. In K. Thoirs (Ed.), *Sonography* (Vol. 2006, p. 15pp.). Rijeka, Croatia: InTech Europe. Retrieved from www.intechopen.com/books/sonography/professional-learning-in-sonography
- Shanahan, M., Herrington, A., & Herrington, J. (2009). Workplace culture and accessibility of the Internet for professional learning. In G. Siemens & C. Fulford (Eds.), *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications 2009* (pp. 4423–4432). Honolulu, HI: AACE. Retrieved from <http://www.editlib.org/p/32129>
- Shankland, S. (2010). Jobs: why Apple banned Flash from the iPhone. Retrieved February 9, 2015, from <http://www.cnet.com/news/jobs-why-apple-banned-flash-from-the-iphone/>
- Shaw, P., & Lloyd, J. (2013). *Supporting the library and information needs of UWE health and social care students on placement: final report*. Bristol. Retrieved from <http://eprints.uwe.ac.uk/20615>
- Shaw, S., Elston, J., & Abbott, S. (2004). Comparative analysis of health policy implementation. *Policy Studies*, 25(4), 259–266. <https://doi.org/10.1080/0144287042000288451>
- Shearer, K. M. (2010). Blogging and Internet filters in schools. *Community and Junior College Libraries*, 16(4), 259–263. <https://doi.org/10.1080/02763915.2010.526913>
- Sheikh, A., Cornford, T., Barber, N., Avery, A., Takian, A., Lichtner, V., ... Cresswell, K. (2011). Implementation and adoption of nationwide electronic health records in secondary care in England: final qualitative results from prospective national evaluation in “early adopter” hospitals. *BMJ (Clinical Research Ed.)*, 343(oct17_1), d6054. <https://doi.org/10.1136/bmj.d6054>
- Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO / IEC 27001 services for information security management. *Indian Journal of Science and Technology*, 5(2), 2170–2177.
- Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, 22, 63–75.
- Shepherd, M. M., & Klein, G. (2011). Using deterrence to mitigate employee Internet abuse. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 5261–5266). <https://doi.org/10.1109/HICSS.2012.627>
- Shepherd, M. M., Mejias, R., & Klein, G. (2014). A longitudinal study to determine non-technical deterrence effects of severity and communication of Internet use policy for reducing employee Internet abuse. *2014 47th Hawaii International Conference on System Sciences*, 3159–3168. <https://doi.org/10.1109/HICSS.2014.392>
- Shuck, B. (2011). Four emerging perspectives of employee engagement: an integrative literature review. *Human Resource Development Review*, 10(3), 304–328. <https://doi.org/10.1177/1534484311410840>
- Siau, K., Fui-Hoon Nah, F., & Teng, L. (2002). Acceptable use policy. *Communications of the ACM*, 45(1), 75–79.

- Silic, M. (2015). *Shadow IT - steroids for innovation*. St Gallen.
- Silva, L. (2007). Epistemological and theoretical challenges for studying power and politics in information systems. *Information Systems Journal*, 17, 165–183. Retrieved from http://www.profjayrfigueiredo.com.br/STI_AC_11.pdf
- Silva, L., & Backhouse, J. (2003). The circuits-of-power framework for studying power in institutionalization of information systems. *Journal of the Association for Information Systems*, 4(6), 294–336. Retrieved from <http://eprints.lse.ac.uk/2357/>
- Silverman, D. (1993). *Interpreting qualitative data : methods for analysing talk, text and interaction*. London: London : Sage, 1993.
- Sim, M. G., Khong, E., Jiwa, M., & Moyez, J. (2008). Does general practice Google? *Australian Family Physician*, 37(6), 471–4. Retrieved from http://www.supportiveandpalliativecare.org.au/documents/2008/Does_general_practice_Google.pdf
- Simmons, D. G. (2005). Internet filtering : the effects in a middle and high school setting. *Meridian*, (Winter). Retrieved from http://www.ncsu.edu/project/meridian/win2005/Internetfiltering/internet_filtering.pdf
- Simons, H. (2008). *Case study research in practice*. London: Sage.
- Singh, J. B., & Chandwani, R. (2014). Adoption of Web 2.0 technologies among knowledge workers: a theoretical integration [sic] of knowledge sharing and seeking factors. In *Twenty Second European Conference on Information Systems*. Tel Aviv.
- Singleton, P., Pagliari, C., & Detmer, D. E. (2008). *Critical issues or electronic health records: considerations from an expert workshop*. London. Retrieved from http://www.nuffieldtrust.org.uk/sites/files/nuffield/publication/Critical_Issues_for_Electronic_Health_Records_March_2009.pdf
- Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective contributions. *The Data Base for Advances in Information Systems*, 38(1), 60–80.
- Siponen, M. T., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270. <https://doi.org/10.1016/j.im.2008.12.007>
- Sjouwerman, S. (2013). Avoiding dodgy web sites no longer works to stay safe. Retrieved July 1, 2013, from <http://blog.knowbe4.com/bid/311054/Avoiding-Dodgy-Web-Sites-No-Longer-Works-To-Stay-Safe>
- Skoudis, E. (2005). Will Web browsers ever be fully equipped to detect and remove malware? Retrieved May 29, 2013, from http://searchsecurity.techtarget.com/answer/Will-Web-browsers-ever-be-fully-equipped-to-detect-and-remove-malware#.UaZQH_9fM0.mendeley
- Slawson, D. C., & Shaughnessy, A. F. (2005). Teaching evidence-based medicine: should we be teaching information management instead? *Academic Medicine*, 80(7), 685–689.

- Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative Science Quarterly*, 28(3), 339–358. <https://doi.org/10.2307/2392246>
- Smith, D., & Toft, B. (2010, March 15). Risk and Crisis Management in the Public Sector: Editorial: Issues in Public Sector Risk Management. Taylor & Francis Group. Retrieved from <http://www.tandfonline.com/doi/abs/10.1111/1467-9302.00133?journalCode=rpmm20>
- Smith, M. L. (2006). Overcoming theory-practice inconsistencies: critical realism and information systems research. *Information and Organization*, 16(3), 191–211. <https://doi.org/10.1016/j.infoandorg.2005.10.003>
- Smith, R. (1996). What clinical information do doctors need? *BMJ*, 313(7064), 1062–1068. <https://doi.org/10.1136/bmj.313.7064.1062>
- Smith, R. (2010). Strategies for coping with information overload. *BMJ*, 341, 1281–1282 (c7126). <https://doi.org/10.1136/bmj.c7126>
- Smith, S. W. (2012). Security and cognitive bias: exploring the role of the mind. *IEEE Security and Privacy*, 10(5), 75–78. <https://doi.org/10.1109/MSP.2012.126>
- Solomon, M., Beale, A., & Lennox-Chhugani, N. (2016). *NHS IT: older, fatter and twisted*. London.
- Solutionary. (2014). Security threat report - May 2014. Retrieved March 10, 2017, from <https://www.solutionary.com/threat-intelligence/threat-reports/monthly-threat-reports/2014/05/security-threat-report-may-2014/>
- Sonnenwald, D. H. (1999). Evolving perspectives of human information behavior: Contexts, situations, social networks and information horizons. In T. D. Wilson & D. K. Allen (Eds.), *Exploring the contexts of information behavior: Proceedings of the Second International Conference in Information Needs* (pp. 176–190). London: Taylor Graham.
- Sophos. (2016a). Checklist of technology, tools and tactics for effective web protection. Abingdon: Sophos. Retrieved from <https://www.sophos.com>
- Sophos. (2016b). *Preventative measures: an independent survey of the current state of security across the NHS*. Abingdon.
- Spacey, R., & Cooke, L. (2014). *Managing access to the Internet in public libraries [MAIPLE]* (Vol. 19). Loughborough.
- Spacey, R., Cooke, L., Creaser, C., & Muir, A. (2013). Regulating Internet access and content in UK public libraries: Findings from the MAIPLE project. *Journal of Librarianship and Information Science*. <https://doi.org/10.1177/0961000613500688>
- Spacey, R., Cooke, L., Muir, A., & Creaser, C. (2013). Regulating use of the Internet in public libraries: a review. *Journal of Documentation*, 70(3), 478–497. <https://doi.org/10.1108/JD-02-2013-0021>
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, 34(3), 503–522. <https://doi.org/10.2337/dc10-0368>

- Spenceley, S. M., O’Leary, K. A., Chizawsky, L. L. K., Ross, A. J., & Estabrooks, C. A. (2008). Sources of information used by nurses to inform practice: An integrative review. *International Journal of Nursing Studies*, 45(6), 954–970. <https://doi.org/10.1016/j.ijnurstu.2007.06.003>
- Spencer, L., Ritchie, J., Lewis, J., & Dillon, L. (2003). *Quality in qualitative evaluation: a framework for assessing research evidence*. London: Government Chief Social Researcher’s Office, Cabinet Office. Retrieved from http://collections-r.europarchive.org/tna/20070705130742/http://www.policyhub.gov.uk/docs/qqe_rep.pdf
- Spencer, L., Ritchie, J., O’Connor, W., Morrell, G., & Ormston, R. (2014). Analysis in practice. In J. Ritchie, J. Lewis, C. McNaughton Nicholls, & R. Ormston (Eds.), *Qualitative research practice: a guide for social science students and researchers* (2nd ed., pp. 295–345). London: Sage.
- Stahl, B. C. (2007). Positivism or non-positivism - *tertium non datur*: a critique of ontological syncretism in IS research. *Ontologies*, 1–28.
- Stahl, B. C. (2008). *Information systems: critical perspectives*. London: Routledge.
- Stahl, B. C. (2013). Interpretive accounts and fairy tales: a critical polemic against the empiricist bias in interpretive IS research. *European Journal of Information Systems*, (January 2012), 1–11. <https://doi.org/10.1057/ejis.2012.58>
- Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, 22(1), 77–94. <https://doi.org/10.1111/j.1365-2575.2011.00378.x>
- Stahl, B. C., Tremblay, M. C., & LeRouge, C. M. (2011). Focus groups and critical social IS research: how the choice of method can promote emancipation of respondents and researchers. *European Journal of Information Systems*, 20(4), 378–394. <https://doi.org/10.1057/ejis.2011.21>
- Stanley, C., & Stovall, J. (2008). The blocked blog (or Websense and the technical colleges’ fight for academic freedom). *Georgia Library Quarterly*, 45(1), 4–8.
- Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional*, 18(5), 26–32. <https://doi.org/10.1109/MITP.2016.84>
- Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, 24(2), 124–133. <https://doi.org/10.1016/j.cose.2004.07.001>
- “Stars are aligned” for health IT - Freeman. (2016). Retrieved March 5, 2016, from <http://www.digitalhealth.net/cio/47234/'stars-are-aligned'-for-health-it---freeman>
- Steier, F. (1991). *Research and reflexivity*. London: Sage.
- Stein, M.-K., Galliers, R. D., & Markus, M. L. (2012). Towards an understanding of identity and technology in the workplace. *Journal of Information Technology*, 28(3), 167–182. <https://doi.org/10.1057/jit.2012.32>

- Steinmetz, G. (1998). Critical realism and historical sociology: a review article. *Comparative Studies in Society and History*, 40(1), 170–186. Retrieved from <http://www-personal.umich.edu/~geostein/docs/SteinmetzRealism.pdf>
- Stephenson, J. (2015, February). NHS nurses using their own smartphones for work. *Nursing Times*. Retrieved from <http://www.nursingtimes.net/roles/nurse-managers/nhs-nurses-using-their-own-smartphones-for-work/5090960.article>
- Steven, A., Magnusson, C., Smith, P., & Pearson, P. H. (2014). Patient safety in nursing education: contexts, tensions and feeling safe to learn. *Nurse Education Today*, 34(2), 277–284. <https://doi.org/10.1016/j.nedt.2013.04.025>
- Steves, M., Chisnell, D., Sasse, M. A., Krol, K., Theofanos, M., Wald, H., ... Mclean, A. H. (2014). *Report: Authentication Diary Study*. Gaithersburg, MD. <https://doi.org/10.6028/NIST.IR.7983>
- Stewart, A. (2004). On risk: perception and direction. *Computers and Security*, 23(5), 362–370. <https://doi.org/10.1016/j.cose.2004.05.003>
- Stewart, D. (1992). Responsibility for funding NHS library services. *Health Libraries Review*, 9, 62–65.
- Stratton, M. T. (2010). Uncovering a new guilty pleasure: a qualitative study of the emotions of personal web usage at work. *Journal of Leadership & Organizational Studies*, 17(4), 392–410. <https://doi.org/10.1177/1548051809350893>
- Streeton, R., Cooke, M., & Campbell, J. (2004). Researching the researchers: using a snowballing technique. *Nurse Researcher*, 12(1), 35–46.
- Stritter, B., Freiling, F., König, H., Rietz, R., Ullrich, S., von Gernier, A., ... Dressler, F. (2016). Cleaning up Web 2.0's security mess — at least partly. *IEEE Security and Privacy*, (April), 48–57.
- Strong, D., & Volkoff, O. (2010). Understanding organization-enterprise system fit: a path to theorizing the information technology artifact. *MIS Quarterly*, 34(4), 731–756.
- Sullivan, B., & Liu, V. (2012). *Web application security: a beginner's guide*. New York: McGraw-Hill.
- Sullivan, D. (2015). How can enterprises prevent shadow data leakage? Retrieved January 13, 2017, from <http://searchcloudsecurity.techtarget.com/answer/How-can-enterprises-prevent-shadow-data-leakage>
- Sunderland, D. (2000). *Social capital, trust and the Industrial Revolution: 1780–1880*. London: Routledge.
- Sundin, O., & Hedman, J. (1996). *Theory of professions and occupational identities*. Göteborg / Borås. Retrieved from <http://lup.lub.lu.se/>
- Sutton, A., Booth, A., Ayiku, L., & O'Rourke, A. (2005). e-FOLIO: using e-learning to learn about e-learning. *Health Information and Libraries Journal*, 22(1), 84–88.
- Sutton, L. (2005). *Experiences of high school students conducting term paper research using filtered Internet access*. *Teachers College Record*. Wayne State University, Pittsburgh, PA. Retrieved from <http://www.tcrecord.org/content.asp?contentid=12248#UdqxS3NSH6g.mendeley>

- Sutton, L. (2006). *Access denied: how Internet filters impact student learning in high schools*. Youngstown, NY: Cambria Press.
- Svensson, A., Snis, U. L., Svanberg, P., & Svensson, L. (2009). Attitudes to information technology in health care professions. In *ECIS 2009 Proceedings*. Verona. Retrieved from <http://is2.lse.ac.uk/asp/aspectis/20090210.pdf>
- Takian, A., & Cornford, T. (2012). NHS information: revolution or evolution? *Health Policy and Technology*, 1(4), 193–198. <https://doi.org/10.1016/j.hlpt.2012.10.005>
- Tang, H., & Ng, J. H. K. (2006). Googling for a diagnosis--use of Google as a diagnostic aid: internet based study. *BMJ (Clinical Research Ed.)*, 333(7579), 1143–5. <https://doi.org/10.1136/bmj.39003.640567.AE>
- Tatnall, A. (2003). Actor-network theory as a socio-technical approach to information systems research, 266–283. Retrieved from <http://dl.acm.org/citation.cfm?id=766867.766885>
- Tatnall, A., & Gilding, A. (1999). Actor-network theory and information systems research. In *10th Australasian Conference on Information Systems* (pp. 955–966).
- Taylor, L., McMinn, M. R., Bufford, R. K., & Chang, K. B. T. (2010). Psychologists' attitudes and ethical concerns regarding the use of social networking web sites. *Professional Psychology Research and Practice*, 41, 153–159. <https://doi.org/10.1037/a0017996>
- Teague, M. (2014). NHS and eduroam/shared use of wireless/PSNroam? Retrieved March 24, 2015, from <https://community.ja.net/groups/nhs-he-forum-connectivity-project/article/nhs-and-eduroamshared-use-wirelesspsnroam>
- Technical Design Authority Group. (2009a). *Survey of access to online resources in healthcare libraries in England conducted on behalf of the National Library for Health*. London.
- Technical Design Authority Group. (2009b). *TDAG survey of access to electronic resources in healthcare libraries*. London: TDAG.
- Tellis, W. (1997a). Application of a case study methodology. *Qualitative Report*, 3(3). Retrieved from <http://www.nova.edu/ssss/QR/QR3-3/tellis2.html?ref=dizinler.com>
- Tellis, W. (1997b). Introduction to case study. *Qualitative Report*, 3(3). Retrieved from <http://www.nova.edu/ssss/QR/QR3-2/tellis1.html>
- Tennakoon, H., Ezingear, J.-N., & Benson, V. (2012, September 1). Social networks and information security: extant research and future perspectives. Retrieved from <http://eprints.kingston.ac.uk/22867/>
- Thain, A., & Wales, A. (2005). Information needs of specialist healthcare professionals: a preliminary study based on the West of Scotland Colorectal Cancer Managed Clinical Network. *Health Information and Libraries Journal*, 22(2), 133–42. <https://doi.org/10.1111/j.1471-1842.2005.00570.x>

- Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6), 472–484. <https://doi.org/10.1016/j.cose.2005.05.002>
- Thiel, V. (2013, March). CSU structures and how they will operate. *Health Service Journal*. Retrieved from <https://www.hsj.co.uk/home/commissioning/csu-structures-and-how-they-will-operate/5055935.article?blocktitle=Resource-Centre&contentID=8630>
- Thomas, B. (2013). The impact of social media in the healthcare context and its implications for the nursing profession. Retrieved February 13, 2014, from <http://www.florence-nightingale-foundation.org.uk/content/page/122/>
- Thomas, G. (2011). A typology for the case study in social science following a review of definition, discourse, and structure. *Qualitative Inquiry*, 17(6), 511–521. <https://doi.org/10.1177/1077800411409884>
- Thomas, S. (2006). Application security: good practice guidelines. Exeter: NHS Connecting for Health.
- Thompson, C., Cullum, N., McCaughan, D., Sheldon, T., & Raynor, P. (2004). Nurses, information use, and clinical decision making - the real world potential for evidence-based decisions in nursing. *Evidence-Based Nursing*, 7, 68–72.
- Thompson, C., McCaughan, D., Cullum, N., Sheldon, T. A., Mulhall, A., & Thompson, D. R. (2001a). The accessibility of research-based knowledge for nurses in United Kingdom acute care settings. *Journal of Advanced Nursing*, 36(1), 11–22. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/11555045>
- Thompson, C., McCaughan, D., Cullum, N., Sheldon, T., Mulhall, A., & Thompson, D. R. (2001b). Research information in nurses' clinical decision-making: what is useful? *Journal of Advanced Nursing*, 36(3), 376–88. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/11686752>
- Thompson, C., McCaughan, D., Cullum, N., Sheldon, T., Thompson, D., & Mulhall, A. (s.d.). *Nurses' use of research information in clinical decision making: a descriptive and analytical study*. [London].
- Thompson, D. S., O'Leary, K., Jensen, E., Scott-Findlay, S., O'Brien-Pallas, L., & Estabrooks, C. A. (2008). The relationship between busyness and research utilization: it is about time. *Journal of Clinical Nursing*, 17(4), 539–548. <https://doi.org/10.1111/j.1365-2702.2007.01981.x>
- Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: a review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), 245–257. <https://doi.org/10.1002/asi.20121>
- Thorne, C. (2012). Royal Liverpool pioneers “BYOD” in NHS. *E-Health Insider*. Retrieved from <http://www.ehi.co.uk/news/industry/7851/royal-liverpool-pioneers-byod-in-nhs>
- Thorne, S. (2000). Data analysis in qualitative research. *Evidence Based Nursing*, 3(3), 68. <https://doi.org/10.1136/ebn.3.3.68>

- Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security*, 2013(4), 12–13. [https://doi.org/10.1016/S1353-4858\(13\)70050-3](https://doi.org/10.1016/S1353-4858(13)70050-3)
- Topakas, A., & Dawson, J. (2010). *Outcomes of staff engagement in the NHS: a trust level analysis*. Birmingham.
- Toth, B., Muir Gray, J. A., Fraser, V., & Ward, R. (2000). National electronic Library for Health: progress and prospects. *Health Libraries Review*, 17(1), 46–50. <https://doi.org/10.1046/j.1365-2532.2000.00261.x>
- Tracy, S. J. (2010). Qualitative quality: eight “big-tent” criteria for excellent qualitative research. *Qualitative Inquiry*, 16(10), 837–851. <https://doi.org/10.1177/1077800410383121>
- Trauth, E. M., & Quesenberry, J. L. (2006). Gender and the information technology workforce : issues of theory and practice. In P. Yoong & S. Huff (Eds.), *Managing IT professional in the Internet age* (pp. 18–36). Hershey, PA: Idea Group Publishing.
- Trushina, I. (2004). Freedom of access: ethical dilemmas for Internet librarians. *Electronic Library, The*, 22(5), 416–421.
- Truss, C., Alfes, K., Delbridge, R., Shantz, A., & Soane, E. (Eds.). (2013). *Employee engagement in theory and practice*. London: Routledge.
- Tuckett, A. G. (2015). Applying thematic analysis theory to practice - a researcher’s experience. *Contemporary Nurse*, 6178(October), 1–2, 75–87. <https://doi.org/10.5172/conu.19.1-2.75>
- Turle, M. (2009). Data security: past, present and future. *Computer Law & Security Review*, 25(1), 51–58. <https://doi.org/10.1016/j.clsr.2008.11.001>
- Turner, A. (2004). A joined-up approach: how England’s National electronic Library for Health (NeLH) is working with librarians. *Health Information and Libraries Journal*, 21 Suppl 1(1), 55–57. <https://doi.org/10.1111/j.1740-3324.2004.00503.x>
- Turner, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*, 15(3), 754–760. <https://doi.org/http://www.nova.edu/ssss/QR/QR15-3/qid.pdf>
- Turner, M. E., & Pratkanis, A. R. (1998). Twenty-five years of groupthink theory and research: lessons from the evaluation of a theory. *Organizational Behavior and Human Decision Processes*, 73(2/3), 105–15. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/9705798>
- UKCHIP. (2014). Health informatics career framework. Cardiff: Velindre NHS Trust. Retrieved from <https://www.hicf.org.uk/>
- Ulger, F., Esen, S., Dilek, A., Yanik, K., Gunaydin, M., & Leblebicioglu, H. (2009). Are we aware how contaminated our mobile phones with nosocomial pathogens? *Annals of Clinical Microbiology and Antimicrobials*, 8(1), 7. <https://doi.org/10.1186/1476-0711-8-7>
- University Health and Medical Librarians Group. (2014). Higher education institution / NHS OpenAthens wiki. Retrieved March 24, 2015, from <http://nhs-hei-athens.wikispaces.com/>

- Urbaczewski, A., & Jessup, L. M. (2002). Does electronic monitoring of employee internet usage work? *Communications of the ACM*, 45(1). <https://doi.org/10.1145/502269.502303>
- Urquhart, C. J., Light, A., Thomas, R., Barker, A., Armstrong, A., Yeoman, J., ... Armstrong, C. (2003). Critical incident technique and explicitation interviewing in studies of information behavior. *Library and Information Science Research*, 25(1), 63–88. [https://doi.org/10.1016/S0740-8188\(02\)00166-4](https://doi.org/10.1016/S0740-8188(02)00166-4)
- Utin, D. M., Utin, M., & Utin, J. (2008). General misconceptions about information security lead to an insecure world. *Information Security Journal: A Global Perspective*, 17(4), 164–169. <https://doi.org/10.1080/19393550802369792>
- Vaast, E. (2007). Danger is in the eye of the beholders: social representations of information systems security in healthcare. *The Journal of Strategic Information Systems*, 16(2), 130–152. <https://doi.org/10.1016/j.jsis.2007.05.003>
- Vaast, E., & Kaganer, E. (2013). Social media affordances and governance in the workplace: An examination of organizational policies. *Journal of Computer-Mediated Communication*, 19(1), 78–101. <https://doi.org/10.1111/jcc4.12032>
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences*, 15(3), 398–405. <https://doi.org/10.1111/nhs.12048>
- Valli, C. (2004). Non-business use of the WWW in three Western Australian organisations. *Internet Research*, 14(5), 353–359. <https://doi.org/10.1108/10662240410566944>
- van Teijlingen, E. R., & Hundley, V. (2001). The importance of pilot studies. Retrieved June 21, 2017, from <http://sru.soc.surrey.ac.uk/SRU35.html>
- Van Velsen, L. S., Steehouder, M. F., & De Jong, M. D. T. (2007). Evaluation of user Support: factors that affect user satisfaction with helpdesks and helplines. *IEEE Transactions on Professional Communication*, 50(3), 219–231. <https://doi.org/10.1109/TPC.2007.902660>
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37(1), 21–54. Retrieved from <http://aisel.aisnet.org/misq/vol37/iss1/3>
- Verma, S., Kavita, & Budhiraja, S. (2012). Internet security. *International Journal of Computer Applications in Engineering Sciences*, II(III), 210–213.
- Verschuren, P. (2003). Case study as a research strategy: Some ambiguities and opportunities. *International Journal of Social Research Methodology*, 6(2), 121–139. <https://doi.org/10.1080/13645570110106154>
- Volkamer, M., & Renaud, K. (2013). Mental models – general introduction and review of their application to human-centred security. *Number Theory and Cryptography SE - 18*, 8260, 255–280. https://doi.org/10.1007/978-3-642-42001-6_18

- Volkoff, O., Strong, D. M., Elmes, M. B., Volkoff, O., Strong, D. M., & Elmes, M. B. (2007). Technological embeddedness and organizational change. *Organization Science*, 18(5), 832–848. <https://doi.org/10.1287/orsc.1070.0288>
- Volpentesta, A. P., Ammirator, S., & Palmieri, R. (2011). Investigating effects of security incident awareness on information risk perception. *International Journal of Technology Management*, 54(2/3), 304–320.
- von Muhlen, M., & Ohno-Machado, L. (2012). Reviewing social media use by clinicians. *Journal of the American Medical Informatics Association*, 19(5), 777–81. <https://doi.org/10.1136/amiajnl-2012-000990>
- von Solms, B. (2011). Securing the Internet: fact or fiction? In J. Camenisch, V. Kisimov, & D. M (Eds.), *iNetSec, LNCS 6555* (pp. 1–8). IFIP International Federation For Information Processing.
- Vratonjic, N., Manshaei, M. H., & Hubaux, J.-P. (2011). *Online advertising fraud*. Lausanne. Retrieved from <https://infoscience.epfl.ch/record/165674/files/OnlineAdFraud.pdf>
- Wachter, R. M. (2016). *Making IT work: harnessing the power of health information technology to improve care in England: report of the National Advisory Group on Health Information Technology in England*.
- Wainwright, D. W., & Waring, T. S. (2007). The application and adaptation of a diffusion of innovation framework for information systems research in NHS general medical practice. *Journal of Information Technology*, 22(1), 44–58. <https://doi.org/10.1057/palgrave.jit.2000093>
- Walley, P. J., & Davies, C. (2002). Implementing IT in NHS hospitals: internal barriers to technological advancement. *International Journal of Healthcare Technology and Management*, 4(3/4), 259–272.
- Walmsley, S. (2012). DigiPharm - multiscreen healthcare: presentation given at DigiPharm 2012 conference, London, 25-27 September. London. Retrieved from <http://www.slideshare.net/sammielw/digipharm-multiscreen-healthcare>
- Walsham, G. (1993). *Interpreting information systems in organizations*. Chichester: Wiley.
- Walsham, G. (1995a). Interpretive case-studies in IS research - nature and method. *European Journal of Information Systems*, 4(2), 74–81. <https://doi.org/10.1057/ejis.1995.9>
- Walsham, G. (1995b). The emergence of interpretivism in IS research. *Information Systems Research*, 6(4), 376–394.
- Walsham, G. (1997). Actor-network theory and IS research: current status and future prospects. In A. S. Lee, J. Liebenau, & J. I. DeGross (Eds.), *Information systems and qualitative research: proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research* (pp. 466–480). Dordrecht: Springer US. <https://doi.org/10.1007/978-0-387-35309-8>
- Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, 15(3), 320–330. <https://doi.org/10.1057/palgrave.ejis.3000589>

- Walsham, G. (2013). Empiricism in interpretive IS research: a response to Stahl. *European Journal of Information Systems*, 23, 12–16. <https://doi.org/10.1057/ejis.2012.57>
- Walshe, K., & Rundall, T. G. (2001). Evidence-based management: from theory to practice in health care. *The Milbank Quarterly*, 79(3), 429–57, IV–V. Retrieved from <http://www.pubmedcentral.nih.gov>
- Walton, G., Smith, A., Gannon-Leary, P., & Middleton, A. (2005). Supporting learning in practice in the EBL curriculum: pre-registration students' access to learning resources in the placement setting. *Nurse Education in Practice*, 5(4), 198–208. <https://doi.org/10.1016/j.nepr.2004.10.003>
- Wang, Y., Smith, S., & Gettinger, A. (2012). Access control hygiene and the empathy gap in medical IT. In *HealthSec'12 Proceedings of the 3rd USENIX conference on Health Security and Privacy*. Association for Computing Machinery.
- Ward, L., Sutton, S., Divall, P., & Hull, L. (2008). Practitioner commentary on Garfield E. The impact of health information delivery on the quality of patient care: whither medical information science? *Health Libraries review* 1985, 2 (4), 159-169. *Health Information and Libraries Journal*, 25 Suppl 1, 63–5. <https://doi.org/10.1111/j.1471-1842.2008.00809.x>
- Ward, R., & Moule, P. (2007). Supporting pre-registration students in practice: A review of current ICT use. *Nurse Education Today*, 27(1), 60–7. <https://doi.org/10.1016/j.nedt.2006.02.008>
- Ward, R., Moule, P. a., & Lockyer, L. (2009). Adoption of Web 2.0 technologies in education for health professionals in the UK: Where are we and why? *Electronic Journal of eLearning*, 7(2), 165–172.
- Ward, R., Stevens, C., Brentnall, P., & Briddon, J. (2008). The attitudes of health care staff to information technology: a comprehensive review of the research literature. *Health Information and Libraries Journal*, 25(2), 81–97. <https://doi.org/10.1111/j.1471-1842.2008.00777.x>
- Waring, J., & Currie, G. (2009). Managing expert knowledge: organizational challenges and managerial futures for the UK medical profession. *Organization Studies*, 30(7), 755–778. <https://doi.org/10.1177/0170840609104819>
- Warm, D. L., Thomas, S. E., Heard, V. R., Jones, V. J., & Hawkins-Brown, T. M. (2008). Benefits of information technology training to National Health Service staff in Wales. *Learning in Health and Social Care*. <https://doi.org/10.1111/j.1473-6861.2008.00195.x>
- Watters, P. A. (2009). Data loss in the British government: bounty of credentials for organised crime. In *UIC-ATC 2009 - Symposia and workshops on ubiquitous, autonomic and trusted computing in conjunction with the UIC'09 and ATC'09 conferences* (pp. 531–536). <https://doi.org/10.1109/UIC-ATC.2009.73>
- Weatherbee, T. G. (2010). Counterproductive use of technology at work: information and communications technologies and cyberdeviancy. *Human Resource Management Review*, 20(1), 35–44. <https://doi.org/10.1016/j.hrmr.2009.03.012>
- Webb, C. (2008). Dear diary: recommendations for researching knowledge transfer of the complex. *Proceedings of the European Conference on Knowledge Management, ECKM*, 7(1), 939–946.

- Weber, M. (1947). The theory of economic and social organization. *Trans. AM Henderson and Talcott Parsons*. New York: Oxford University Press.
- Webopedia. (s.d.). What is phishing? Retrieved May 31, 2013, from <http://www.webopedia.com/TERM/P/phishing.html>
- Wehmeyer, J. M., & Wehmeyer, S. (1999). The comparative importance of books: clinical psychology in the health sciences library. *Bulletin of the Medical Library Association*, 87(2), 187–91. Retrieved from <http://www.pubmedcentral.nih.gov>
- Weightman, A., & Urquhart, C. (2008). How's our impact? Developing a survey toolkit to assess how health library services impact on patient care. In *AWHILES Conference*. Wrexham. Retrieved from http://www.libraryservices.nhs.uk/document_uploads/Impact/awhiles_july_2008_library_impact.pdf
- Welbourn, D. (2013). *Leadership of innovation in the NHS - a literature review of good practice*. London. Retrieved from <https://www.england.nhs.uk/wp-content/uploads/2013/10/cass.pdf>
- Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4–19. <https://doi.org/10.1108/09685220910944722>
- Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. (2009). Security practitioners in context: their activities and interactions with other stakeholders within organizations. *International Journal of Human Computer Studies*, 67(7), 584–606.
- West, M. A., & Dawson, J. F. (2012). *Employee engagement and NHS performance*. King's Fund. London. Retrieved from <http://www.kingsfund.org.uk/sites/files/kf/employee-engagement-nhs-performance-west-dawson-leadership-review2012-paper.pdf>
- West, M. A., Topakas, A., & Dawson, J. F. (2014). Climate and culture for health care performance. In B. Schneider & K. M. Barbera (Eds.), *The Oxford handbook of organizational climate and culture and climate* (pp. 335–359). New York: Oxford University Press.
- West, M., Dawson, J., Admasachew, L., & Topakas, A. (2011). *NHS staff management and health service quality: results from the NHS staff survey and related data*. Birmingham. Retrieved from http://e3idocs.fmhs.fastmail.net/dh_129656.pdf
- West, R., Mayhorn, C., Hardee, J., & Mendell, J. (2008). The weakest link: a psychological perspective on why users make poor security decisions. In M. Gupta & R. Sharman (Eds.), *Social and Human Elements of Information Security: Emerging Trends and Countermeasures: Emerging Trends and Countermeasures* (pp. 43–60). Hershey, PA: IGI Global. Retrieved from https://www.researchgate.net/profile/Christopher_Mayhorn/publication/289274684_The_weakest_link_A_psychological_perspective_on_why_users_make_poor_security_decisions/links/5697ca9308ae1c4279051e81.pdf
- Westbrook, J. I., Coiera, E. W., & Gosling, A. S. (2005). Do online information retrieval systems help experienced clinicians answer clinical questions? *Journal of the American Medical Informatics Association*, 12(3), 315–322. <https://doi.org/10.1197/jamia.M1717.Online>

- Westerman, S., & Hurt, E. (2007). Use of the internet to support learning in practice. In S. West, T. Clark, & M. Jasper (Eds.), *Enabling learning in nursing and midwifery practice: a guide for mentors* (pp. 181–196). Chichester: Wiley.
- What desktop virtualization really means. (s.d.). Retrieved December 16, 2014, from <http://www.infoworld.com/article/2627220/vdi/what-desktop-virtualization-really-means.html>
- What is desktop virtualization? (s.d.). Retrieved December 16, 2014, from http://www.webopedia.com/TERM/D/desktop_virtualization.html
- WhatIs.com. (2008). What is black box (black box testing)? Retrieved February 12, 2016, from <http://searchsoftwarequality.techtarget.com/definition/black-box>
- Whitfield, L. (2005). Email and internet policies: cracking down on misuse. *IRS Employment Review*, (830).
- Whitfield, L. (2016a). First free NHS wi-fi targets outlined at NIB meeting. Retrieved April 21, 2016, from <http://www.digitalhealth.net/infrastructure/47589/first-free-nhs-wi-fi-targets-outlined-at-nib-meeting>
- Whitfield, L. (2016b). NHS “to do” list puts IT and funding focus on STPs. Retrieved January 24, 2017, from <http://www.digitalhealth.net/news/48088/nhs-'to-do'-list-puts-it-and-funding-focus-on-st>
- Whitman, M., & Mattord, H. J. (2010). *Management of information security* (3rd ed.). Boston, MA: Course Technology Cengage Learning.
- Whitty, M. T. (2004). Should filtering software be utilised in the workplace? Australian employees' attitudes towards Internet usage and surveillance of the Internet in the workplace. *Surveillance and Society*, 2(1), 39–54.
- Wikgren, M. (2005). Critical realism as a philosophy and social theory in information science? *Journal of Documentation*, 61(1), 11–22. <https://doi.org/10.1108/00220410510577989>
- Wilde, G. J. S. (1998). Risk homeostasis theory: an overview. *Injury Prevention*, 4, 89–91.
- Wilkinson, A., Papaioannou, D., Keen, C., & Booth, A. (2009). The role of the information specialist in supporting knowledge transfer: a public health information case study. *Health Information and Libraries Journal*, 26(2), 118–25. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/19490150>
- Willard, N. (2010). Teach them to swim. *Knowledge Quest*, 39(1), 54–61. Retrieved from <http://search.proquest.com/openview/acaf5e320275bf37dfc4dda7d0057bf8/1?pq-origsite=gscholar&cbl=6154>
- Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices (Auckland, N.Z.)*, 8, 305–16. <https://doi.org/10.2147/MDER.S50048>

- Willis, J. W. (2007). *Foundations of qualitative research: interpretive and critical approaches*. Thousand Oaks, CA: Sage. <https://doi.org/10.4135/9781452230108>
- Willson, J., & Oulton, T. (2000). Controlling access to the Internet in UK public libraries. *OCLC Systems and Services*, 16(4), 194–201.
- Wilson, M., & Greenhill, A. (2004). Theory and action for emancipation. In B. Kaplan, D. Truex III, D. Wastell, T. Wood-Harper, & J. DeGross (Eds.), *Information systems research: relevant theory and informed practice* (Vol. 143, pp. 667–674). Amsterdam: Kluwer Academic Publishers. Retrieved from <http://www.springerlink.com/index/10.1007/b115738>
- Wilson, T. D. (1981). On user studies and information needs. *Journal of Documentation*, 37(1), 3–15.
- Wilson, T. D. (1999). Models in information behaviour research. *Journal of Documentation*, 55(3), 249–270. Retrieved from <http://informationr.net/tdw/publ/papers/2005SIGUSE.html>
- Wilson, T. D. (2006). A re-examination of information seeking behaviour in the context of activity theory. *Information Research*, 11(4). Retrieved from <http://informationr.net/ir/11-4/paper260.html>
- Wilson, T. D. (1997). Information behaviour: An interdisciplinary perspective. *Information Processing & Management*, 33(4), 551–572. [https://doi.org/10.1016/S0306-4573\(97\)00028-9](https://doi.org/10.1016/S0306-4573(97)00028-9)
- Wilson, T., & Walsh, C. (1996). *Information behaviour: an interdisciplinary perspective* (British Library Research and Innovation Reports No. 10). London. Retrieved from <http://www.informationr.net/tdw/publ/infbehav/>
- WinZip. (s.d.). Potentially unsafe file types. Retrieved July 25, 2017, from <http://kb.winzip.com/help/ZipSecurity.htm>
- Wong, G., Greenhalgh, T., Russell, J., Boynton, P., & Toon, P. (2003). Putting your course on the Web: lessons from a case study and systematic literature review. *Medical Education*, 37(11), 1020–3. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/14629417>
- Wood, H. (2015). Bring your own disaster? Retrieved July 27, 2015, from http://www.himssinsights-digital.com/insights/vol_3_number_3#pg44
- Woodhouse, S. (2007). Information security: end user behavior and corporate culture. In *7th IEEE International Conference on Computer and Information Technology (CIT 2007)* (pp. 767–774). Fukushima: IEEE. <https://doi.org/10.1109/CIT.2007.186>
- Worth, D., & Neal, D. (2015). UK government confirms Windows XP support deal has ended. Retrieved April 29, 2016, from <http://www.v3.co.uk/v3-uk/news/2406304/windows-xp-government-support-deal-ends-leaving-pcs-open-to-attack>
- Wright, A., & Bingham, H. (2008). E-learning scoping exercise for NHS South Central: results and recommendations: part one: trusts and PCTs. Winchester: NHS South Central.
- Wyatt, J. C. (2012). The new NHS information strategy. *BMJ*, 344(7860), 9–10.

- Wyatt, J. C., & Sullivan, F. (2005). *ABC of health informatics: keeping up: learning in the workplace*. *BMJ* (Vol. 331). London: BMJ Publishing.
- Wynn, D., & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *MIS Quarterly*, *36*(3), 787–810.
- Yen, T.-F., Heorhiadi, V., Oprea, A., Reiter, M. K., & Juels, A. (2014). An epidemiological study of malware encounters in a large enterprise. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 1117–1130.
<https://doi.org/10.1145/2660267.2660330>
- Yin, R. K. (2009). *Case study research: design and methods* (4th ed., Vol. 5). Thousand Oaks, CA: Sage.
- Yorkshire and the Humber Joint Improvement Partnership. (2015). What is commissioning?
 Retrieved March 2, 2015, from <http://www.yhsccommissioning.org.uk/index.php?pageNo=539>
- Young, R. F. (2008). *Defining the information security posture: An empirical examination of structure, integration and managerial effectiveness*. University of North Texas.
- Young Foundation. (2011). *NHS chief executive's review of innovation in the NHS: summary of the responses to the Call for Evidence and Ideas*. London.
- Zachariadis, M., Scott, S., & Barrett, M. (2013). Methodological implications of critical realism for mixed-methods research. *MIS Quarterly*, *37*(3), 855–879. Retrieved from
<http://aisel.aisnet.org/misq/vol37/iss3/12>
- Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C., & Vigna, G. (2014). The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. *IMC '14 (ACM SIGCOMM Conference on Internet Measurement)*, 373–380. <https://doi.org/10.1145/2663716.2663719>
- Zhang, W., & Janssen, F. (s.d.). The relationship between PR and ROC curves. Darmstadt: Technische Universität Darmstadt.
- Zimmerman, D. H., & Wieder, D. L. (1977). The diary: diary-interview method. *Urban Life*, *5*(4), 479–498.
- Zinn, J. O. (2005). The biographical approach: a better way to understand behaviour in health and illness. *Health, Risk & Society*, *7*(1), 1–9. <https://doi.org/10.1080/13698570500042348>
- Zinn, J. O. (2006). Recent developments in sociology of risk and uncertainty. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *7*(1), article 30. Retrieved from
<http://www.qualitative-research.net/index.php/fqs/article/view/68/139>
- Zorabedian, J. (2014). How malware works: Anatomy of a drive-by download web attack. Retrieved March 6, 2017, from <https://blogs.sophos.com/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/>
- Zurn, P., Dal Poz, M. R., Stilwell, B., & Adams, O. (2004). Imbalance in the health workforce. *Human Resources for Health*, *2*, 13. <https://doi.org/10.1186/1478-4491-2-13>
- Zwerman, W. L. (1999). Profession/occupation without a history. *IEEE Annals of the History of Computing*, *21*(1), 66–70.

Appendices

Appendix A: Main search statements

Appendix B: Information behaviour of health care staff

Appendix C: Studies of other groups of health service staff

Appendix D: Web-based cybersecurity threats

Appendix E: Ethics documents

E.1. Proposal for research ethics review

E.2 Information School Research Ethics Panel: Letter of Approval

E.3 Research ethics review outcome

E.4: Participant information sheet and consent form

Appendix F: Interview guides:

F.1 Information technology staff (version 3.11)

F.2 Clinical staff (sample – nursing v. 1.1)

F.3 Library staff (version 2.0)

F.4 Communications staff (version 2.0)

F.5 Training and development staff (version 2.0)

F.6 Human resources staff (version 1.0)

F.7 Clinical staff (sample – nursing) (version 1.0)

Appendix G: HSCIC model Internet use policy

Appendix J: Mobile phones and infection control

Appendix J: Correspondence from NICE re: browser versions:

J.1. Internet browser survey of link resolver and knowledge base administrators

J.2 Letter from NICE to NHS IT managers

Appendix K: The ISMS plan-do-check-act cycle

Appendix L: Precision (specificity) and recall (sensitivity) of web filtering

Appendix M: Usability problems with mobile apps for accessing e-content

Appendix N: Summary of responses: access to YouTube / streamed services query

Appendix P: Information security and cybersecurity measures compared

Appendix R: Examples of data analysis matrices

Appendix A.

Main search statements

The following represent the main search statements used in literature searching for this thesis.

In the statements below, “ ” represents a search string, * a stem truncation, ? a wildcard truncation. AND, OR are Boolean operators; brackets enclose alternative search terms linked by OR. Statements in italics had document type limitations applied to them, where available within the individual databases.

Information behaviour

((“information (need*” OR use” OR behavio?” OR seeking)” OR “evidence seeking”) AND (clinician* OR doctor* OR nurs* OR midwi* OR “allied health” OR “health* professional*” OR therapist* OR dentist* OR psychologist* OR “social work”) AND (online OR Internet OR web-* or database*))

(“information need*” OR “information use” OR “information behavio?” OR evidence*) AND manager AND health

(theor* OR model*) AND (“information need*” OR “information use” OR “information behavio?”) AND health

(“information (need*” OR use” OR behavio?” OR seeking)” OR “evidence seeking”) AND (barrier* OR obstacle* OR hindrance*)

“professional identit*” AND (health OR NHS) AND “information (need*” OR use” OR behavio?” OR seeking)”

(“clinical autonomy” OR “freedom of enquiry”) AND “information (need*” OR use” OR behavio?” OR seeking)”

“clinical autonomy” AND (“freedom of enquiry” OR “academic freedom”)

e-learning

(e-learning AND (NHS OR “National Health Service”))

(e-learning AND (NHS OR “National Health Service”) AND “mobile devices”)

(e-learning AND (NHS OR “National Health Service”) AND (strategy* OR history OR development))

(NHS OR “National Health Service”) and m-learning

IT services

“IT service climate” AND (“IT service quality” OR “client satisfaction” OR “customer satisfaction” OR orientation)

“(IT OR “information technology”) service* management”

“IT service* management” AND “best practice framework*”

(“IT service framework*” OR “IT service management framework*”) AND (NHS OR “National Health Service”)

(NHS OR “National Health Service”) AND (COBIT OR ITIL)

Organisational characteristics of the NHS

“organizational culture” AND (review or overview) - *document type limitation used here where available*

“organizational culture*” AND health – limit to UK

organization* WITH (sub-culture* OR subculture)

Staff engagement, organisational values and organisational trust

(“staff engagement” OR “work engagement” OR “employee engagement”) AND (review OR overview OR introduction)

(“staff engagement” OR “work engagement” OR “employee engagement”) AND (“conceptual analysis” OR theor*)

(“staff engagement” OR “work engagement” OR “employee engagement”) AND (NHS OR “National Health Service”)

(“job resources” OR “job demands”) AND (“staff engagement” OR “work engagement” OR “employee engagement”)

(staff OR employee OR work) AND burnout AND (“conceptual analysis” OR theor*)

“organisational trust” AND (“conceptual analysis” OR theor*)

“organizational trust” AND (NHS OR “National Health Service”)

(“values statement*” OR “statement* of values”) AND (NHS OR “National Health Service”)

“NHS Constitution” AND values

“competing values framework” AND (review OR overview OR introduction)

“competing values framework” AND (NHS OR “National Health Service”)

Professionals within the NHS

“system of professions” AND (review OR overview OR introduction)

(“professional jurisdiction” OR “professional project”) AND (review OR overview OR introduction) - (“system of professions” OR “professional jurisdiction” OR “professional project”) AND (health OR NHS OR “National Health Service”)*

professionalism AND (“NHS OR “National Health Service”)

“professional identit” AND (“NHS OR “National Health Service”)*

(professional OR inter-professional) AND (conflict OR tension* OR rivalr* OR dispute* OR relations) AND (NHS OR (“National Health Service”)*

“health professional OR doctor* OR clinician*) AND manage* AND (conflict* OR tension* OR rivalr* OR dispute*OR relations) AND (NHS OR (“National Health Service”)*

(“professionalism OR professionalization) AND (IT OR ICT OR “information technology”)

“professional bureaucracy” AND (NHS OR (“National Health Service”)

“New Public Management” AND (NHS OR (“National Health Service”)

Information security / cybersecurity management

(“information technology” OR “information and communications technology” OR IT OR ICT) AND (sub-culture or subculture*)*

(“information security” OR cybersecurity OR cyber-security OR “cyber security”) AND (culture OR climate) AND “service management”

“information security polic” AND (development OR implementation OR “decision making” OR decision-making)*

*(“information security” OR cybersecurity OR cyber-security OR “cyber security”) AND power AND organi?ation**

power AND organi?ation AND (review OR overview OR introduction)*

power AND organi?ation AND “information (systems OR security)”*

(“information security” OR cyber-security OR cybersecurity OR “cyber security”) AND “risk (assess OR manag* OR analysis)”*

(“information security” OR cyber-security OR cybersecurity OR “cyber security”) AND end-users OR “end users” OR users)

(“information security” OR cyber-security OR cybersecurity OR “cyber security”) AND culture

“Web application security”

“web-borne malware” AND (vulnerabilit* OR threat*)

“drive-by download**”

malvertising

malware AND browser* AND (vulnerabilit* OR threat*)

malware AND (ActiveX OR Java) AND (vulnerabilit* OR threat*)

malware AND browser* AND (plug-in* OR plugin* OR add-on* OR BHO or “browser helper object**” AND (vulnerabilit* OR threat*))

(“user* OR end-user*”) AND (education OR training OR awareness OR SETA) (effectiveness OR evaluation)

(“Internet misuse” OR “Internet abuse” OR “cyber?loafing” or “cyber?slacking”) OR “personal web use” OR PWU) AND (review OR overview OR introduction)

(“Internet misuse” OR “Internet abuse” OR “cyber?loafing” or “cyber?slacking”) OR “personal web use” OR PWU) AND (health OR NHS)

(“Internet misuse” OR “Internet abuse” OR “cyber?loafing” or “cyber?slacking”) OR “personal web use” OR PWU) AND (health OR NHS) AND (prevent* OR deter* OR detect*)

(“Internet misuse” OR “Internet abuse” OR “cyber?loafing” or “cyber?slacking”) OR “personal web use” OR PWU) AND (health OR NHS) AND “organi?ational trust”

“acceptable use (policy OR policies)” AND (NHS OR “National Health Service”)

(“Internet misuse” OR “Internet abuse” OR “cyber?loafing” or “cyber?slacking”) AND monitoring AND “United Kingdom”

Web filtering / blocking

(web OR website) AND (filtering OR blocking OR “access control”) AND (review OR overview OR introduction)

(web OR website) AND (filtering OR blocking OR “access control”) AND “acceptable use polic**”

(web OR website) AND (filtering OR blocking OR “access control”) AND (health OR NHS)

(web OR website*) AND (filtering OR blocking OR “access control”) AND (over-blocking OR overblocking OR “false positive**”)

(web OR website*) AND (filtering OR blocking OR “access control”) AND ((ROC OR “receiver operating characteristic”) OR (specificity OR sensitivity))

(web OR website*) AND (filtering OR blocking OR “access control”) AND (over-blocking OR overblocking OR “false positive**”) AND (effect* OR impact* OR consequence*)

(web OR website) AND (filtering OR blocking OR “access control”)

Risk

risk AND “conceptual analysis”

(“theory of risk” OR “risk theory”) AND (review OR overview OR introduction)

(“cultural theory” OR Douglas OR Wildavsky) AND risk

“risk thermostat” OR “risk homeostasis”

“risk society” AND (review OR overview OR introduction)

(NHS OR “National Health Service”) AND (attitude* to risk” OR “risk appetite* OR risk-averse OR “risk averse” OR “aversion to risk”)

“risk perception” AND (“cyber security” OR cybersecurity OR cyber-security) OR “information security)

“risk perception” AND (“cyber security” OR cybersecurity OR cyber-security OR “information security) AND (“health service” OR NHS or healthcare)

“empathy gap” AND “IT services” AND (“health service” OR NHS or healthcare)

Diffusion of innovations

“diffusion of innovation” AND theor* AND (review OR overview OR introduction)*

“diffusion of innovation” AND (IT OR ICT OR “information technology”)*

“diffusion of innovation*” AND (IT OR ICT OR “information technology”) AND (NHS OR “National Health Service”)

(“organizational culture*” OR organizational values”) AND (“social media” OR Web 2.0”) AND conflict*

“IT-culture conflict” AND (NHS OR “National Health Service”)

“diffusion of innovation*” AND (“organizational readiness”) AND (NHS OR “National Health Service”)

(barrier* OR obstacle* OR hindrance*) AND “diffusion of innovation*” AND (NHS OR “National Health Service”)

“IT consumerization” OR “consumer IT” OR “shadow IT” OR “user-led innovation”) AND “diffusion of innovation*”

"IT consumerization" OR "consumer IT" OR "shadow IT" OR "user-led innovation") AND (IT department* OR "IT services")

"IT consumerization" OR "consumer IT" OR "shadow IT" OR "user-led innovation")

"IT consumerization" OR "consumer IT" OR "shadow IT" OR "user-led innovation") AND ("IT governance" OR security)

("social media" OR "Web 2.0") AND (policy OR policies OR guideline*)

("social media" OR "Web 2.0") AND (NHS OR "National Health Service")

("social media" OR "Web 2.0") AND (clinician* or "health professional*" OR nurs* OR therap*)

("diffusion of innovation*" OR adoption) AND ("social media" OR "Web 2.0")

("Bring Your Own Device" OR BYOD) AND "diffusion of innovation*"

("Bring Your Own Device" OR BYOD) AND (security OR risk)

("mobile device*" AND "diffusion of innovation*"

("mobile device*") AND (security OR risk OR governance)

("mobile device*") AND (NHS OR "National Health Service")

("National Health Service" OR NHS) AND ("technology acceptance" OR "information technology") AND attitude*

Appendix B. Information behaviour of multi-professional groups of health care staff

Table B.1 Information behaviour of health care staff: primary research

Authors	Date published	Country	Researchers' discipline/ background	Subjects	Methods	Research focus
Andrews, Pearce, Ireson, & Love	2005	USA	LIS/medical research	practitioner members of a primary care practice-based research network: medical, nursing, physician assistants	survey	information-seeking behaviour to improve LIS support; excluded clinical questions related to drug dosages or interactions
Doney, Barlow, & West	2005	UK	LIS / medical education	primary care staff in Nottingham and Rotherham	survey	usage of LIS, internet and biomedical databases; information literacy training needs
Thain & Wales	2005	UK	LIS	staff of colorectal cancer managed clinical network	survey semi-structured interviews	access to and use of library and knowledge services; informing design of cancer portal
Podichetty, Booher, Whitfield, & Biscup	2006	USA	medical research and education	health professionals attending CME programmes: medical; physical therapists, physician assistants	survey (IUHP questionnaire)	internet use and its effects among health professionals, including patients' perceptions of Internet information
Hider, Griffin, Walker, & Coughlan	2009	NZ	medical education / LIS	clinical staff in a single health board: medical, nursing, AHP, dental	survey	information-seeking behaviour using online resources provided by LIS
Rutland & Smith	2010	UK	LIS	representatives of occupational groups providing public health services	semi-structured interviews	Information needs of 'frontline' public health workforce, whether needs are being met, barriers to meeting needs
Sedghi, Sanderson, & Clough	2012	UK	LIS/computer science	health professionals in Sheffield teaching hospitals	think-aloud protocols in structured searching tasks; semi-structured interviews	resources used for medical image searching; relevance criteria applied to medical image searching
Kostagiolas, Ziavrou, Alexias, & Niakas	2012	Greece	LIS	all clinical staff (not auxiliaries) of Metaxa Cancer Hospital	survey	Information needs, resources preferences, obstacles to information seeking
Jackson et al.	2007	UK	various	health and social care professionals involved in providing care to children with health-care needs in Barnsley	survey	information-seeking behaviours, sources of information currently received, information requirements and preferences for future provision

Appendix C.

Studies of other groups of health service staff

Many of the themes that have featured in the accounts in Chapter 2 of the information behaviour of doctors, nurses and health service managers occur again in these studies. Social workers are an important group of professionals working within health services, most particularly in mental health and learning disabilities settings, where they frequently work in multidisciplinary teams within integrated services (Allen, 2014; Lilo & Vose, 2016). A number of research findings relating to social workers' information behaviour were thus of potential interest and importance. These related to lack of Internet access in the workplace, poor IT and information literacy skills, technophobia, poor understanding of library services, dependence upon verbal information sharing, lack of a research culture within the profession, and lack of management support for information-seeking in the workplace (Beddoe, 2010; Gannon-Leary, 2006; Gosling & Westbrook, 2004; Harrison, Hepworth, & de Chazal, 2004).

Particular phenomena have been noted in relation to the information behaviour of other groups of health professionals: the high levels of use of journals and websites by AHPs (Fell, Burnham, & Dockery, 2013; Haigh, 2006; Kloda & Bartlett, 2009; Nail-Chiwetalu & Ratner, 2007); the degree of variation in the use of bibliographic databases by AHPs according to professional group (physiotherapists very high, speech and language therapists low) (Fell et al., 2013; Nail-Chiwetalu & Ratner, 2007); the persistence of workplace cultures which discourage information seeking and restrict access to the Internet (Duffy, 2000; Gilmour et al., 2008; Shanahan, 2009, 2012; Shanahan, Herrington, & Herrington, 2009; Westerman & Hurt, 2007); the low levels of library use by AHPs and social workers (Haigh, 2006; Harrison et al., 2004); the perceptions of poor information literacy as a barrier to information-seeking among AHPs as well as among nurses (Fell et al., 2013; Kloda & Bartlett, 2009; Nail-Chiwetalu & Ratner, 2007); the relatively low level of use of the Internet by dentists (Funkhouser et al., 2012; Landry, 2006); and clinical psychologists' high level of knowledge of research methods and designs, coupled with low awareness of online information resources (Berke, Rozell, Hogan, Norcross, & Karpiak, 2011) and use of books for educational purposes (Wehmeyer & Wehmeyer, 1999).

Appendix D. Web-based cybersecurity threats

Phishing is defined as the act of sending an email or social media message to a user falsely claiming to be an established legitimate enterprise or trusted individual, in an attempt to lure the user into surrendering private information that will be used for identity theft (Webopedia, s.d.). Spear-phishing is a variant in which the messages are customised to a particular individual (Brozycki, 2009; Kassner, 2013). Spear-phishing is a variant in which the messages are customised to a particular individual (Brozycki, 2009; Kassner, 2013). Pharming employs a variety of techniques to direct users to malicious websites. One form of pharming, DNS cache poisoning, also known as search engine poisoning or DNS spoofing, exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards malicious ones (How-To Geek, 2015). DNS cache poisoning can occur without the user's knowledge or involvement. Malicious websites may install malware; they may also use attack techniques such as cross-site scripting, cross-site request forgery, SQL injection or so-called clickjacking to steal important credentials (such as logins and passwords) or other personal information from the victim in order to facilitate identity theft, or to gain unauthorised access to an application (Egele, Kirda, & Kruegel, 2009; Eshete, Villafiorita, Weldemariam, & Kessler, 2011; Grossman, 2012).

Pharming employs a variety of techniques to direct users to malicious websites. One form of pharming, DNS cache poisoning, also known as search engine poisoning or DNS spoofing, exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards malicious ones (How-To Geek, 2015). DNS cache poisoning can occur without the user's knowledge or involvement. Malicious websites may install malware; they may also use attack techniques such as cross-site scripting, cross-site request forgery, SQL injection or so-called clickjacking to steal important credentials (such as logins and passwords) or other personal information from the victim in order to facilitate identity theft, or to gain unauthorised access to an application (Egele, Kirda, & Kruegel, 2009; Eshete, Villafiorita, Weldemariam, & Kessler, 2011; Grossman, 2012).

In a drive-by download (2.6.2), cyber-attackers may gain access to and compromise a legitimate website to serve malicious pages via four prevalent mechanisms: the exploitation of vulnerabilities in web server security and server-side scripting applications, code injection attacks via user-contributed content, advertising, and third-party widgets. Such malicious pages typically contain JavaScript code, which may be obfuscated (thereby effectively unreadable) or polymorphic (the code

changes with each view), rendering it impossible to detect using signature-based antivirus solutions. There are five stages in a drive-by download: 1) the entry point (visiting the compromised website); 2) distribution (the compromised page redirects the browser to another website containing a so-called exploit kit); 3) exploit (the exploit kit probes the browser, operating system and other potentially vulnerable software (e.g. PDF reader, media player or browser extensions) looking for a vulnerability which it can attack); 4) infection (if the exploit kit discovers such a vulnerability in a browser component or extension, it can download the attack payload, i.e. the malware itself); 5) execution (the malware, of whatever type, runs on the infected computer) (Zorabedian, 2014).

So-called “black hat” search optimisation techniques are often used to lure unsuspecting end-users to malicious websites, which are thereby led to rank highly in search engine results for popular search terms (Julisch, 2013). The term “search engine optimisation” (SEO) in general refers to the methods and techniques, both technical and creative, that can be employed to improve a website’s rankings in web search engine results and drive traffic to its pages. “Black hat” techniques are those that are considered unethical, and which are banned by common search engines. They include so-called keyword stuffing (filling a web page with keywords), cloaking (showing to search engine crawlers different content from that shown to users), artificially increasing the number of links to a site through link farming or use of paid links, posting spam comments on other sites which incorporate back links, and plagiarising other sites to create duplicate content (Cahill & Chalut, 2009; Kent, 2006; Killoran, 2013; Malaga, 2008, 2010).

Phishing is defined as the act of sending an email or social media message to a user falsely claiming to be an established legitimate enterprise or trusted individual, in an attempt to lure the user into surrendering private information that will be used for identity theft (Webopedia, s.d.). Spear-phishing is a variant in which the messages are customised to a particular individual (Brozycki, 2009; Kassner, 2013). Spear-phishing is a variant in which the messages are customised to a particular individual (Brozycki, 2009; Kassner, 2013). Pharming employs a variety of techniques to direct users to malicious websites. One form of pharming, DNS cache poisoning, also known as search engine poisoning or DNS spoofing, exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards malicious ones (How-To Geek, 2015). DNS cache poisoning can occur without the user’s knowledge or involvement. Malicious websites may install malware; they may also use attack techniques such as cross-site scripting, cross-site request forgery, SQL injection or so-called clickjacking to steal important credentials (such as logins and passwords) or other personal information from the victim in order to facilitate identity theft, or to

gain unauthorised access to an application (Egele, Kirda, & Kruegel, 2009; Eshete, Villafiorita, Weldemariam, & Kessler, 2011; Grossman, 2012).

Pharming employs a variety of techniques to direct users to malicious websites. One form of pharming, DNS cache poisoning, also known as search engine poisoning or DNS spoofing, exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards malicious ones (How-To Geek, 2015). DNS cache poisoning can occur without the user's knowledge or involvement. Malicious websites may install malware; they may also use attack techniques such as cross-site scripting, cross-site request forgery, SQL injection or so-called clickjacking to steal important credentials (such as logins and passwords) or other personal information from the victim in order to facilitate identity theft, or to gain unauthorised access to an application (Egele, Kirda, & Kruegel, 2009; Eshete, Villafiorita, Weldemariam, & Kessler, 2011; Grossman, 2012).

In a drive-by download (2.6.2), cyber-attackers may gain access to and compromise a legitimate website to serve malicious pages via four prevalent mechanisms: the exploitation of vulnerabilities in web server security and server-side scripting applications, code injection attacks via user-contributed content, advertising, and third-party widgets. Such malicious pages typically contain JavaScript code, which may be obfuscated (thereby effectively unreadable) or polymorphic (the code changes with each view), rendering it impossible to detect using signature-based antivirus solutions. There are five stages in a drive-by download: 1) the entry point (visiting the compromised website); 2) distribution (the compromised page redirects the browser to another website containing a so-called exploit kit); 3) exploit (the exploit kit probes the browser, operating system and other potentially vulnerable software (e.g. PDF reader, media player or browser extensions) looking for a vulnerability which it can attack); 4) infection (if the exploit kit discovers such a vulnerability in a browser component or extension, it can download the attack payload, i.e. the malware itself); 5) execution (the malware, of whatever type, runs on the infected computer) (Zorabedian, 2014).

So-called "black hat" search optimisation techniques are often used to lure unsuspecting end-users to malicious websites, which are thereby led to rank highly in search engine results for popular search terms (Julisch, 2013). The term "search engine optimisation" (SEO) in general refers to the methods and techniques, both technical and creative, that can be employed to improve a website's rankings in web search engine results and drive traffic to its pages. "Black hat" techniques are those that are considered unethical, and which are banned by common search engines. They include so-

called keyword stuffing (filling a web page with keywords), cloaking (showing to search engine crawlers different content from that shown to users), artificially increasing the number of links to a site through link farming or use of paid links, posting spam comments on other sites which incorporate back links, and plagiarising other sites to create duplicate content (Cahill & Chalut, 2009; Kent, 2006; Killoran, 2013; Malaga, 2008, 2010).

*Appendix E.
Ethics documents*

E.1. Proposal for research ethics review
Information School

Proposal for
Research Ethics Review

Students	
This proposal submitted by:	
	Undergraduate
	Postgraduate (Taught) – PGT
x	Postgraduate (Research) – PGR

Staff	
This proposal is for:	
x	Specific research project
	Generic research project
This project is funded by:	

Project Title:	Access to e-resources within the English NHS: the role and impact of organisational cultures, information governance, and IT strategy		
Start Date:	01/10/2012	End Date:	30/09/2015

Principal Investigator (PI): <i>(student for supervised UG/PGT/PGR research)</i>	Catherine Ebenezer		
Email:	lip12cme@sheffield.ac.uk		

Supervisor: <i>(if PI is a student)</i>	Professor Peter Bath		
Email:	p.a.bath@sheffield.ac.uk		

Indicate if the research: <i>(put an X in front of all that apply)</i>	
<input type="checkbox"/>	Involves adults with mental incapacity or mental illness, or those unable to make a personal decision
<input type="checkbox"/>	Involves prisoners or others in custodial care (e.g. young offenders)
<input type="checkbox"/>	Involves children or young people aged under 18 years of age
<input type="checkbox"/>	Involves highly sensitive topics such as 'race' or ethnicity; political opinion; religious, spiritual or other beliefs; physical or mental health conditions; sexuality; abuse (child, adult); nudity and the body; criminal activities; political asylum; conflict situations; and personal violence.

Please indicate by inserting an "X" in the left hand box that you are conversant with the University's policy on the handling of human participants and their data.

x	We confirm that we have read the current version of the University of Sheffield <i>Ethics Policy Governing Research Involving Human Participants, Personal Data and Human Tissue</i> , as shown on the University's research ethics website at: www.sheffield.ac.uk/ris/other/gov-ethics/ethicspolicy
---	--

Part B. Summary of the Research

B1. Briefly summarise the project's aims and objectives:

(This must be in language comprehensible to a layperson and should take no more than one-half page. Provide enough information so that the reviewer can understand the intent of the research)

Summary:

The overall aim of the research is to investigate the possible relationship between stated policy regarding evidence-based practice and professional learning, particularly e-learning, and the actual provision of computing facilities and IT security practice at NHS trust level, both from a technical and an organisational perspective.

More specifically, the objectives of the research are to investigate:

- 1) the impacts of inadequate functionality and restrictions on access to information resources and applications on professional information seeking within the NHS;
- 2) the attitudes, presuppositions and practices of information governance, communications, human resources and technical staff which bear on how the security of networks and devices (PCs, laptops, and smartphones) is implemented within NHS trusts, in relation to overall organisational priorities and strategies.

B2. Methodology:

Provide a broad overview of the methodology in no more than one-half page.

- Overview of Methods:

It is proposed to carry out an exploratory case study using mixed methods, involving one or more geographically accessible NHS trusts, which may be of the same type or of different types. It could also, if indicated, involve publishers of e-resources and the current cohort of MSc Health Informatics students within the Information School; members of both groups are likely to have interesting experiences to investigate. It would follow an embedded, single-case design, treating the English NHS as the actual case, with the trust(s) and the groups of students and publishers' representatives. As a first stage, the nature and extent of e-access problems will be described, quantified and analysed, and an initial exploration undertaken of attitudes and values, probably via:

- 1) Semi-structured interviews with library and workforce development staff (3-5 per trust)
- 2) Semi-structured interviews with key informants (around 10 per trust) of staff within information governance, network security, human resources and communications departments, selected via purposive sampling
- 3) Obtaining from the trust IT departments technical information about information security

measures in place within the trust

4) The findings will be set in the context of documentary analysis, for each trust, of relevant strategy and risk assessment documents, policies, and information system documentation

5) Q-methodology could be used to investigate further the attitudes of information security and information governance staff to web-based information-seeking. The Q-sort could, if indicated, include statements about the nature of the “core business of the NHS”, and the core purposes of information technology within the NHS. as the embedded units of analysis (Yin, 2009).

6) If possible within the time available, telephone interviews will be conducted with representatives (5-8) of information providers (publishers, aggregators) for them to provide information about the technical aspects of problems they have encountered in setting up access to e-resources for NHS customers, and with members of the current cohort of MSc Health Informatics students within the Information School to report on technical problems they have encountered in relation to information-seeking.

If more than one method, e.g., survey, interview, etc. is used, please respond to the questions in Section C for each method. That is, if you are using both a survey and interviews, duplicate the page and answer the questions for each method; you need not duplicate the information, and may simply indicate, “see previous section.”

C1. Briefly describe how each method will be applied

Description – how will you apply each method?

Method (e.g., survey, interview, observation, experiment):

- 1) Interviews
 - 1) Semi-structured face-to-face and telephone interviews with members of relevant NHS staff groups and other relevant parties(see above under B2)
 - a) Semi-structured interviews with library and workforce development staff, including professional heads, to gain their perspectives on access to e-resources within the organisation and upon organisational readiness, in terms of technical infrastructure and support, for e-learning;
 - b) Semi-structured interviews with key informants (around 10 per trust) within information governance, network security, human resources and communications, to explore their assumptions about information-seeking, their understanding of their role and of organisational priorities in managing information risk and access to e-resources for teaching and learning;
 - c) Telephone interviews with representatives (5-8) of information providers (publishers, aggregators) for them to provide information about the technical aspects of problems they have encountered in setting up access to e-resources for NHS customers;
 - d) Telephone interviews with members of the current cohort of MSc Health Informatics students within the Information School, to identify problems they may have experienced in accessing information from with NHS networks.
- 2) Q methodology (if time allows)

Q methodology is said to be useful in profiling attitudes about a phenomenon, and seeks to measure the relative importance of personal beliefs on issues or debates of social or economic consequence. It is best suited to the task of unravelling the subjective structures, attitudes and perceptions of the person or issue that is being observed, and

is particularly appropriate for sensitive topics (Anandarajan et al., 2006). Its purpose in the present context would be to investigate further the attitudes of information security and information governance staff to web-based information-seeking. The method involves two stages. The first is the creation of a collection of around 40 statements, known as the Q-sample, representing themes or belief categories, in this case derived from the literature search and from the interviews as previously coded by the researcher. The second is the testing of the Q-sample on a group of respondents, known as the p-set; the respondents are invited to rank-order each of the statements on a scale representing their level of agreement with it, ranging from “most disagree” to “most agree” e.g. +5 “most agree”, +4 “strongly agree”, -2 “somewhat disagree”, -1 “slightly disagree, etc., generating a so-called Q-sort which includes the item rankings of each participant. The objective here is to sort the items. The completed Q-sort can then be analysed using factor analysis techniques.

- 3) Q methodology could involve a wider group of staff (probably around 25-30) than were able to participate in the interviews. The Q-sample would include statements representing beliefs and attitudes relating to the themes of the research, such as views concerning the nature of the “core business of the NHS” and the core purposes of information technology within the NHS, also statements about aspects of web-based information-seeking.

About your Participants

C2. Who will be potential participants?

- 1) NHS trust staff in various categories (see above, under C1)
- 2) Marketing and technical staff of companies providing information resources and e-learning platforms to the NHS (EBSCO, Emerald, Wolters Kluwer, ProQuest, Sage, Wiley, Blackboard, Cisco, Citrix etc.)
- 3) (Possibly) UoS MSc Health Informatics students

C3. How will the potential participants be identified and recruited?

For categories 1) and 2), potential participants will be identified as follows (see above under C2 for respondent categories):

- 1) Initially via recommendations or suggestions from the trust R&D Lead and Senior Librarian, thereafter via ‘snowball’ sampling
- 2) Via the researcher’s initial contacts with marketing departments at the companies concerned, and indirectly via a circular email to health librarians on the LIS-MEDICAL JISCmail list inviting them to suggest potential respondents.

Individuals identified initially within categories 1) and 2) will be contacted by the researcher via email or letter with information about the study and an invitation to take part.

- 3) Potential respondents in this category are the MSc Health Informatics students. Professor Peter Bath will circulate an email to members of this group (category 3) on

the researcher's behalf, with an invitation to contact the researcher directly if they wish to participate.

C4. What is the potential for physical and/or psychological harm / distress to participants?

Minimal, if any, beyond what would be experienced in day-to-day work.

C5. Will informed consent be obtained from the participants?

X	Yes
	No

If Yes, please explain how informed consent will be obtained?

Each participant will be sent an information sheet in advance of the interview. Informed consent will be obtained in writing at the start of the interview, with an opportunity to raise questions with the researcher immediately beforehand.

If No, please explain why you need to do this, and how the participants will be de-briefed?

C6. Will financial / in kind payments (other than reasonable expenses and compensation for time) be offered to participants? (Indicate how much and on what basis this has been decided)

No

About the Data

C7. What data will be collected? (Tick all that apply)

	Print	Digital
Participant observation		
Audio recording		x
Video recording		
Computer logs		
Questionnaires/Surveys		
Other: trust documents (policies, strategies, technical documentation)	x	x
Other:		

C8. What measures will be put in place to ensure confidentiality of personal data, where appropriate?

The researcher's desktop computer at home and university laptop are both password-protected and have internet security (firewall and anti-malware) and encryption software (Boxcryptor) installed; see below under C9.

Individual participants will be assigned codes according to an encrypted, password-protected 'master list' stored on the researcher's U: drive; these codes will be used in filenames, transcripts, analysis and reports.

Within reports of the research the trust(s) will be referred to by pseudonym(s) and described only as, e.g. 'an acute NHS trust in the north of England', 'a mental health / learning disabilities trust in northern England' etc. Any information that could indirectly identify the trust or individual participants will be removed in the course of transcribing recordings of interviews. An anonymisation log will be kept, which will be password-protected and stored on the researcher's U: drive.

C9. How/Where will the data be stored?

Following a recorded interview, audio files will be uploaded from the recording device as soon as possible to the researcher's personal cloud storage (Microsoft SkyDrive) and deleted from the device. A university-supplied laptop will be used for this purpose, using the Boxcryptor encryption service (<https://www.boxcryptor.com>), which supports a number of cloud storage services including SkyDrive. A backup copy will also be uploaded to the researcher's U: drive. These files will not be shared. No other portable media or devices will be used. Anonymised transcripts will subsequently be uploaded to NVivo loaded on the researcher's desktop PC at home for analysis.

All project data will be held in specific directories within MS SkyDrive and retained until the PhD has been awarded and subsequent publications accepted.

Paper records containing personal or confidential data (e.g. signed consent forms) will be stored within the researcher's locked filing cabinet at the School.

C10. Will the data be stored for future re-use? If so, please explain

Future use of the data by other researchers is not currently envisaged.

About the Procedure

E11. Does your research raise any issues of personal safety for you or other researchers involved in the project (especially if taking place outside working hours or off University premises)? If so, please explain how it will be managed.

Not to my knowledge; the interviews etc. will be carried out in normal office hours within the trust premises.

References

Anandarajan, M., Paravastu, N., & Simmers, C. a. (2006). Perceptions of personal Web usage in the workplace: AQ-methodology approach. *CyberPsychology and Behavior*, 9(3), 325–35.

Yin, R. K. (2009). *Case study research: design and methods* (4th ed.). Thousand Oaks, CA: Sage.

The University of Sheffield.
Information School

Research Ethics Review Declaration

Title of Research Project:

Access to e-resources within the English NHS: the role and impact of organisational cultures, information governance, and IT strategy

We confirm our responsibility to deliver the research project in accordance with the University of Sheffield's policies and procedures, which include the University's '*Financial Regulations*', '*Good Research Practice Standards*' and the '*Ethics Policy Governing Research Involving Human Participants, Personal Data and Human Tissue*' (Ethics Policy) and, where externally funded, with the terms and conditions of the research funder.

In submitting this research ethics application form I am also confirming that:

- The form is accurate to the best of our knowledge and belief.
- The project will abide by the University's Ethics Policy.
- There is no potential material interest that may, or may appear to, impair the independence and objectivity of researchers conducting this project.
- Subject to the research being approved, we undertake to adhere to the project protocol without un-agreed deviation and to comply with any conditions set out in the letter from the University ethics reviewers notifying me of this.
- We undertake to inform the ethics reviewers of significant changes to the protocol (by contacting our academic department's Ethics Coordinator in the first instance).
- we are aware of our responsibility to be up to date and comply with the requirements of the law and relevant guidelines relating to security and confidentiality of personal data, including the need to register when necessary with the appropriate Data Protection Officer (within the University the Data Protection Officer is based in CiCS).
- We understand that the project, including research records and data, may be subject to inspection for audit purposes, if required in future.
- We understand that personal data about us as researchers in this form will be held by those involved in the ethics review procedure (e.g. the Ethics Administrator and/or ethics reviewers) and that this will be managed according to Data Protection Act principles.
- If this is an application for a 'generic' project all the individual projects that fit under the generic project are compatible with this application.
- We understand that this project cannot be submitted for ethics approval in more than one department, and that if I wish to appeal against the decision made, this must be done through the original department.

Name of the Student (if applicable):

Catherine Ebenezer

Name of Principal Investigator (or the Supervisor):

Professor Peter Bath

Date: 10/10/2013

E.2 Information School Research Ethics Panel: Letter of Approval

Date: 14th November 2013

TO: Catherine Ebenezer

The Information School Research Ethics Panel has examined the following application:

Title: Access to e-resources within the English NHS: the role and impact of organisational cultures, information governance, and IT strategy

Submitted by: Catherine Ebenezer

And found the proposed research involving human participants to be in accordance with the University of Sheffield's policies and procedures, which include the University's '*Financial Regulations*', '*Good Research Practice Standards*' and the '*Ethics Policy Governing Research Involving Human Participants, Personal Data and Human Tissue*' (Ethics Policy).

This letter is the official record of ethics approval by the School, and should accompany any formal requests for evidence of research ethics approval.

Effective Date: 14th November 2013

A handwritten signature in black ink, appearing to be 'C. Ebenezer', written in a cursive style.

E.3. Research ethics review outcome

The University of Sheffield.

Information School

Name of Ethics Coordinator (or replacement):	Dr Angela Lin
Date of the Review:	14 th November 2013

I confirm that I do not have a conflict of interest with this project proposal (insert "x")	x
---	---

Research Project Title:	Access to e-resources within the English NHS: the role and impact of organisational cultures, information governance, and IT strategy
Principal Investigator:	Catherine Ebenezer
Supervisor: (if PI is a student)	Peter Bath

This proposal is (put an X in front on only one)	
x	Approved (as submitted)
	Pending approval provided compulsory requirements are met (explained in A)
	Not approved (explained in B)

A. Compulsory requirements that must be met:

Please revise your initial proposal and resubmit. Once these requirements are approved the research may commence.

B. If the proposal is not approved, clearly explain why:

Research Issues: These issues were identified by the reviewers. They are suggestions for consideration only, have no effect on the research ethical issues.

I am not clear how the suggested number of semi-structured interviews (10) within the NHS Trust/Trusts will give a clear picture of the opinions of the various groups identified.

There seems to be an imbalance in the depth of opinions sought from library staff (3/5) in relation to other stakeholder groups. Why not have 3/5 interviews with all stakeholder groups?

There may be an explanation for this.

Section C3.1) highlights snowball sampling, which is methodologically a weak way of sampling and it's worth considering if this is the best option. It may well be due to access issues, but important to think about and potentially reconsider.

Why are the students interviewed on the phone? Is there a specific reason to do it this way? Also, is there a methodological issue (similar to weakness of snowball sampling) in interviewing students at your own University? Is it worth thinking about gaining access to students at a different University?

In terms of the various strategies for anonymising participants, how will the course be identified? Similar to the way in which the trusts and publishers (though details of how publishers are anonymised only appear on the relevant consent form) are dealt with, how will the course be de-identified?

On the consent forms for the face to face interviews it might be useful to highlight where the Interviews will take place.

Finally, I found the objectives of the study written in a rather dense way that makes it quite hard to make sense of them on first reading. This does not make them bad objectives, but it's worth considering if they could be phrased slightly differently so that the objectives of the research are made clearer to participants.

The student has clearly covered all issues regarding data security and participant ambiguity and has proposed appropriate measures for these.

C.4 Participant information sheet and consent form

The University of Sheffield. Information School	<i>Access to e-resources within the NHS in England: the role and impact of organisational culture, information governance, and IT strategy</i>
--	--

Researchers

Catherine Ebenezer

Information School, University of Sheffield, Regent Court, 211 Portobello, Sheffield, S1 4DP

lip12cme@sheffield.ac.uk

01270 669589 / 07876 494421

Purpose of the research

The overall aim of the research is to investigate the possible relationship between stated policy regarding evidence-based practice and professional learning, particularly e-learning, and the actual provision of computing facilities and IT security practice at NHS trust level, both from a technical and an organisational perspective. More specifically, the objectives of the research are to investigate:

- 1) the impacts of inadequate functionality and restrictions on access to information resources and applications on professional information seeking within the NHS;*
- 2) the attitudes, presuppositions and practices of information governance, communications, human resources and technical staff which bear on how the security of networks and devices (PCs, laptops, tablets and smartphones) is implemented within NHS trusts, in relation to overall organisational priorities and strategies.*

Who will be participating?

The researcher is seeking to conduct semi-structured interviews with library and workforce development staff to gain their perspectives on access to e-resources within the organisation and upon organisational readiness, in terms of technical infrastructure and support, for e-learning, with clinical professional leads, and with managers from information governance, IM&T, human resources and communications.

What will you be asked to do?

The researcher will ask you to participate in a semi-structured interview of up to one hour in length.

What are the potential risks of participating?

The risks of participating are the same as those experienced in everyday working life.

What data will we collect?

The interviews will be audio-recorded.

What will we do with the data?

Following a recorded interview, audio files will be uploaded from the recording device as soon as possible to the researcher's personal cloud storage and deleted from the device. A university-supplied encrypted laptop will be used for this purpose. A backup copy will also be uploaded to the researcher's university network drive. These files will not be shared. No other portable media or devices will be used. Anonymised transcripts will subsequently be uploaded to the researcher's desktop PC at home for analysis.

All project data will be held in specific directories within the researcher's cloud storage and retained until the PhD has been awarded and subsequent publications accepted.

Signed consent forms will be stored within the researcher's locked filing cabinet at the Information School. Future use of the data by other researchers is not currently envisaged.

Will my participation be confidential?

Individual participants will be assigned codes according to an encrypted, password-protected 'master list' stored on the researcher's university network drive; these codes will be used in filenames, transcripts, analysis and reports.

Within reports of the research the trust will be referred to by pseudonym(s) and described only as, e.g. 'an acute NHS trust in the north of England'. Any information that could indirectly identify the trust or individual participants will be removed in the course of transcribing recordings of interviews.

What will happen to the results of the research project?

The results of this study will be included in the researcher's PhD thesis, which will be publicly available via the White Rose eTheses Online (WREO) website <http://etheses.whiterose.ac.uk/> and in journal articles; also a summary of the results will be available from the researcher on request.

I confirm that I have read and understand the description of the research project, and that I have had an opportunity to ask questions about the project.

I understand that my participation is voluntary and that I am free to withdraw at any time without any negative consequences.

I understand that I may decline to answer any particular question or questions. If I stop participating at all time, all of my data will be purged.

I understand that my responses will be kept strictly confidential, that my name or identity will not be linked to any research materials, and that I will not be identified or identifiable in any report or reports that result from the research.

I give permission for the research team members to have access to my anonymised responses.

I agree to take part in the research project as described above.

Participant Name (Please print)

Participant Signature

Researcher Name (Please print)

Researcher Signature

Date

Note: If you have any difficulties with, or wish to voice concern about, any aspect of your participation in this study, please contact Dr. Angela Lin, Research Ethics Coordinator, Information School, The University of Sheffield (ischool_ethics@sheffield.ac.uk), or to the University Registrar and Secretary.

Appendix F.

Interview guides

F. 1 Information technology staff (version 3.11)

Basic factual information:

- How many staff do you manage?
- Number of hospital sites? PCs?
- Are any IT functions outsourced? If so, which?
- Wi-Fi support? Staff? Patients? Both?
- Mobile device support / provision?
- What web security device(s) are used within your Trust? (web security gateway e.g. WebSense, WebMarshal; proxies; firewalls, etc.)?
- What is/are the web browser(s) in general use? Are alternatives permitted for particular purposes? How are browser add-ons managed/updated?
- Contacts with LIS/e-learning/CPD functions?
- Trust LIS / other LIS?
- T&D
- Professional educators? Medicine, nursing, AHP, pharmacy, etc.?
- CKO?

Could you please outline for me your role within the IT department, particularly as it relates to information security within the trust?

In an era of increasing information security threat levels, the staff responsible for information security within the trust obviously have a difficult task in safeguarding the security and integrity of its IT infrastructure.

How would you describe your main priorities in information security?

What are the most difficult issues that you face?

How would you characterise the general approach to network / information security within the trust's information governance structures? What would you say were the main strengths and weaknesses of this approach? How well do the existing structures work?

In addressing information security problems generally, what are your main sources of professional information and guidance?

What communication channels does the IT department have across the trust for informing strategic planning mechanisms for information systems development and for obtaining feedback from internal customers? How effective would you say that they were?

In particular, through what channels are you and your colleagues generally informed of the IT system requirements of e-learning and 'library-related' applications accessed by trust staff?

Looking now at more day-to-day issues: writers on information security often justify their decisions on practical security matters by reference to "business need".

How do you understand "business need" within the NHS?

How in practice is a "business need" established?

How do you perceive, or where do you locate, library / knowledge / information services in relation to overall NHS "business need"

In the context of information resources, what, for instance, might or might not constitute a legitimate "business need"?

What is your view of / what approach is taken by your department to the following?

- Professional networking sites e.g. LinkedIn, ResearchGate, doc2doc, WeNurses
- Prezi
- Web conferencing solutions requiring client software installation, e.g. GoToMeeting, WebEx
- Skype
- (Professional) resource sharing sites e.g. Slideshare, educational YouTube channels?
- Google apps
- Professional use of Twitter, Facebook, YouTube, Pinterest
- Blogs, wikis, portals
- Personal cloud storage, e.g. Dropbox, OneDrive?

How would you rate the trust's e-learning readiness from a technical perspective?

It is often said that "Users are the weakest link". Can you understand why someone might say that?

What approach is taken to the enforcement of acceptable use policies and other information security-related policies? (Technical means, disciplinary measures, a mixture of both?) On what basis are such decisions made?

If a 'legitimate' website (i.e. one which has not been compromised as a delivery vehicle for malware and whose content is of potential professional relevance for NHS staff) is incorrectly blocked by a security device, i.e. there is a false positive, is there a process within the trust for getting that site unblocked? If so, what is it, and how long does it usually take?

About how many such requests would you estimate are received in any one month?

To what extent do you perceive that false positives create problems for users?

Is the national whitelist of 'never to be blocked' websites (produced by LKSL IMTG) implemented on [the trust's web security device]?

The article I sent you by Prince et al. from the journal *Medical Education* about e-resource availability within the NHS comments as follows on their findings: "Shouldn't we be managing the risks more effectively in order to allow learners the freedom to use IT resources to better effect?"

Could you comment on your overall approach to the management of risk? What in practice constitutes an acceptable level of risk?

Has the trust suffered any form of data loss or data breach within the last few years?

If so, what would you say have been the effects in terms of information security and information governance policy and practice?

F.2 Information governance staff (version 1.2)

Could you please outline for me the scope of your role within information governance within the Trust? How does it relate to risk management?

Information security risk management is obviously part of the picture. In an era of increasing information security threat levels, the staff responsible for information security within the Trust obviously have a difficult task in safeguarding the security and integrity of its IT infrastructure.

Within [name of Trust] how far / to what extent does information governance have a role in information security?

What are the most difficult issues that you face in information governance?

How would you rate your own and your colleagues' understanding of the technical issues in information security that relate to information governance? How dependent are you in practice on members of the IT staff?

In addressing information security problems generally, what are your main sources of professional information and guidance?

How would you characterise the general approach to information security risk within the Trust's information governance structures? What would you say were the main strengths and weaknesses of this approach? How well do the existing structures work?

I am particularly interested in the Trust's approach to staff use of mobile devices, and in social media access and use in relation to risk management, professional cultures and overall organisational culture. What are you able to tell me in general? (I am concerned more with staff use of social media for professional purposes than with organisational use for public engagement purposes, although the two are evidently related.)

Writers on information security often justify their decisions on practical security matters by reference to "business need".

How do you understand "business need" within the NHS?

How in practice is a "business need" established?

In the context of information resources, what, for instance, might or might not constitute a legitimate “business need”?

(It might help to imagine, for instance, that a request has been made to the IT Department to provide access to a web conferencing application such as Blackboard Collaborate or GoToMeeting, or to Second Life for e-learning purposes).

What communication channels does the Information Governance department have relating to information security across the Trust and for obtaining input/feedback from internal stakeholders regarding the impact of information governance policies? How effective would you say that they were?

Many writers on information system security speak of an inevitable ‘trade-off’ between the functionality and the security of computer systems. Are you aware of any such issues within the trust’s systems and services that might bear on the provision of access to e-resources?

[Bruce Schneier, the author of a well-known book on information security, *Secrets and Lies* (Wiley, 2000) famously stated that “Users are the weakest link”. Can you understand why someone might say that? What might be the implications for the trust?]

What approach is taken to the enforcement of acceptable use policies and other information security-related policies? (Technical means, disciplinary measures, a mixture of both?) On what basis are such decisions made?

If a ‘legitimate’ website (i.e. one which has not been compromised and whose content is of potential professional relevance for NHS staff) is blocked by a security device, is there a process within the trust for getting that site unblocked? If so, what is it, and how long does it usually take?

Has the trust suffered any form of data loss or data breach within the last few years?

If so, what would you say have been the effects in terms of information security and information governance policy and practice?

F.3 Interview guide: library / information managers (version 2.0)

Could I please ask you some background questions about the library?

How long have you yourself been in post?

Which organisations and staff groups do you serve?

How is your stock and IT infrastructure provided and supported?

I sent you a synopsis of findings of the survey on e-resource availability carried out by the then Technical Design Authority Group (TDAG) of SHALL (Strategic Health Authority Library Leads) in 2008 following a post on the LIS-MEDICAL JISCmail list by a library manager in Teesside, John Blenkinsopp, and his subsequent article in *He@lth Information on the Internet (issue 62, 2008)*. This related primarily to library-managed e-resources, but had a section devoted to e-learning.

Along the lines of the survey, could you please outline in as much detail as possible any problems you have encountered with access to electronic content, or that learners have reported? I am interested both in technical and in organisational issues, if such exist.

How well in general would you say that the Trust's network infrastructure now supports e-resource access?

Do your readers ever report to you problems in accessing or using electronic content?

Do learners access e-learning content on Trust smartphones or on their own smartphones and tablets? If so, what issues does this raise?

If a 'legitimate' website (i.e. one which has not been compromised and whose content is of potential professional relevance for NHS staff) is blocked by a security device, is there a process within the Trust for getting that site unblocked? If so, what is it, and how long does it usually take?

To what extent do you perceive that 'over-blocking' of legitimate websites creates problems for users?

Is the national whitelist of 'never to be blocked' websites (produced by SIMTG, TDAG's successor) implemented on [the trust's web security device]?

How do you perceive the attitude of IT and information governance staff in dealing with e-resource access problems? And library issues in general?

Has the Trust suffered any form of data loss or data breach within the last few years?

If so, what would you say have been the effects in terms of information security and information governance policy and practice?

F.4 Communications staff (version 2.0)

For the purposes of my research I am concerned mainly with social media and the benefits, as well as the risks, for information security as well as for corporate reputation, which they present for organisations.

The TDAG survey (which I sent you) highlighted access to social media as a particular problem. A number of information resources which provide content that are highly relevant for NHS staff have a 'social' component (e.g. YouTube, SlideShare, ResearchGate). Also, blogs, wikis and discussion boards are frequently used in e-learning.

Could you please outline for me your own role in communications?

Social media, even those with a professional and educational focus, evidently present a huge range of issues for organisations.

What approach has been taken corporately to social media? What are [name of Trust's] priorities? What have been the main operative considerations?

Have particular policies or guidance on use of social media been produced within [name of Trust]?

F. 5 Training and development staff (version 3.0)

Can you please tell me about the areas for you are responsible?

I sent you a synopsis of findings of the survey on e-resource availability carried out by the then Technical Design Authority Group of SHALL (Strategic Health Authority Library Leads) in 2008. This related primarily to library-managed e-resources, but had a section devoted to e-learning.

Along the lines of the survey, could you please outline in as much detail as possible any problems you have encountered with access to e-learning content, or that learners have reported? I am interested both in technical and in organisational issues, if such exist.

There have been huge organisational changes within the NHS, and notable developments in the provision of e-learning within the NHS, since 2008. How and in what areas do you perceive that have things changed for training and development since then? I am interested both in national and in local developments.

What systems are in place for managing the e-learning undertaken by [name of Trust] staff?

How would you rate the Trust's readiness for e-learning?

Does the Trust's PC and network infrastructure, and the way it is managed, provide an adequate platform for e-learning, in your view? In particular, how widely available to staff are computers that meet system requirements (sound cards, browser functionality etc.) to run e-learning applications?

Do learners access e-learning content on trust smartphones or on their own smartphones and tablets? If so, what issues does this raise?

Some social media applications, such as blogs and wikis, and also resource sharing sites such as SlideShare and YouTube, are widely used in e-learning. The TDAG survey, whose findings we discussed earlier, highlighted social media as a particular problem.

Are you aware of any policies or guidance on use of social media that have been produced within [name of Trust]?

Have you encountered any issues with social media applications?

How involved is the Trust's library service with provision of support for e-learning?

How do you perceive the attitude of IM&T and information governance staff in relation to information resources and e-learning?

F. 6 Human resources staff (version 1.0)

Could you please outline for me your own role within HR, particularly with relation to ESR implementation within the trust?

My interest is primarily in 1) computer misuse as a disciplinary issue 2) social media policy 3) the overall effects of blocking access to web-based information resources and applications.

'Computer misuse is not an IT problem, it's a management problem.' Do you agree? What are the practical implications of your view?

What approach is taken within the Trust to the enforcement of acceptable use policies and other information security-related policies? (Technical means, disciplinary measures, a mixture of both?)
On what basis are such decisions made?

Social media, even those with a professional and educational focus, present a huge range of issues for organisations.

What would you say are the main issues in general?

What stage has the policy process regarding social media reached at [name of Trust]? What are [the Trust's] priorities?

In an era of increasing information security threat levels, the staff responsible for information security within the trust obviously have a difficult task in safeguarding the security and integrity of its IT infrastructure , so ...

Does e-learning raise particular information security issues of which you are aware?

Should the Prezi.com web application be blocked, as I am told it is within [name of Trust]? What issues does the blocking of websites and web applications raise?

Has the Trust suffered any form of data loss or data breach within the last few years?

If so, what would you say have been the effects on the organisation in terms of general culture?

F.7 Clinical staff (sample – nursing v. 1.1)

Can you please tell me about the areas for you are responsible?

I sent you a synopsis of findings of the survey on e-resource availability carried out by the then Technical Design Authority Group of SHALL (Strategic Health Authority Library Leads) in 2008, and of an article by Prince, Cass and Klaber (2010). These related primarily to library-managed e-resources, such as bibliographic databases, e-journals and e-books, and to e-learning.

Along the lines of the 'TDAG' survey, could you please outline in as much detail as possible any problems reported to you that staff or students on placement have encountered with access to e-resources, or that you have personally experienced? I am interested both in technical and in organisational issues, if such exist.

Have you any other comments to make about these articles?

There have been huge organisational changes within the NHS in England as a whole, and notable developments in the provision and availability of e-resources and e-learning within the NHS, since 2008. How and in what areas do you perceive that have things changed within [nurse] education since then? I am interested both in national and in local developments.

Have you been involved at all in the provision of e-learning? If so, please tell me about this.

How would you rate your Trust's organisational and technical readiness for e-learning?

Are there cultural implications, do you think, in rolling out e-learning within your Trust?

How would you rate the adequacy / suitability of your Trust's PC and network infrastructure, and the ways in which it is managed, as a platform for access to professional learning content, and in particular e-learning? In particular, how widely available to staff are computers that meet system requirements (sound cards, browser functionality etc.) to run e-learning applications?

To what extent are staff and students on placement access professional learning content on trust smartphones or on their own smartphones and tablets? What issues does this raise?

Some Web 2.0 and social media applications, such as podcasts, blogs and wikis, and also resource sharing sites such as SlideShare and YouTube, are widely used in e-learning. The TDAG survey, whose findings we discussed earlier, highlighted access to social media as a particular problem.

Are you aware of any policies or guidance on use of social media that have been produced within your Trust?

Have you encountered any issues with blocking of Web 2.0 or social media applications? If so, did you attempt to get the site unblocked? What was the outcome?

What is the relationship of education and training within your profession to the Trust's library service?

How do you perceive the attitude of IM&T and information governance staff within your Trust in relation to e-learning and access to learning content?

F.8 NICE manager (version 1.0)

Could I please ask you some background questions about your role at NICE?

How long have you yourself been in post?

My contact with you arose from a survey I heard about that you were conducting of browser availability across the NHS following reports that some library staff were unable to administer the link resolver or OpenAthens owing to browser incompatibilities.

Could you please tell me the full story about that?

What wider issue does this raise, do you think? (e.g. relating to NHS IT and how it is managed?)

I sent you a synopsis of findings of the survey on e-resource availability carried out by the then Technical Design Authority Group (TDAG) of SHALL (Strategic Health Authority Library Leads) in 2008, and another article by Prince et al. with similar findings.

What would your comments be on this and on the article by Prince et al.? Is the situation they describe still the same? Worse? Better?

Are there other issues relating to NHS IT and access to NHS Evidence content of which you are aware?

Thinking perhaps more widely, are you able to comment on the 'politics' of all this and of the role and position of NHS Evidence?

*Appendix G.
HSCIC model Internet use policy*

[insert logo here]

Policy title:	[Insert title here]
---------------	---------------------

Issue date:	[Enter date here]	Review date:	[Enter date here]
-------------	-------------------	--------------	-------------------

Version:	[Insert version number here]	Issued by:	[Enter Directorate here]
----------	------------------------------	------------	--------------------------

Aim:	[Insert broad policy aim here. See Section 2.2]
------	---

Scope:	[Insert scope of policy here]
--------	-------------------------------

Associated documentation:	Legal Framework: [For example The Data Protection Act (1998), Copyright Designs & Patents Act (1988), Computer Misuse Act (1990), Human Rights Act (1998)] Policies: [Enter any policies that relate to this policy. For example, staff discipline, email, Information Security]
Appendices:	[Note any appendices here]
Approved by:	[Enter relevant Board/Post here]
Date:	[Enter date approved here. This may differ from the date of issue]

Review and consultation process:	[Enter review details here. For example, 'Annually from review date above. Information Governance Board to oversee process']
Responsibility for Implementation & Training:	[Day to day responsibility for implementation: officer title] [Day to day responsibility for training: officer title]

HISTORY

Revisions:	[Enter details of revisions below]	
Date:	Author:	Description:

Distribution methods:	[Enter the methods used to distribute the policy here]
-----------------------	--

INTRODUCTION

This document defines the Internet use Policy for [enter name of organisation]. The Internet use Policy applies to all users of the Internet and relevant people who support the Internet system. The Internet is a general term that covers access to numerous computers and computer systems worldwide that are accessed electronically. Such systems include the World Wide Web (WWW), email (dealt with in a separate policy), File Transfer Protocol (FTP), newsgroups, Gopher, etc. The Organisation uses NHSnet to access these systems. This document:

- Sets out the Organisation's policy for the protection of the confidentiality, integrity and availability of the Internet system.
- Establishes Organisation and user responsibilities for the Internet system.
- Provides reference to documentation relevant to this policy.

1. OBJECTIVE

The objective of this policy is to ensure the security of [enter name of organisation] Internet system. To do this the Organisation will:

- 1.1. Ensure Availability - Ensure that the Internet system is available for users.
- 1.2. Preserve Integrity - Protect the Internet system from unauthorised or accidental modification ensuring the accuracy and completeness of the Organisation's assets.
- 1.3. Preserve Confidentiality - Protect assets against unauthorised disclosure.

The purpose of this policy is to ensure the proper use of the Organisation's NHS Internet system and make users aware of what the Organisation deems as acceptable and unacceptable use of its Internet system. By following the guidelines in this policy, the Internet user can minimise the legal risks involved in the use of Internet. If any user disregards the rules set out in this Internet use Policy, the user will be fully liable and may be subject to disciplinary action by the Organisation.

2. ORGANISATION RESPONSIBILITIES

- 2.1. The Organisation will ensure that all users are properly trained before using the Internet system.
- 2.2. The Organisation will take all reasonable steps to ensure that users of the Internet service are aware of policies, protocols, procedures and legal obligations relating to the use of Internet. This will be done through training and staff communications at departmental and Organisation-wide levels.
- 2.3. The Organisation will ensure all users of the Internet are registered.

3. ACCESS TO THE INTERNET SYSTEM

- 3.1. Anyone wishing to open an Internet account must obtain an Internet Access Application Agreement from the IT Department. Complete the agreement and return it to the IT department.

4. BEST PRACTICES

- 4.1. The Organisation considers the Internet as an important means of communication and recognises the importance of proper Internet content and speedy replies in conveying a professional image and delivering good customer service. Therefore the Organisation wishes users to adhere to the following guidelines:
 - 4.2. Acceptable Internet Usage
 - 4.2.1. To access research material and other information relevant to your work.
 - 4.2.2. To access web sites and webmail accounts for personal use [delete if not applicable] so long as this does not interfere with work.

4.3. Unacceptable Internet Usage

- 4.3.1. Creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- 4.3.2. Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material.
- 4.3.3. Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people.
- 4.3.4. Creating or transmitting “junk-mail” or “spam”. This means unsolicited commercial webmail, chain letters or advertisements.
- 4.3.5. Using the Internet to conduct private or freelance business for the purpose of commercial gain.
- 4.3.6. Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user’s data or hardware.
- 4.3.7. Downloading streaming video or audio for entertainment purposes.

5. SYSTEM MONITORING

- 5.1. All Internet traffic is logged automatically (each site a user visits is included in the log, with the time visited and pages viewed) to ensure that damaging code or viruses do not enter the organisation’s network or systems. The organisation also uses [delete if not applicable] software that prevents users visiting sites that may contain illegal or pornographic material. These logs are audited periodically by the [enter appropriate officer title].
- 5.2. If there is evidence that you are not adhering to the guidelines set out in this policy, the Organisation reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action.

6. QUESTIONS

- 6.1. If you have any questions or comments about this Internet use Policy, please contact the [enter appropriate officer title and contact details]. If you do not have any questions the Organisation presumes that you understand and are aware of the rules and guidelines in this Internet Use Policy and will adhere to them.

7. DEFINITIONS

7.1. Defamation - What is defamation?

A published (spoken or written) statement or series of statements that affects the reputation of a person (a person can be a human being or an organisation) and exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true then it is considered slanderous or libellous and the person towards whom it is made has redress in law.

What you must not do

Make statements about people or organisations on any web pages you are including on the website without verifying their basis in fact.

What are the consequences of not following this policy?

You and the Organisation may be subject to expensive legal action.

7.2. Harassment - What is harassment?

[If the organisation has a definition of harassment it should be entered here. If there is no definition then the organisation should consider one. The Human Resources department should define the term.]

What you must not do

Use the internet to harass other members of staff by displaying particular web sites that they consider offensive or threatening.

What are the consequences of not following this policy?

The Organisation deals with harassment by providing advice, support and mediation. Those perpetrating harassment can also be made subject to the Organisation's Disciplinary procedure. *Any proven case of harassment will result in disciplinary action against the guilty party which could ultimately lead to their dismissal.*

7.3. Pornography - What is pornography?

Pornography can take many forms. For example, textual descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography that is legal in the UK may be considered illegal elsewhere. Because of the

global nature of Internet these issues must be taken into consideration. Therefore, the Organisation defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The Organisation will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

What you must not do

- Create, download or transmit (other than for properly authorised and lawful research) pornography.
- Send or forward emails with attachments containing pornography. If you receive an email with an attachment containing pornography you should report it to the (IM&T) Security officer or your supervisor.

What are the consequences of not following this policy?

- Users and/or the Organisation can be prosecuted or held liable for transmitting or downloading pornographic material, in the UK and elsewhere.
- The reputation of the Organisation will be seriously questioned if its systems have been used to access or transmit pornographic material and this becomes publicly known.
- Users found to be in possession of pornographic material, or to have transmitted pornographic material, may be subject to Organisation disciplinary action.

7.4. Copyright - What is copyright? [Use the definition below or insert your own definition]

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright. In the case of computer software, users purchase a licence to use the work. The Organisation purchases licences on behalf of its users.

What you must not do

- Alter any software programs, graphics etc without the express permission of the owner.
- Claim someone else's work is your own

- Send copyrighted material by Internet without the permission of the owner. This is considered copying.

What are the consequences of not following this policy?

- A user and/or the Organisation can face fines and/or up to two years imprisonment for infringing copyright.

8. WHAT TO DO NEXT

- Sign and date one copy of the policy and return to the IT [enter appropriate department or officer]
- Keep a copy of the policy for your reference purposes

Name of User (Please print):	Department:
Signed:	Date:

Appendix H.

Mobile phones and infection control

There is one issue regarding mobile devices that is worth highlighting, although it falls within the scope more of integrated governance (Deighan & Bullivant, 2006) than of information governance: that of possible infection control risks. Hospital-acquired infections (HAI) present an ongoing problem for acute hospitals in England despite concerted infection control efforts (Health Protection Agency, 2012). The most high-risk clinical areas for HAI are generally thought to be intensive care units, operating theatres, surgical wards, and neonatal intensive care units (NICUs). The patient groups considered to be the most likely to develop HAI are neonates and elderly people (NHS Choices, 2012). Within the last 15 years a considerable number of studies have been published documenting contamination of the mobile devices used by health care workers with a variety of bacteria, including organisms associated with HAI (also referred to as nosocomial pathogens) such as methicillin-resistant *Staphylococcus aureus* (MRSA), *Acinetobacter* species, and *Pseudomonas* species. These devices are therefore thought to present a possible or probable infection control risk. The studies cover a variety of countries and types of setting. Most are concerned with mobile phones; however a number of recent studies (Hirsch, Raux, Lancaster, Mann, & Leonard, 2014; Kiedrowski, Perisetti, Loock, Khaita, & Guerrero, 2013; Manning, Davis, Sparnon, & Ballard, 2013) focus specifically on iPads.

The earlier work is reviewed by Brady, Verran, Damani, and Gibb (2009). Most of the studies they included were concerned with mobile phones, but some included other devices, such as pagers and personal digital assistants (PDAs). In all the included studies, between 6.8% and 40% of the devices examined were contaminated with some form of pathogen. Despite a wide variability in the level and type of bacteria discovered, the majority of studies reported an overall contamination rate with HAI-associated bacteria of around 9% to 25%. Three of the studies investigated the possible transmission of bacteria from mobile devices to clinician's hands, demonstrating co-contamination (i.e. the same strain of the bacterium was present on both) of up to 10% of samples.

Ten other studies demonstrating infection of mobile devices by HAI-associated pathogens are cited by Manning *et al.* (2013). These include the work of Ulger *et al.* (2009) based in New York and Israel, which demonstrated a rate for contamination of mobile phones with nosocomial pathogens of 94.5%. Among the health care workers sampled in this study, only 10.5% (n = 200) routinely decontaminated their phones. The most recent UK-based research in this area is that of Brady *et al.*, (2012), who aimed to evaluate the impact of a simple cleaning intervention on the level of surface

bacterial contamination of hospital-issued mobile phones. Over a period of three months, a sample of on-call mobile phones provided to health care workers (n = 87) were tested for bacterial growth before and 12 hours after cleaning with 70% isopropyl alcohol. Testing focused on Gram-positive cocci, in particular *Staphylococcus aureus*. Health care workers were also surveyed regarding their demographics and their opinions and practices relating to infection control. It was found that the number of phones growing bacteria was reduced from 55% to 16% by the cleaning. While 78% of doctors (n = 87) were aware that mobile phones could carry pathogenic bacteria, only 8% cleaned their phones regularly. There were no differences by gender, seniority or clinical speciality in the levels or types of contamination observed. The authors conclude that simple cleaning interventions could substantially reduce the potential of cross-contamination via mobile phones, and that health care workers, as well as keeping the number of their mobile devices to a minimum, should be taught the importance of regular cleaning of mobile devices as well as good hand hygiene. The authors conclude from this and from earlier studies that no conclusive link has been demonstrated from mobile phone surface bacteria to clinical infection.

Among the iPad studies, Hirsch *et al.* (2014) conducted a small-scale study which investigated bacterial contamination of 30 iPads belonging to two groups of university pharmacy teachers, those practising within a hospital setting (n = 14) and those outside (n = 16). Although more of the hospital-based participants used their iPads at their practice sites and within patient care areas, there were no substantial differences between the two groups in presence, absence or quantity of the pathogens isolated, which included MRSA (64.3% and 37.5%), vancomycin-resistant enterococci (VRE) (7.1% and 0%) and *P. aeruginosa* (7.1% and 6.3%). *C. diff.* was not screened for. Two of the iPad studies have a particular focus on techniques of decontamination, which are at variance with the recommended cleaning guidelines. Kiedrowski *et al.* (2013) tested 20 hospital iPads for contamination with MRSA and *Clostridium difficile* (*C. diff.*) Three of them (15%) grew MRSA, while none grew *C. diff.* These authors tested a variety of decontamination methods, and found that damp cloths, alcohol swabs and bleach wipes were able to remove 100% of MRSA from iPad screens. Howell *et al.* (2014) compared the effects of six different disinfectant wipes on removal of MRSA, *C. diff.* and VRE from iPads, finding in favour of a proprietary chlorhexidine and alcohol wipe. Neither study assessed sterilisation of Gram-negative pathogens. None of the methods of cleaning advocated accord with the manufacturer's recommendations, and the long-term effect on the functionality of the devices was not assessed.

Appendix J.

Browser versions: NICE survey and correspondence

J.1 Internet Browser Survey of Link Resolver/Knowledge Base Administrators

1. Introduction

The OCLC Knowledge Base and Link Resolver provide core functionality for the HDAS and A-Z list services. It enables the management of purchased and free content at national, regional and local levels and ensures users access the content available to them. OCLC is continuously updating their product in order to meet the needs of customers and to ensure their products remain competitive in the global market. As part of this continuous development OCLC will be upgrading the Knowledge Base administration area in February 2014.

OCLC has informed NICE that the new administration site will only work with browsers Internet Explorer 9, Google Chrome, or Firefox. OCLC cannot guarantee that it will work on older browsers including Internet Explorer 6, 7 or 8.

There is an assumption that Internet Explorer 6, 7 or 8 are the most commonly used browsers across the NHS. Therefore NICE may need to assist administrators to upgrade their web browser so they can continue to use the Knowledge Base.

The need to upgrade the browser is only for the administrator; it does not impact on services users and there is no requirement for organisation wide upgrades.

2. Questionnaire

The questionnaire was sent to all 300 Knowledge Base administrators and 135 administrators responded, which is a 44% response rate. The aim of the questionnaire was to gain evidence of browser usage, and from this to understand the size of the issue, and to better understand how NICE might help local administrators.

3. Summary of Survey

- 74% of administrators use a browser that is not compatible with the upgraded Knowledge Base administration area.

- 17% confirm they will be able to upgrade. 37% will not be able to upgrade and 45% do not know.
- 52% reported organisational systems are the reason for the use of a particular browser.
- 63% of respondents thought a letter to their organisation from NICE or Health Education England would be helpful.

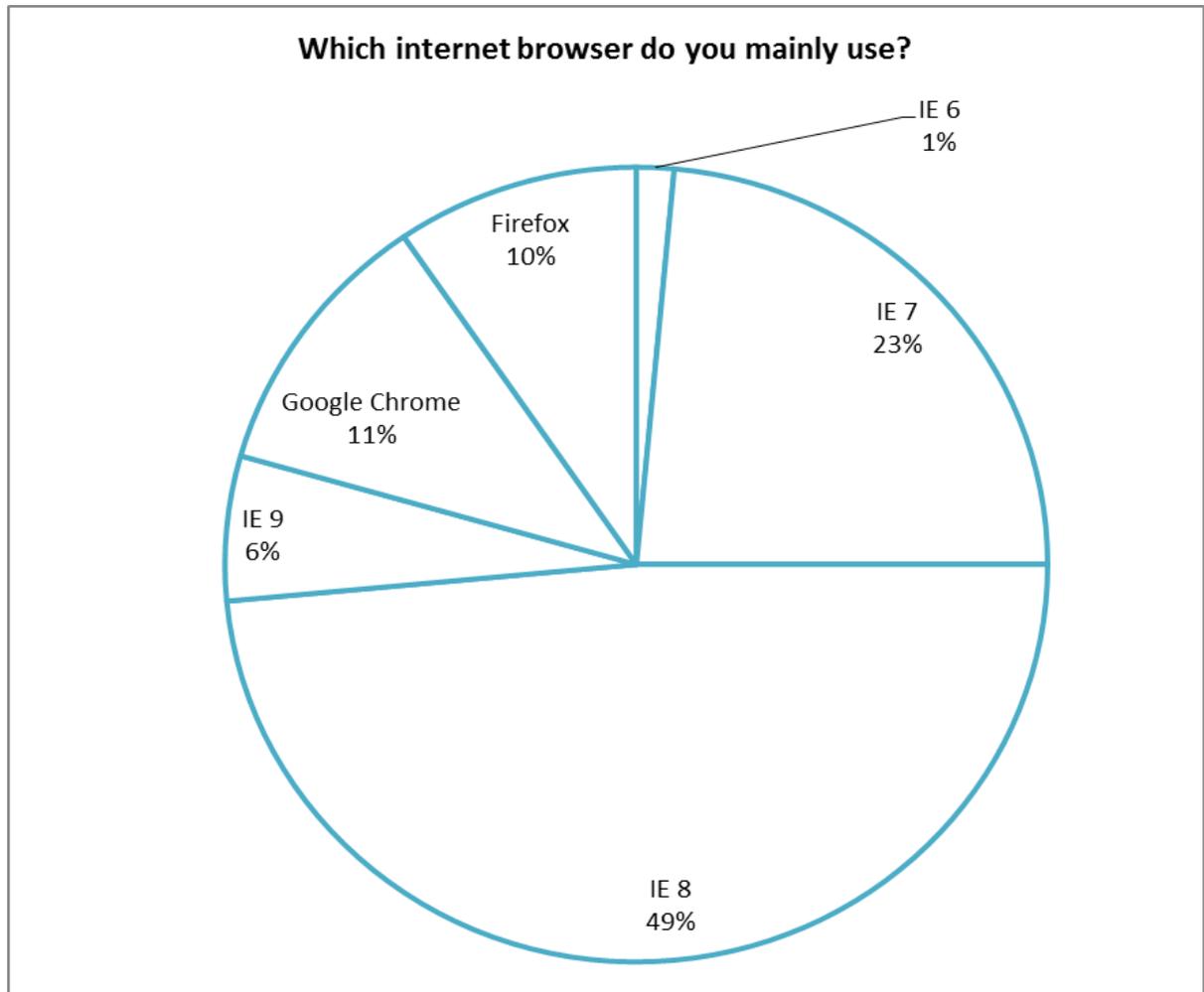
4. Options

The changes will take place in February 2014 and so there is time to prepare and make sure administrators can access the new Knowledge Base. The options for helping administrators upgrade include:

1. Write to all Trusts (a letter from Alexia and/or Health Education England). 63% of respondents thought this would be helpful.
2. Prepare a generic business case that administrators can use to upgrade their browser. 42% of respondents thought this would be helpful.

5. Questionnaire

5.1. Which internet browser do you mainly use?



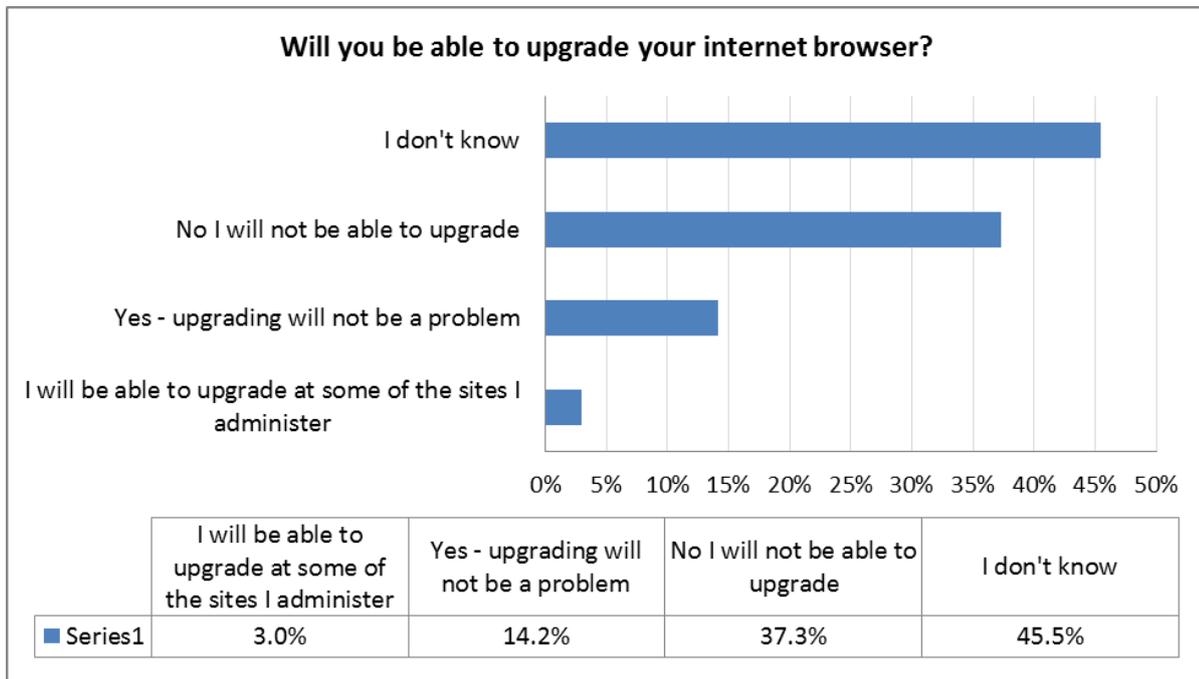
74% of administrators that responded to the survey use a browser that is not compatible with the upgraded Knowledge Base administration area. In order for administrators to continue using the system they will need to upgrade to IE9, Google Chrome, or Firefox.

The data reports that 26% are using a browser that is compatible and therefore the upgraded Knowledge Base will have no impact on their ability to access and use the administration area.

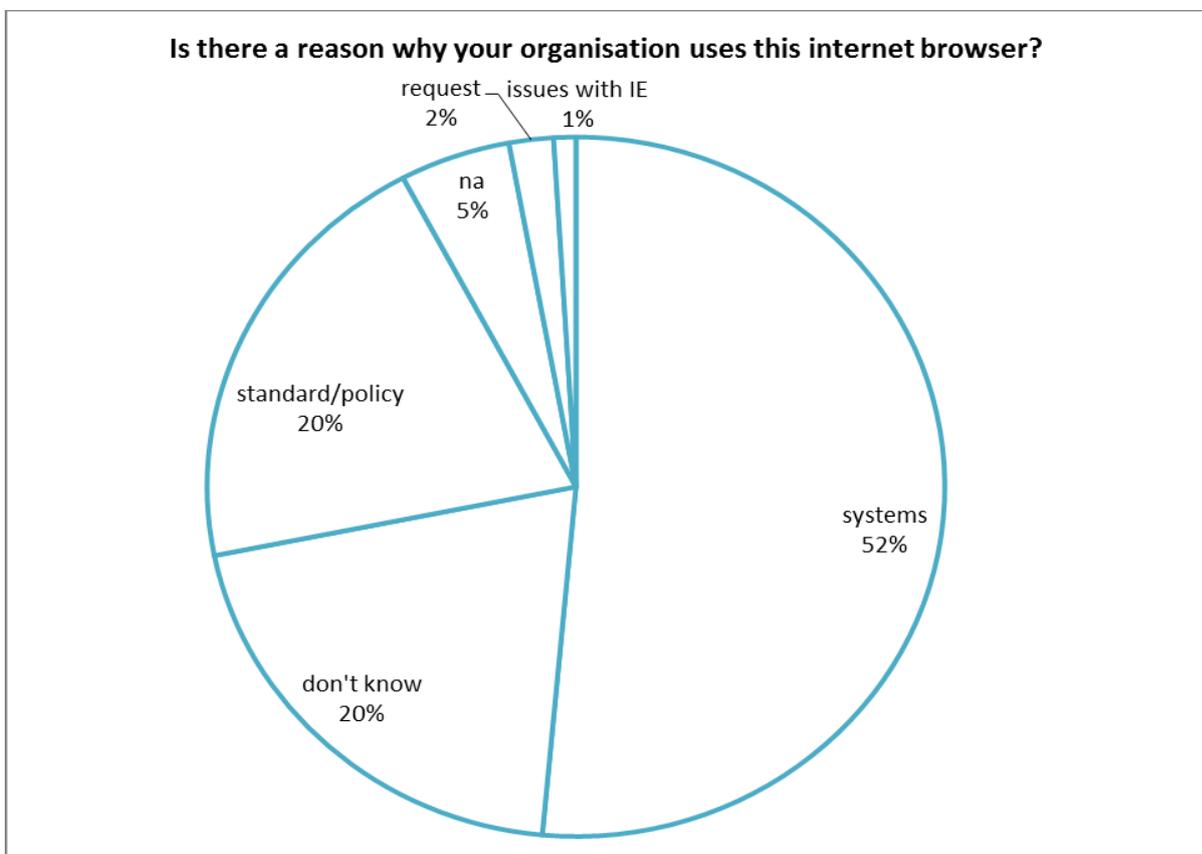
5.2. Will you be able to upgrade your internet browser?

17% of those administrators who responded confirm that they will be able to upgrade. 37% will not be able to upgrade and 45% do not know.

Based on the data that 74% are using incompatible browsers but 17% can upgrade; this means 57% of administrators will need some support in upgrading their browser.



5.3. Is there a reason why your organisation uses this internet browser?



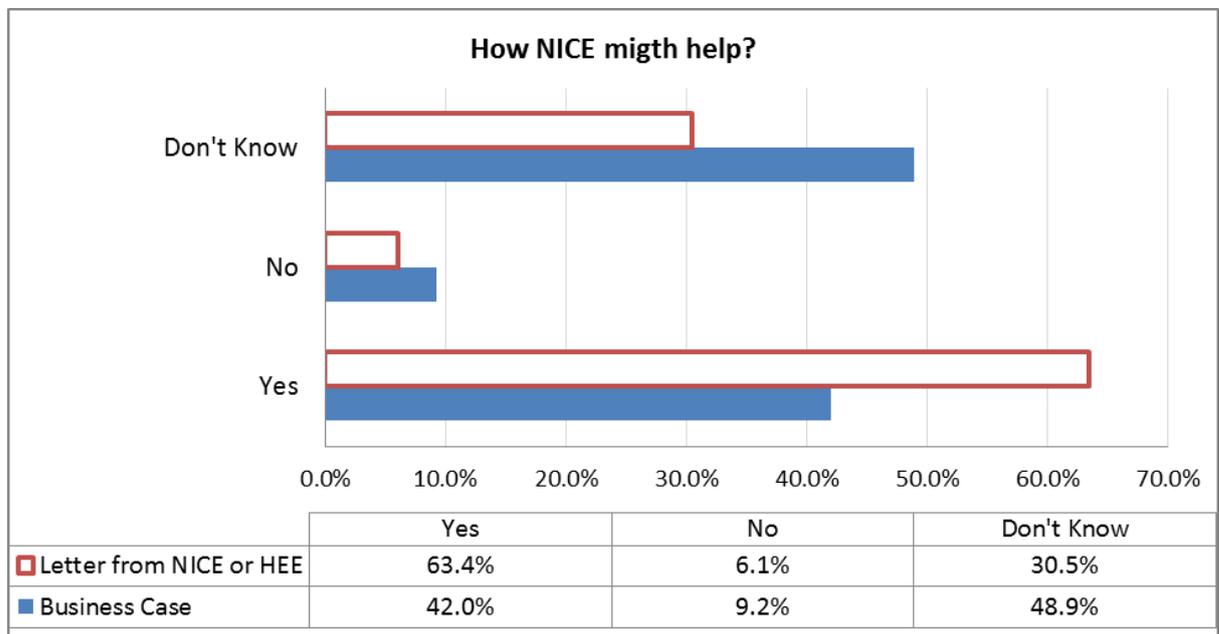
52% responded that organisational systems are the reason for the use of a particular browser. Of this 52% - 92% reported clinical systems, 4% reported the ESR, and 4% reported education and training.

Several respondents reported that it is possible to have Google Chrome as a browser, but this would not be supported (maintained) by their local IM&T department.

5.4. How NICE might help in local administrators upgrading their browser

Several options were presented to administrators in the questionnaire. The first was for NICE to write a generic business case that administrators could localise and use to create their case with local IM&T managers. The second was for a letter to be sent either from NICE or Health Education England requesting that Knowledge Base administrators are able to upgrade to a suitable browser.

A high percentage of respondents thought these options would be helpful. However, a high number did not know if these options would be helpful.



5.5. Administrator Ideas

The questionnaire asked the administrator what ideas they had in making a case to upgrade their internet browser?

1.	Patient care reasons
2.	Clinical system requirements will always take priority. The above would have to come from a recognised body and explain why it is necessary for us to have a browser upgrade in order to continue running library services and why library services themselves are essential.
3.	It might be worth providing the above documentation, but I don't think it will necessarily influence our IT department. Not sure what I'm going to do in that case - it looks like I won't be able to administer the link resolver next year.
4.	At the moment our Trust allows us to have access to Firefox but if for any reason that was removed it might be helpful for NICE to get involved. The Trust is normally very helpful at helping us to resolve any access issues we have.
5.	I think it should be possible, but anything to help explain why this is necessary would be good.
6.	Updating the browser will enable users to access health information from NICE Evidence, Up-To-Date, Clinical Key and other web-based popular clinical information services so much quicker and easier. It will also enable library staff to train users and demonstrate resources to them successfully.
7.	I have been able to put forward the case for the library PCs to have an IE upgrade based on resource need and no requirement to access clinical systems. It is possible that any upgrade, discretionary or not, would have to have the authority from the relevant NHS body for IT systems.
8.	Cost implications for the Trust of not being able to access full text material and having to resort to interlibrary loans...
9.	I can usually make a case for myself, but it would be nice to feel there was some external "weight" behind it and it wasn't just me being a difficult demanding librarian
10.	Establish that this is the evidence base
11.	I think we should be able to use an internet browser other than IE as we get lousy results no matter what version of IE we use. Firefox is fine. NICE should identify the best browser for its applications and recommend to all Trusts that this browser be made available to all employees.
12.	When I needed Chrome for another application IT were very understanding

13.	I will continue to use Google Chrome, unless IT decides to ban it.
14.	Benchmarking against other Trusts might also help.
15.	Approach Department of Health re NHS protocols on IT
16.	Normally the response to any requests to upgrade browsers is met with a no because of information governance. It would be useful to have some clarity around this issue i.e. have some evidence on the different browsers and to what extent or not they pose a risk to security and information governance.
17.	We have good relations with our IT department and so long as we state an appropriate case for upgrade we usually get what we ask for. Although IE9 would be a step too far I suspect.
18.	It is possible that the Trust will be upgraded to IE9 by February 2014.
19.	Argument in favour of installing Firefox. Our Trust will do so on request but are mildly reluctant because they think it isn't so 'secure' as IE.
20.	The decision about which browser I am able to use is out of my control.
21.	I can probably make a case to the IT department if the browser on my computer needs upgrading in order for me to undertake admin tasks or to access particular online information resources.
22.	We have pleaded our case for an upgrade on several occasions but these pleas have fallen on deaf ears.
23.	Our IT dept. have been quite kind to us and allowed us access to Firefox but it is the lack of support for this package that may need to be addressed as opposed to the actual upgrade.
24.	That it wouldn't cost the Trust any money.
25.	How important it is that we can access the systems i.e. the reason we need access to the knowledge base (especially if there is some relation to how the resources supports patient care).
26.	Stress the differences/benefits of changing/showing shortfalls in cases of not making the change, as this will then make them consider the request.
27.	Assurance that upgrade will not interfere with local systems.
28.	I don't think there would need to be a case produced for library upgrades, but the above would both help, should there be one.

29.	Outdated browsers are not secure (no MS patching for older browsers). Increasing amount of resources is not compatible with older browsers.
30.	A letter sent not just to the library but to the Chief Executive, and the head of IT services.
31.	NICE letter will help but aimed at director level.
32.	Explain how inability to upgrade impairs ability to provide and maintain evidence-based healthcare information for patient care.
33.	Just stating the facts of why it is necessary.
34.	Give local units more control over what is loaded on their own PCs.
35.	A letter from NICE might go some way, but I'm not sure how many local issues influence above this.
36.	A demonstration of the implications of failure to upgrade.
37.	Above worth trying but OCLC need to be made aware of NHS constraints if they're dealing with NHS systems.
38.	The above would both be useful if I had a problem but IT have said they are happy to upgrade me.
39.	If they are not upgraded, the information for staff would not be current due to inability to update NHS Evidence Search. Our Trust no longer has any paper journals.
40.	Evidence of the impact not having the latest version has on flexibility and capability to deliver clinical care, research or education and training. A consensus and guidelines across sector including industry and public sector on policy.
41.	Looking at business models for how IT industry adds value across sectors with longer term contracts and incentives for maximising implementation of products to ROI, rather than focus on new/cutting edge continually to maintain profitability. Better contracts for provision to sectors delivering basic citizenship resources like health care.

J.2 Letter from NICE to NHS IT managers

NICE National Institute for
Health and Care Excellence

Level 1A
City Tower
Manchester
M1 4BT
United Kingdom

+44 (0)845 003 7780

INSERT ADDRESS LINE 1

INSERT DATE

Dear

REQUEST TO UPGRADE LIBRARY ADMINISTRATOR BROWSERS TO IE9 OR ABOVE OR TO
GOOGLE CHROME, OR FIREFOX

Your Trust Library Service plays an important role in supporting your clinical staff and managers to access and use the very best evidence and information to inform their decision making and continuous professional development.

These resources include leading journals such as the BMJ and the Lancet and many thousands of other journal titles and bibliographic references.

Suppliers of these resources are constantly upgrading their services and it is for this reason it is essential that your library administrator has a modern internet browser installed, such as Internet Explorer 9 or Google Chrome or Firefox. This will enable your library service to continue to manage these resources efficiently and effectively, so that they can continue to make these available to those that need them.

This is a relatively simple request, but without a modern browser, access to evidence and information via your library service is likely to be limited and in some cases will not function at all. From our own research we know that this issue affects up to 70% of NHS library administrators.

This upgrade need only be made on the equipment used by your library administrator, responsible for managing access to these resources on your behalf. We need the upgrade to take place by May 2014. It is not necessary to install upgraded browsers for any other staff and there is no impact on users

Library back-office services are often unseen by library users. However, they are essential to ensuring appropriate resources are accessed and used to their maximum. We are grateful for your efforts in ensuring that this service is appropriately supported.

Yours faithfully,



Alexia Tonnel

Director for Evidence Resources
NICE



Chris Welsh

Director of Education &
Quality
Health Education England

A handwritten signature in black ink that reads "Alison Hill".

Alison Hill

Deputy to the Chief
Knowledge Officer
[Public Health England](#)

*Appendix K.
The ISMS plan-do-check-act cycle*

A requirement is set out in the document *Information security management: NHS code of practice* (NHS Connecting for Health, 2007) for the establishment within each NHS organisation of an information security risk management system (ISMS), the details of which are set out in the BS ISO/IEC 27001 standard as shown below in Figure J.1. It should be noted that the Plan element of the cycle requires the organisation to establish a security policy establishing information security control objectives and controls (safeguards or countermeasures to avoid, counteract or minimize security

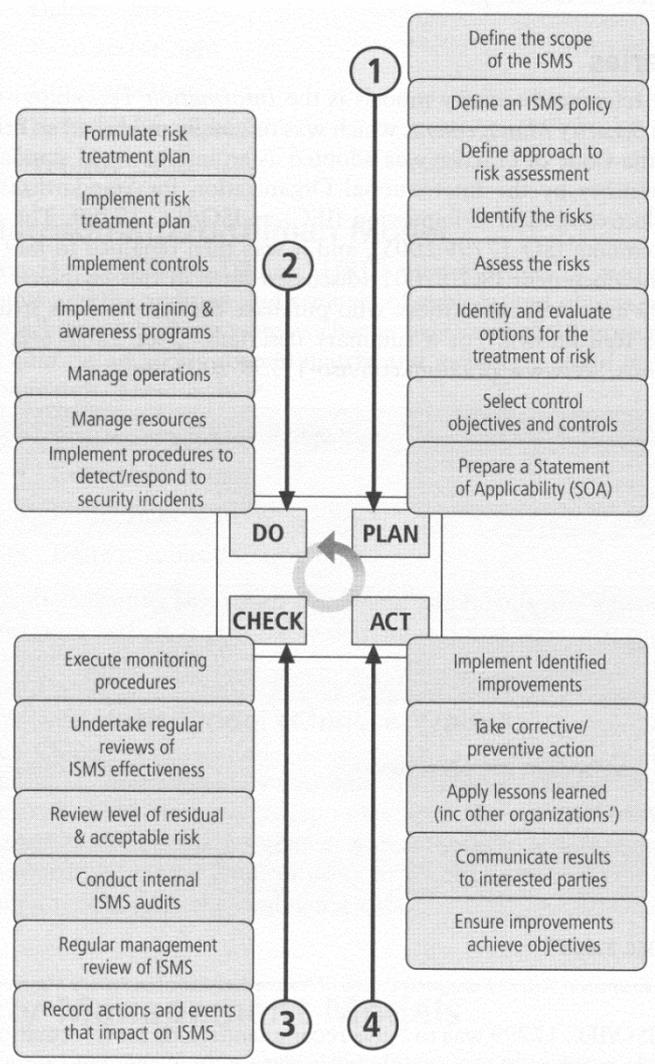


Figure K.1 BS ISO/IEC 27001 major process step: PDCA cycle
Whitman & Mattord (2010), p. 226.

© 2011 Delmar Learning, a part of Cengage Learning, Inc.

Reproduced by permission. www.cengage.com/permissions

risks), together with and a statement of applicability justifying why these particular controls were selected and others not (Siponen & Willison, 2009).

A process of this scope and complexity inevitably incorporates many PDCA sub-cycles within it, operating asynchronously and at different speeds (Whitman & Mattord, 2010, citing Gamma Secure Systems, s.d.) The core aspects of risk management with which we are concerned are more evident in another PDCA cycle, as described by Jones (2007) (Figure K.2):

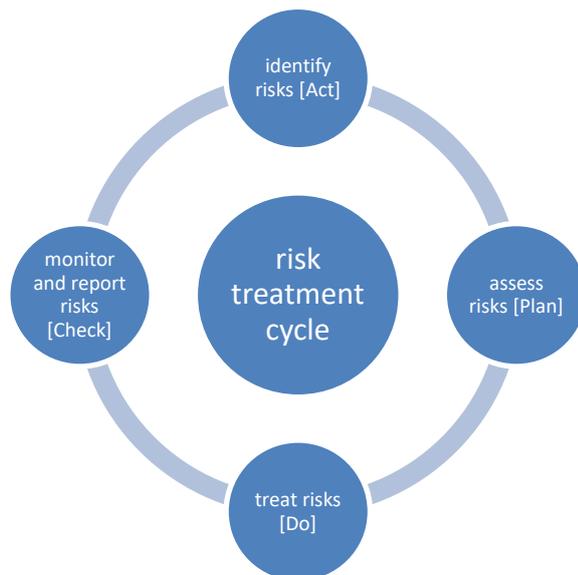


Figure K.2 Risk treatment cycle

Jones (2007), p. 31

Reproduced by permission

Identify risks [Act]: by way of background, this includes identification of policies, standards, and legislative requirements, as well as a detailed mapping of the IT infrastructure and the business processes which it supports, and of information flows through the organisation, including storage, capture and processing. The process of risk identification proper (which can also be described as risk analysis) requires several stages: identification of potential threats to the system; identification of exploitable vulnerabilities; identification of existing controls and counter-measures that will mitigate the likelihood of a vulnerability being exploited; calculation of the *likelihood* that a particular threat could successfully exploit a particular vulnerability; calculation of the level of *impact* that this would entail; identification and documentation of the so-called residual risk. Residual risk is defined as a combination of 1) a threat less the effect of counter-measures; 2) a vulnerability less the effect of safeguards; and 3) an asset less the effect of asset-value-reducing; it is the amount of risk unaccounted for the application of controls safeguards (Whitman & Mattord, 2010, citing Gamma

Security Systems, s.d.). This process is undertaken for each threat and associated vulnerability. Residual risks need to be classified as being either acceptable or unacceptable (Gerber & von Solms, 2005).

Assess risks [Plan]: this process is achieved by the “establishment of a *qualitative* or quantitative interrelationship between identified risks” (Jones, 2007, p. 32; my italics). This involves the process of determining the significance of the identified threat-vulnerability pairings, and estimating the risks to those systems that may be affected by them. Sources to inform this process include: self-assessments as a result of internal or external audits; advisory notices issued by the NHS Information Centre, information security standards bodies, and system vendors; and the findings of information security vulnerability assessments. A scoring system may be applied (Calder, 2013). Once risks are identified and assessed, *risk reduction planning* is undertaken to reduce the risk exposure of the organisation to an acceptable level; includes the evaluation of options and identification of desired solutions. The assessment process also includes *risk modelling* (exploration of the “what-if” questions relating to potential information security incidents) and business *continuity planning* (the development of response protocols as a response to identified crisis scenarios) as important components.

Treat risks [Do]: once risks have been analysed, risk mitigation actions should be prioritised, based on the probability of occurrence and the legal, regulatory, financial or reputation impact to the organisation. Such impacts are not easy to quantify. Once they have been identified, it is normal to address (treat) risks in one of four ways: *risk avoidance* (not performing an activity that could carry a potential risk); *risk reduction or mitigation* (measures taken to reduce the severity of impact of an incident); *risk acceptance* (accepting the impact of an incident where it occurs) and *risk transfer* (transferring the risk to another party via contract or via insurance). Contracting out the development and hosting of an e-learning application would include an element of risk transfer. Blocking social media sites would be one example of risk avoidance. Use of host and network defences against malware-based threats would be an example of risk reduction; here a balance has to be struck between the cost of the measures and the benefits they provide, and between the level of restriction of functionality of the system and impaired performance compared with the proportion of attacks that are deterred, detected or prevented. It should be noted that all risks that are not avoided, mitigated or transferred are accepted by default.

Appendix L.

Precision (specificity) and recall (sensitivity) of web filtering

For any content classifier, the errors in filtering a sample set of URLs may be represented in the form of a “confusion matrix” as follows (Figure L.1):

	Real – positive	Real - negative
Filter - positive	TP	FP
Filter - negative	FN	TN

TP = true positive / FP = false positive / TN = true negative / FN = false negative

Figure L.1 Confusion matrix
after Gomez Hidalgo (2009), p. 294

Simple formulae can be derived from this representation to define P, R, accuracy (proportion of items correctly classified) and error (proportion of items incorrectly classified):

$$R = \frac{TP}{TP+FN} \quad P = \frac{TP}{TP+FP} \quad A = \frac{TP+TN}{N} \quad E = \frac{FP+FN}{N}$$

Over-blocking and under-blocking are represented here by 1-P and 1-R respectively.

The trade-off between precision and recall (specificity and sensitivity) can be represented graphically using a Receiver Operating Characteristic (ROC) curve, as in the following example (Figure L.2):

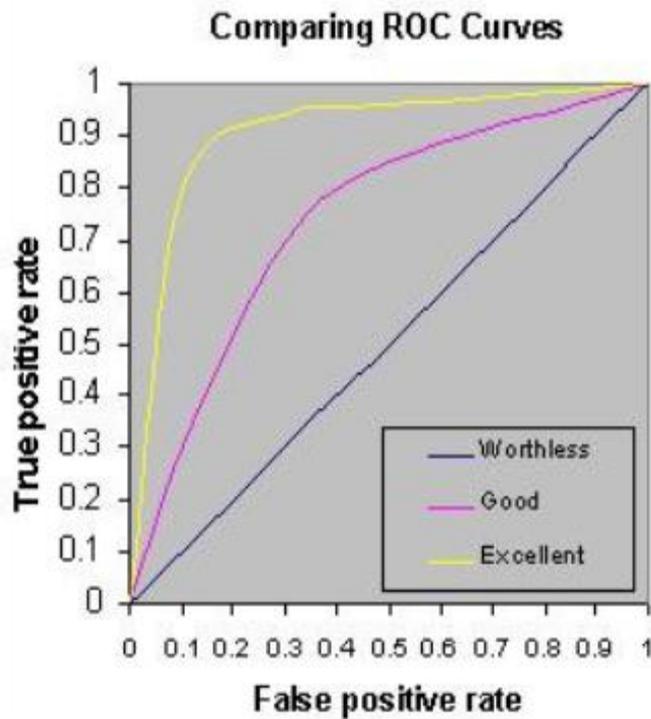


Figure L.2 ROC curve for content classifier

Zhang and Janssen (s.d.)

Reproduced by permission

It can be seen here that the 'excellent' classifier generates the largest area under the curve; the false positive rate increases only slightly as the proportion of true positives increases.

Appendix M. Usability problems with mobile apps for accessing e-content

The librarian E10, in her correspondence with the researcher, made some trenchant observations about usability problems with publishers and aggregators' mobile apps for accessing e-content, which merit quoting in full.

"My biggest complaint last year was the withdrawal of the [trade name] mobile app. Pub4 launched their [app name] in a blaze of publicity, claiming that this had been tested and approved by loads of people who know about this kind of stuff. Yes, when you eventually get to a full text article it does look very nice and works on a mobile device, but you can't use the rest of their ... website on a mobile device. They clearly tested the mobile article view in isolation with absolutely no thought for the customer's journey to the resource.

Most providers can't see further than their own resource and don't understand that the majority of users do not go to the publisher website (they don't know who publishes the title they want), but access full text by following links in other databases, Google, library catalogues, lists of references etc., and in any case the institutional access point is often different from that provided for individual subscribers.

The bottom line is that all roads should lead to Rome but they don't. The resource providers do not pay enough attention to the customer's journey to the end product. You can only reach your destination by trekking miles and miles through jungle, swamps, ravines etc. but you have inappropriate clothing/equipment and no navigation aids." (Librarian, E10)

The point she was making here seems essentially to have been that the design of publishers' mobile apps reflected a very a publisher- or aggregator-centric approach to accessing e-resources which did not fit end-users' approaches to information seeking and use.

Appendix N.

Summary of responses: access to YouTube / streamed services query

LIS-MEDICAL [https://www.jiscmail.ac.uk\(18/07/16\)](https://www.jiscmail.ac.uk(18/07/16))

Dear Colleagues

I submitted a request to the list on 8 June, asking for details from trusts who provide access to YouTube or similar digital services. The purpose was to establish the prevalence of social media policies which cover this form of Internet use and determine how such access is regulated (if at all).

Thank you very much to those who responded and those who provided examples (e.g. policy docs). I received 6 replies and also made a quick search via Google - 6 further policies were added (there were a few more out there!).

In summary (12 trust policies were examined):

- (1) Access to YouTube or other social media for staff without restriction (i.e. all staff for business and personal use): 2/12
- (2) Access with limitations (business use only for named individuals or teams): 10/12
- (3) Policy available to view and included reference to YouTube or similar digital services: 7/12

- Most trusts acknowledged that social media (including digitally streamed services like YouTube) can be beneficial for staff in the course of their work and advantageous to the organisation with regard to strategic aims and operational objectives;
- Social media policies are becoming more common and incorporate data security and information governance principles;
- 40% of trusts sampled did not specify YouTube (or streaming services) in their policies and so localised discussion/negotiation by library or L&D has shaped their response to access requests;
- There is a lack of consistency between policies and in attitude to 'risk' (data loss/inappropriate use/confidentiality) which is reflected in diverse approaches to risk assessment and access controls across the sampled NHS organisations.

Martin Elcock Librarian: Outreach / Deputy Library Manager

Tel: +44 (0) 121 371 2487 Email: Martin.Elcock@uhb.nhs.uk

Appendix P.

Information security and cybersecurity measures compared

	<i>Information security / governance</i>	<i>Cybersecurity</i>
<i>Behavioural measures</i>	Internet / email / social media acceptable use policy Use of encrypted portable media Screen locking Mandatory use of secure email systems (e.g. NHSmail) and / or encryption facilities and / or password protection to send files Policy controls on PII / sensitive information – how stored / sent / transported Prohibition of password disclosure or sharing	Internet / email / social media acceptable use policy Strong password policies
	User training re: social engineering, data protection, confidentiality, privacy, password practices	User training re: social engineering, safe browsing, avoidance of links and attachments in unsolicited email, password practices
<i>Non-behavioural / technical measures</i>	Enforced use of prescribed encrypted portable media via USB port blocking Disabling of optical drives Computer screen timeouts SWG controls on access to web content – inappropriate material DLP systems Encryption of critical files Controls on privileged accounts	Endpoint anti-malware Firewalls Restrictions on browser functionality and extensions Restrictions on types of downloadable files Intrusion detection systems Intrusion prevention systems Server OS ‘hardening’ Separation of applications within networks Penetration testing of networks SWG malware screening Software and OS updates/ patches
	Enforced password changes at set intervals Disabling macros in email attachments Restrictions on allowed email attachment file types Technical authentication requirements for OSs and applications	

Table P.1 Information security and cybersecurity measures: comparison matrix

Appendix R.

Data analysis matrices

Table R.1 Results matrix outline as at 28/01/15

	Background	Trust IT infrastructures and their management	Published information resources	E-learning	Social media	Mobile devices
Professional information behaviour	<p>1.1 T1-DGH partnership arrangements with university to manage library -- offers walk-in access to a wider range of resources for NHS staff on site</p> <p>T3-MH largely a virtual library T4-TH very well stocked. LIS manager is national expert on e-content and collections</p> <p>No trust implementing Map of Medicine</p>	<p>1.2 Requirement to use encrypted USB memory sticks Availability of networks Network performance Need to run trust and university networks in parallel</p> <p><i>NB applies also to e-learning</i></p> <p>Lack of single sign-on at T1</p> <p>Problems accessing T2 systems from within T1 premises/network including e-learning</p>	<p>1.3 Most clinicians making use of LIS e-resources via OpenAthens – di d not always realise that LIS administered this. Dietician spoke of online service from BDA – no need to use LIS.</p>	<p>1.4 <i>Use of e-learning resources in information seeking not discussed by respondents</i></p> <p><i>T3-MH library services promoted in computer suites and via training events</i></p>	<p>1.5 <i>LIS at T4 had developed social media platforms to support information seeking – Pinterest with infographics, current awareness portal</i></p> <p><i>Very little use of social media within workplaces other than YouTube videos</i></p> <p><i>Lack of use related to negative attitudes / fear of social media</i></p>	<p>1.6 <i>Support by LIS</i></p> <p><i>BYOD at T4-TH – permits staff to access social media resources via own mobile devices</i></p> <p><i>Helga’s stuff about problems with publishers’ and aggregators’ mobile apps</i></p> <p><i>Little use observed of mobile devices for information seeking</i></p>

Education and training arrangements	<p>2.1 Mand & stat – CNST Prof ed – contracts with universities – which students present in the three trusts and requiring e-resource access</p> <p>Drivers for growth of e-learning History of e-learning in each trust</p>	<p>2.2 Network access policies re students on placement [describe situation across trusts] <i>Add stuff about student levels of access to clinical systems</i></p> <p>Availability of computer facilities to students</p> <p>Wireless networks: Eduroam, other</p> <p>Problems with e-learning related to IT infrastructure</p> <p>Virtualisation? Implications for age of PC hardware</p>	<p>2.3 <i>Contacts between education, training, LIS</i></p>	<p>2.4 Drivers for growth History in each trust 3.2.1 Scope and utilisation of e-learning to deliver education and training: mandatory and statutory training professional education – pre-reg. and post-reg. 3.2.2 Attitudes to e-learning 3.2.3 Problems with e-learning: access to facilities, computer literacy – addressed via computer literacy training initiatives, supported sessions, computer suites, tablets for loan, home access</p>	<p>2.5 <i>Use of social media applications and resources for education and training purposes not discussed by respondents-</i></p> <p><i>Mandatory and statutory e-learning provided by trusts did not make use of social media / web 2.0 platforms</i></p> <p><i>Educationalists not aware of social media use by students for educational purposes e.g. Facebook study groups</i></p> <p><i>Professionals expressing need for training on social media (T2)</i></p>	<p>2.6 <i>T1-use of tablets for e-learning</i></p> <p>T3 training loan of tablets for e-learning</p> <p><i>U3-Med iPad project</i></p> <p><i>Variable use of mobile devices otherwise: medicine and pharmacy yes, nursing and AHP no</i></p>
-------------------------------------	---	---	---	---	---	--

Professional cultures and organisational dynamics	<p>3.1 (Possibly include here CQC reports, NHS staff survey results)</p> <p>Statements of values etc. 6 C's in nursing</p>	<p>3.2 (IT strategic planning material goes here: EPR system implementation etc.)</p> <p><i>Role of ? in setting up PG Centre Wi-Fi at T1-DGH T1-DGH and T4-TH not yet implemented EHR – high strategic priority in both</i></p> <p><i>Complaints from T4-TH IG about disadvantageous position, poor communication channels, lack of contact with IT, unresponsiveness of IT helpdesk.</i></p> <p><i>Impression given that IT support at T4 was of inconsistent quality. Clinical staff perceived IT as being understaffed and under-resourced in relation to demands</i></p> <p><i>T4 education facilities manager – education was a lesser priority than clinical services for IT support</i></p> <p><i>IT and IG worked closely together in T1 and T3 via representation on committees</i></p>	<p>3.3 <i>Communication key issue – T1 head of IT will not respond to communications from LIS manager – reportedly unresponsive to others also T1 IT manager seemingly unaware that LIS had trust as well as university computers</i></p> <p><i>T3 LIS proactive in publicising services at training events</i></p> <p><i>IT dept. works closely in T4 with LIS re availability of e-journals – firewall manager</i></p> <p><i>All LIS well regarded by clinicians - all spoke highly of LIS help with searches and document supply</i></p> <p><i>T3 IT manager trusted LIS manager re requests to unblock websites – no need to refer to line manager</i></p> <p><i>NICE attempting to work with HSCIC on IT infrastructure issues relating to e-resources</i></p> <p><i>LIS providing CAS at T1-DGH relating to pressure sores and falls – or 1.3. T3 LIS also providing CAS for WPH</i></p> <p><i>Emphasis on learning from adverse events (T1-Nur-07)</i></p>	<p>3.4 <i>Issues between training department and SMEs at T1 re: territory</i></p> <p><i>Cultural issues re e-learning – T1 HR felt that ESR and e-learning was a major change</i></p> <p><i>Attitudes to e-learning</i></p>	<p>3.5 <i>Social media perceived as high-risk by nurses and AHPs in particular – averse to using in workplace-confidentiality and privacy concerns. Some respondents expressed negativity about social media. (discussed in 1.5 – refer to this)</i></p> <p><i>All students, also junior doctors, receiving training on e-professionalism via university or PG Centre? Maybe move to 4.5?</i></p> <p><i>Interest in using social media to engage with patients (T3-MH-Pharm-18, T2)</i></p> <p><i>Services in T3-MH-WPH have started to do this. Also experiments in T1-DGH with maternity services</i></p>	<p>3.6 <i>iPads a badge of status? CEO at T3-MH had pestered IT for three years before getting one!</i></p> <p><i>iPads issued to board members-all trusts – and widely used for accessing and managing documents-issue of cloud storage?</i></p> <p><i>Provision of mobile devices – who gets what? T4-Med-19 cf. AHP-10</i></p> <p><i>Professional norms of not using mobile devices in clinical areas – relating to 2009 policy, local policies, just unwritten</i></p>
---	--	---	---	---	--	--

Information governance / security structures and practices	<p>4.1 Outsourcing Procurement User support (??)</p> <p>Organisational position of information governance</p>	<p>4.2 <i>Evident security deficiencies: obsolete OS + browsers</i></p> <p><i>lack of screen locking + USB port blocking</i></p> <p><i>Few IG managers in any trust. In T3, IG functions were distributed across departments with IG manager having advisory role and responsibility for IG Toolkit.</i></p> <p><i>In T1, part of integrated governance</i></p> <p><i>NB T1-DGH-IT-11 was not aware of arrangements for students to access network</i></p>	<p>4.3 <i>Blocking of websites – experiences in each trust</i></p> <p><i>IMTG whitelist</i></p> <p><i>Heritage Cirqa IG issue at T4-TH</i></p>	<p>4.4 Problems with password management accessing e-resources and e-learning</p>	<p>4.5 Past misuse of social media: past incidents, warnings, sanctions</p> <p>Blocking of social media - Individual social media applications: what is blocked, what is allowed – table</p> <p>Trust policies on staff use of social media, impacts on trust services (e.g. LIS) and end-users, perceptions of policies</p> <p>Junior doctors in T1 given training on e-professionalism (T1-DGH-Med-06)</p>	<p>4.6 <i>‘Cultural’ inhibitors of mobile device use among clinicians</i></p> <p><i>Trust policies</i></p> <p><i>DH policy</i></p> <p><i>Security management of trust and personal devices</i></p> <p><i>infection control issues- At T1-DGH, IT had insisted on ruggedized laptops with easy-wipe screens- an infection control measure</i></p>
--	---	--	--	---	--	--

Communications policies and practices	<p>5.1 <i>Trust policies – mostly restrictive [see table]</i></p> <p><i>Intranet material here – who creates content etc.- allude to earlier stuff</i></p>	5.2	5.3	5.4	<p>5.5 <i>Trusts varied greatly in extent to which use was being made of social media for public engagement and marketing activities / state of development of social media strategies</i></p> <p><i>T4-TH and T3-MH were using Twitter for research dissemination</i></p>	<p>5.6 <i>Mobile device management?</i></p> <p><i>Policies / guidance for students (T3-MH) and staff</i></p>
---------------------------------------	--	-----	-----	-----	--	--

Table R.2 Example of an individual matrix cell

1.2	Trust IT infrastructures and their management
Professional information behaviour	<p><i>NB much applies also to e-learning</i></p> <p>Within trust networks, negative impacts upon access to published information were experienced in respect of:</p> <p>The requirement to use encrypted portable media (e.g. laptops, USB memory sticks) Network access, availability and performance ‘Legacy’ hardware (see above, section 1.3.2) System policies/limited system privileges (e.g. inability to download updates to browser plugins, or files of a particular type)</p> <p>Requirement to use encrypted portable media It has been NHS policy since early 2008 (Department of Health, 2008) that all portable media and devices should be encrypted, though the requirement was not necessarily implemented immediately in all NHS organisations. In practice this tends to mean laptop computers and USB memory sticks. Difficulties in obtaining trust-approved USB memory sticks can act as a barrier to saving, storing and using information retrieved online.</p> <p>Staff at T1-DGH and some staff at T4-TH reported difficulty in obtaining encrypted USB memory sticks. “Not all our staff have encrypted memory sticks, only the quite senior staff or staff in training roles, erm... have those” (T1-DGH-Nur-08). “Trying to get hold of them is, you know, it is very much forms in triplicate” (T1-DGH-Pharm-04). “There are total obstacles, yes” (T4-TH-AHP-10). The IronKey devices used at T4-TH apparently cost about £80 each, which may be prohibitively expensive for some services (T4-TH-IG-09). Encrypted memory sticks were not available to students on placement in T1-DGH, creating problems for them working on case presentations at home (T1-DGH-Pharm-04). In T3-MH difficulty in obtaining USB memory sticks was not reported, but their use away from NHS sites for non-core purposes (e.g. research or study) required specific permission from information governance (T3-MH-IG-03).</p> <p>The requirement to use encrypted USB memory sticks commonly causes inconvenience to visiting presenters on NHS sites, who are obliged either to use their own laptop for the presentation or to email it in advance (P1). The devices themselves were perceived to have inherent limitations, mainly relating to slow loading of content, causing problems when giving presentations (T3-MH-Med-21). T3-MH-Med-21 complained that hers could not be used on her Macintosh at home. The use of USB memory sticks for transferring information was thought to be old-fashioned in an era of widespread cloud storage (T4-TH-AHP-10).</p> <p>[possible indication of need for NHS-wide secure cloud storage]</p> <p>‘Legacy’ software – in particular older versions of MS Office, Internet Explorer – users may be unable to open, e.g., .pptx files if they still have MS Office 2003 and do not have the required viewer, or may encounter a variety of problems with displaying web-based content owing to issues with lack of browser support for front-end web technologies such as Cascading Style Sheets (CSS),</p>

HTML 5, and JavaScript (“Can I use... Support tables for HTML5, CSS3, etc.,” n.d.; McCarthy, 2013).

[NB Particular impact on LIS]

Network access, availability and performance

Access to networks

Authentication and access management

Policies controlling the availability of network logins, including generic logins, can present barriers to accessing and using published information. This can particularly affect library services, restricting the services they are able to offer to NHS staff from other organisations under reciprocal access agreements

Remote access

All the trusts in the study provided remote access to their systems using VPN tokens, though in practice within T1-DGH the facility is generally available only to “consultants and people like that” (T1-DGH-LIS-01). It is readily available in T3-MH; several respondents referred to using it. Remote access was not mentioned by respondents in T4-TH, though its availability was confirmed by reference to the relevant policy document. In T1-DGH problems with it affecting user profiles was reported:

“It would appear at this site if you hot desk between different computers or if you access your computer via your VPN token from home, what then happens it seems to upset your profile and lose data and it takes a long time to log on” (T1-DGH-Nur-08).

Also, while it is possible to access the OLMS system from home to undertake e-learning, completing the module does not register on the system, thus effectively rendering the remote access facility useless (T1-DGH-T&D-??)

Access to systems across organisational network boundaries

A number of general problems accessing systems across organisational boundaries were reported. T2-DGH staff working on T1-DGH sites reported problems accessing some T2-DGH systems from within the T1-DGH network, particularly the OLMS for e-learning (T2-DGH-AHP-01, T2-DGH-AHP-02). T1-DGH does not have single sign-on for all its clinical systems, resulting in wasted time and password proliferation (T1-DGH-IG-12). In T3-MH, where part of the trust (T3-MH-WPH) is on an outsourced network, problems were reported of inability to access the trust intranet, and also T3-MH e-mail addresses in MS Outlook did not auto-complete on PCs linked to the outsourced network. A member of staff in T3-MH’s community health services (T3-MH-Nur-??) indicated that access to T3-MH’s systems from local authority premises and GP surgeries, where many of the staff are situated, often presents a problem, since it can depend entirely on local information security policies.

In several instances, respondents reported being unable to access NHS systems from within university networks or *vice versa*. The library manager at T1-DGH had encountered a problem with access to e-resources at U15, which was subsequently resolved via the IT department. Part-time students at U3 were reported as being readily able to access their university e-resources from within T3-MH's network (T3-MH-LIS-01). T4-TH-AHP-12, who was jointly employed by T4-TH and U9, reported being unable to connect to her U9 network drive via VPN. The researcher established in consultation with T4-TH-IT-20 that such a connection would not violate trust policy, and the problem was subsequently resolved.

The main problems of this sort arose in connection with HE-NHS collaborations. T1-DGH-LIS, which is a jointly-run service between U2, T1-DGH and other trusts, was required to manage staff PCs and computer clusters on separate trust and university networks, and to run services in parallel. The university would not allow T1-DGH-LIS-01 to connect to the NHS Electronic Staff Record system owing to software compatibility concerns. It did permit walk-in access for visitors and members of the public to the library computers: staff could log them on, requiring only the completion of a record form. In practice it appeared that the library staff were able to use the university network to circumvent system restrictions on the NHS network. In T4-TH it was possible for a member of staff to have logins to three separate systems -- the trust's, U3's and the NIHR research hub's -- and hence to have three email addresses, calendars, network drives etc. This was reported to create problems for communication and information sharing, as research staff tended to use their NIHR email address and to fail to check their other mailboxes. Accessing trust systems from a university or research network required the member of staff to use a VPN token, and not everyone was prepared to make the effort to do this regularly (T4-TH-Com-03).

These are also used to provide access to the information governance e-learning module for new starters who do not yet have network accounts, and to provide access to the NHS Jobs website for staff such as porters and cleaners who would not normally have network accounts (T1-DGH-LIS-01).

Several respondents reported problems in managing the various passwords they required for access to NHS and professional systems. A postgraduate clinical tutor (T3-MH-Med-02) complained of password proliferation in relation to e-resources. A nurse educator (T1-DGH-Nur-08) mentioned passwords in relation to accessing mandatory e-learning, and also complained of the lack of a single sign-on to trust systems. An AHP manager (T2-DGH-AHP-02) reported on the impossibility in practice of following recommended password practices, particularly as she was working across two trusts with two email addresses, and on the demotivating effect of password problems associated with accessing statutory and mandatory e-learning. *Could move this to 4.2 governance*

Network performance

Network performance was reported as a problem in two of the trusts. T2-DGH-AHP-02 reported that the network was slow from lunchtime until late afternoon at T1-DGH's main site, constituting a hindrance to data entry relating to clinical work. Low bandwidth and slow downloads of documents were reported to be a problem also at T4-TH (T4-TH-AHP-10). T3-MH-LIS-01 reported that the network there had improved in speed and reliability during her years in post. T4-TH's connection to the Internet is via Janet rather than N3, as with many teaching hospitals (P1); accordingly web searching, including library literature searching, was reported as being relatively fast (T4-TH-LIS-06).

Professional information behaviour	<p>Policies re: generic logins Generic logins are useful for libraries in providing access to e-resources for visitors, including NHS staff from other trusts in support of reciprocal access or co-operative policies. They are also useful as a stop-gap for temporary staff or for new starters to use before they are assigned network accounts, or for students on short-term placements for whom it is difficult to organise timely network account provision. Many trusts, however, restrict their availability, or will not allow them at all. Moreover, acceptable use policies (e.g. that of T1-DGH) insist that users must not share or use others' email addresses, usernames, passwords or smartcards; this is in line with recognised information security good practice (). In T4-TH, generic logins were permitted, but the library was not assigned any. In T1-DGH, library staff are able to provide access to e-resources for visitors by using generic logins on to the university computer network. No mention of them was made in T3-MH; this may relate to the fact that the library service is primarily virtual in nature.</p> <p>Password management Several respondents reported problems in managing the various passwords they required for access to NHS and professional systems. A postgraduate clinical tutor (T3-MH-Med-02) complained of password proliferation in relation to e-resources. A nurse educator (T1-DGH-Nur-08) mentioned passwords in relation to accessing mandatory e-learning, and also complained of the lack of a single sign-on to trust systems. An AHP manager (T2-DGH-AHP-02) reported on the impossibility in practice of following recommended password practices, particularly as she was working across two trusts with two email addresses, and on the demotivating effect of password problems associated with accessing statutory and mandatory e-learning.</p> <p>Wireless networks, Eduroam, BYOD wireless networks All the trusts had a wireless network or networks. In T1-DGH there is a main trust wireless network that is available only to trust staff. The coverage is of variable quality, being notably poor at the trust's T1-DGH-IN site (T1-DGH-AHP-02). There is also a postgraduate centre network, run in collaboration with the university, to which medical students from U3-Med connect. According to U3-Med-01 all the trusts at which medical students are placed offer a reasonable standard of Wi-Fi connectivity; however, T1-DGH-LIS-01 informed the researcher that students frequently complain about the inadequacies of this network, and visit the library instead to complete e-learning, download lectures etc. Plans exist within the trust IT department to take over its management and run it as a 'dirty' trust network to which staff as well as medical students can connect via their own mobile devices (T1-DGH-IT-11).</p> <p>T3-MH offers Wi-Fi in nearly all of its 200 sites, with 'roaming' access, though the quality is variable (T3-MH-Med-02). T3-MH-WPH staff are conducting an unofficial mapping exercise in which sites with poor connectivity are identified and the IT department notified (T3-MH-Nur-18). Access is available only to staff, not to patients or visitors.</p> <p>NB mobile phone signals (3G, 4G) are often poor or totally non-existent within modern NHS premises due to their method of construction; the metal frames of the buildings act as a giant Faraday cage, screening out the signals. Users of the devices are therefore dependent on local Wi-Fi for Internet connections.</p>	
------------------------------------	--	--

T4-TH, as well as having a staff wireless network which is available on most sites, provides Eduroam in some areas for students; also a Bring Your Own Device (BYOD) network, to which staff can connect with their own personal smartphones, tablets or laptops, is in process of being rolled out across the trust. No problems with the performance of any of these networks were mentioned by respondents. (BYOD is discussed further under sections 2.6, 4.6 and 5.6.)

Could move this to organisational dynamics vs. IT infrastructure

Web blocking

--Blocking of web applications – categories

--Blocking of individual websites

--Frequency of blocking experienced

--Impacts of blocking on individual users

--Responses to website blocking – e.g. contacting IT helpdesk -- outcomes

--Technical issues

--Management aspects

[Table listing commonly blocked sites and the position across the four trusts]