



## **NCEPOD Information Security Policies and Procedures**

All staff members have a fundamental duty to safeguard the integrity and security of the data held by NCEPOD. The procedures that must be followed to achieve this vary according to the duties and responsibilities of each individual member of staff. As such, it is not intended that all staff read this document from cover to cover.

**This document should be read in conjunction with section 4.6 of the NCEPOD Staff Handbook - Information Security, Confidentiality and Data Protection Policy**

References beginning ISO refer to the UK implementation of the International Standard ISO/IEC 27001:2013, implemented in the UK as BS ISO/IEC 27001:2017 (previously referred to as BS ISO/IEC 17799:2005 or sometimes in 3<sup>rd</sup> party documentation as BS7799-1:2005). This is the current standard for the establishment, implementation, control and continual improvement of an Information Security Management System (ISMS).

The numbers that follow the ISO prefix refer to specific sections of the document (e.g. ISO 3.1.2 refers to section 3.1.2 of the document), and (where present) letters refer to specific controls (e.g. ISO A.3.2.1 refers to control A.3.2.1 of ISO/IEC 27001:2013).

**Version Control**

All changes to the NCEPOD Information Security Procedures to be documented here. Supporting documentation (as in last column) to be retained if present (i.e. changes arising as result of internal or external review, or as result of ad hoc review in light of individual security threats/breaches).

<b>Version Number</b>	<b>Date of change</b>	<b>Items changed</b>	<b>Reason for changes</b>	<b>Changes authorised by</b>	<b>Changes made by</b>	<b>Additional documentation (inc. location if present)</b>	<b>Sign-Off by</b>
1.0		-	Original first draft of new Security Procedures	CH	PA		
1.1		Various	Review of initial draft by CH	CH	PA		
1.2	Jan 2003	Replacement of the group “Chief Executive, IT Administrator & Database Administrator” with “The Information Security Forum”. Forum then defined in section 2.3.1	To tighten up the security management side of Information Security, & ensure that the capacity the CE, IT Admin etc. are acting in is explicit when it comes to security. To give more flexibility in changes of staffing.	CH	PA		

Version Number	Date of change	Items changed	Reason for changes	Changes authorised by	Changes made by	Additional documentation (inc. location if present)	Sign-Off by
2	Nov 2002 to Feb 2003	<p>Full publication of Security Procedures, after major revision arising from external audit.</p> <p>Nature of all individual changes can be found in additional documents referred to in “Additional documentation” column.</p>	<p>Full audit of Security Policy, Security Procedures, and NCEPOD network itself, undertaken by external consultancy - Horwath Consulting.</p> <p>Recommendations for bringing Policy and Procedures into line with BS7799 generated for implementation by NCEPOD.</p> <p>Also reviewed current Data Protection practices, with recommendations (also implemented).</p>	CH	PA	<p>Horwath Consulting’ Information Security Risk Assessment – “Summary of Findings and Recommendations” &amp; “Follow-on Action Plan” documents</p>	

Version Number	Date of change	Items changed	Reason for changes	Changes authorised by	Changes made by	Additional documentation (inc. location if present)	Sign-Off by
2.1	April 2003	Section 5.2: 5.2e altered, 5.2c and 5.2f removed. New 5.2f inserted (alarm system). Section 6.2: paras 9, 12 & 16 altered (securing server, security markings & external installations). Section 7.2: 7.2e expanded (mail not left unsecured). Section 17.2.2: para 1 expanded (authorised Internet use by temp staff) Appendix F: updated to reflect changes	Procedures reviewed after physical relocation of office (from Royal College of Surgeons to Epworth House). Changes mainly to reflect different physical environment.	CH	PA		
2.2	October 2003	Altered Sections: 6.5, 11.4, 15.4.3, 15.4.4, 17.3.6, 20.3.8	Procedures reviewed after IT staff changes and a new server installation.	CH	SD		
2.3	October 2004	Altered Sections: 20.3.1, Appendix D, 18.1, 1.2. Added section 19.7	Procedures reviewed after external audit by BlueSpark consulting in September 2004. Amended references to the Office Manager throughout.	CH	SD		

Version Number	Date of change	Items changed	Reason for changes	Changes authorised by	Changes made by	Additional documentation (inc. location if present)	Sign-Off by
2.4	April 2007	Altered Sections: 1.2, 2.3.1,5.2,10.7.2,13.2.3,13.6,14.4,14.4.1,20.4.5.3, 24.3 Appendix C (plan3, 4)	Procedures reviewed due to Office relocation to Maple Street. Removal of Project Manager. Updating the referenced contact information.	MM	RA		<u>M. Mar:</u>
2.5	March 2010	Altered sections: 7.8,7.9	Procedures reviewed after external audit by BlueSpark consulting in November 2009. Using NCEPOD reference numbers instead of full hospital name and details.	MM	RA		<u>M. Mar:</u>
2.6	January 2011	Altered section: Appendix F	Altered Appendix F with new references to ISO 27001:2005.	MM	RA		<u>M. Mar:</u>
2.7	February 2011	Correct document sections and controls with new ISO reference	Correct specific ISO 17799 references to those in ISO 27001	MM	RA		<u>M. Mar:</u>
2.8	March 2011	Altered section 13.2.1	Reference to safe deposit box used for storage of off-site backup	MM	RA		<u>M. Mar:</u>
2.9	February 2013	Altered sections 6.8.1, 19.7	Reference to software used for encryption for removable media	MM	RA		<u>M. Mar:</u>
2.10	February 2016	Font refreshed. IM&T changed to IT	General update	MM	RA		<u>M. Mar:</u>
2.11	May 2018	General update and altered section Appendix F	Altered Appendix F with new references to ISO 27001:2013 (BS EN ISO/IEC 27001:2017).	MM	KMS		<u>M. Mar:</u>

Version Number	Date of change	Items changed	Reason for changes	Changes authorised by	Changes made by	Additional documentation (inc. location if present)	Sign-Off by
2.12	February 2019	Data protection section updated	Added Data Protection Impact Assessment Updated Contents pages Removed unnecessary speech marks	MM	KMS		<u>M. Ma</u>
2.13	March 2020	Updated the business continuity plans and had a general update re software and processes	Ensuring they were still relevant	MM	PA		<u>M. Ma</u>
2.14	March 2021	Updated the business continuity plans. Updated policies		MM	NS		<u>M. Ma</u>
2.14	May 2023	Added the encryption of laptops and clearance of office desktops		MM	PA		<u>M. Ma</u>
2.15	Sept 2025	No changes					<u>M. Ma</u>

**Table of Contents**

Table of Contents..... 7

1. Information Security Policy ..... 15

    1.1 Introduction ..... 15

    1.2 BS ISO/IEC 27001:2017 controls ..... 15

        1.2.1 The NCEPOD Information Security, Confidentiality and Data Protection Policy..... 16

    1.3 Purpose..... 16

    1.4 Scope ..... 16

    1.5 Principles ..... 16

    1.6 Underpinning policies & procedures ..... 17

    1.7 Data protection by design & by default ..... 17

    1.8 Responsibilities ..... 18

    1.9 Review and evaluation (ISO A.5.1.2) ..... 19

    1.10 Information security infrastructure (ISO A.5.1.1 – A.5.1.2) ..... 19

    1.11 Individual responsibility under the Policy ..... 19

    1.12. Who should read which section of this document? ..... 19

Figure 1.1: Areas of responsibility and roles: ..... 21

Figure 1.2: Summary of access rights:..... 22

Figure 1.3: Security responsibilities and staff roles..... 22

The procedures ..... 25

2 Security Management (ISO A.6.1, A.5.1.2) ..... 26

    2.1 Objective ..... 26

    2.2 Allocation of Information Security Responsibilities (ISO A.6.1.1) ..... 26

2.3 Annual review, audit and the Management Information Security Forum ..... 26

    2.3.1 The Information Security Forum ..... 26

    2.3.2 Annual review (ISO A.5.1.2)..... 26

    2.3.3 Audit (ISO 18.2.1) ..... 27

    2.3.4 Technical compliance checking (ISO A.18.2.3) ..... 28

3 Security responsibilities (ISO A.6.1.1)..... 28

3.1 Objective ..... 28

3.2 Responsibilities..... 28

4 Risk Management (ISO A.8.2.1 & A.8.1.3) ..... 28

4.1 Objectives..... 28

4.2 Methods..... 28

    4.2.1 Assessing security risks (ISO Introduction, ix)..... 29

    4.2.2 Selecting controls (ISO Introduction) ..... 29

    4.2.3 Best practice and successful implementation ..... 29

    4.3.4 Reporting..... 29

5 Physical and Environmental Security (ISO A.11)..... 31

5.1	Objective .....	31
5.2	Secure areas and physical entry controls (ISO A.11.1.1 – A.11.1.6) .....	31
6	Computer equipment security (ISO A.11.2).....	32
6.1	Objective .....	32
6.2	Equipment siting and protection (ISO A.11.2.1) .....	32
6.3	Power supply (ISO A.11.2.2) .....	34
6.4	Cabling (ISO A.11.2.3).....	34
6.5	Equipment maintenance (ISO A.11.2.4) .....	34
6.6	Remote diagnostic services (ISO A.6.2.2) .....	35
6.7	Security of hard disks containing sensitive data.....	35
6.8	Security of removable media (ISO A.8.3.1 & ISO A.11.2.8).....	35
6.8.1	Secure destruction of removable media (ISO A.11.2.6 & ISO A.8.3.2).....	36
6.9	Security of equipment off site (ISO A.9.2.5 & ISO A.10.7.3) .....	36
6.10	Disposal of equipment (ISO A.11.2.7).....	37
6.11	Unattended hardware (ISO A.11.2.8) .....	38
6.12	Copying of electronic files .....	38
7	Record keeping and data quality (ISO A.8.2.3) .....	39
7.1	Data accuracy procedures .....	39
7.2	Procedures for the correction of errors .....	39
7.3	Responsibilities.....	40
7.4	Physical security (ISO A.8.3.1) .....	40
7.5	Access control .....	41
7.6	Disposal of paper records (ISO A8.3.2 & A.13.2.4) .....	41
7.7	Copying of paper records .....	41
7.8	Anonymisation of medical case notes.....	42
7.9	Reference numbers and codes.....	42
8	Asset registers (ISO A.8.1.1) .....	43
8.1	Objective .....	43
8.2	IT Assets .....	43
8.2.1	IT Hardware (ISO A.8.1.1) .....	43
8.2.2	Software (ISO A.8.1.1) .....	43
8.2.3	Information assets (ISO A.8.1.1).....	44
8.3	Information classification and handling (ISO A.8.2).....	44
9	Security of third-party access (ISO A.6.2) .....	46
9.1	Objective .....	46
9.2	Identification of risks from third party access (ISO A.6.2.1) .....	46
9.3	Security requirements in third party contracts (ISO A.15).....	46
10	Security of remote access including mobile phones and tablets (ISO A.6.2) .....	48
10.1	Objective .....	48

10.2	Access controls.....	48
10.3	Remote working (ISO A.6.2.1 & A.6.2.2) .....	48
10.4	Equipment used for remote access (ISO A. 6.2.1) .....	49
10.5	User account and password practices for remote users .....	50
10.6	Storage of sensitive information on computers used for remote access .....	50
10.7	Software policy for remote access users.....	51
10.8	Software support .....	51
10.9	Anti-virus controls for remote users .....	51
10.10	Use of other anti-virus software .....	52
11	User access (ISO A.9.1 & A.9.2) .....	53
11.1	Objective .....	53
11.2	Access control policy (ISO A.9.1.1) .....	53
11.2.1	Type of information vs. security classification of information.....	53
11.2.1.2	Location of the elements of access control (ISO A.9.1 & ISO A.9.2) .....	54
11.3	User access management (ISO A.9.2).....	55
11.3.1	Registering and de-registering users (ISO A.9.2.1, A.9.2.2) .....	55
11.3.2	User accounts and access privileges (ISO A.9.2.3).....	55
11.3.3	Review of access user rights (ISO A.9.2.5).....	56
11.4	User passwords (ISO A.9.2.4 & ISO A.9.3.1) .....	56
11.4.1	Objective .....	56
11.4.2	User password management (ISO A.7.1).....	57
11.4.3	Password practices (ISO A.7.2.2, ISO A.9.3.1 & A.9.4.3).....	57
11.4.4	Considerations for other passwords.....	58
11.5	User training (ISO A.7.2.2).....	59
12	Security incident management (ISO A.16.1).....	60
12.1	Objective .....	60
12.2	Security incidents (ISO A.16.1) .....	60
12.3	Individual responsibilities (ISO A.16.1.1).....	60
12.4	Reporting of security incidents (ISO A.16.1.2).....	61
12.4.1	Reporting of security weaknesses (ISO A.16.1.3) .....	61
12.4.2	Reporting of software malfunctions (ISO A.12.4.1) .....	62
12.5	Logging security incidents (ISO A.12.4.1) .....	62
12.6	Incident management procedures (ISO A.16.1.1) .....	62
12.6.1	Information system failures and loss of service (ISO A.17.1).....	65
12.6.2	Denial of service (ISO A.16.1.2) .....	66
12.6.3	Errors resulting from incomplete or inaccurate business data.....	66
12.6.4	Breaches of confidentiality (ISO A.16.1.1).....	66
12.7	Contacts with outside organisations (ISO A.15.1.2) .....	67
13	Housekeeping (ISO 8.1) .....	68

13.1	Objective .....	68
13.2	Data backup (ISO A.12.3).....	68
13.2.1	The backup schedule .....	68
13.2.2	Data that are backed up .....	68
13.2.3	Procedure for running backups .....	69
13.2.4	Procedure for restoring data from backups .....	69
13.2.5	Procedure for testing backup and restoration .....	70
13.3	Incident reporting (ISO A.16.1.2 & A.12.4.1) .....	70
13.4	Media disposal (ISO A.10.7.2 & ISO A.10.7.3).....	70
13.5	Information handling procedures.....	71
13.6	Destruction of electronic data.....	71
13.7	General housekeeping .....	71
14	Data validation .....	74
14.1	Objective .....	74
14.2	Data input validation.....	74
14.3	Control of internal processing.....	75
14.3.1	Internal validation procedures and documentation.....	75
14.3.2	High-level data manipulation and validation.....	75
14.3.3	Reporting of processing errors and suspected errors .....	76
14.4	Data output validation .....	76
14.4.1	Data usage validation (case reviewer meetings and report drafts).....	77
14.5	Handling of database errors.....	77
15	Software protection (ISO A.12.5.1) .....	79
15.1	Objective .....	79
15.2	Licensed software (ISO A.12.5.1 & ISO A.18.1.2).....	79
15.3.1	Software standards (ISO A.12.5.1).....	80
15.3.2	Authorisation for software purchase & software installation .....	80
15.4	Anti-virus controls (ISO A.12.2.1) .....	80
15.4.1	Objective .....	80
15.4.2	Anti-virus education .....	81
15.4.3	Virus prevention.....	81
15.4.4	Virus detection .....	82
15.4.5	Incident reporting .....	82
15.4.6	Virus removal .....	82
15.4.7	Recovery from a network wide virus incident .....	82
16	Business continuity planning (ISO A.17) .....	83
16.1	Objective .....	83
16.2	Need for an effective plan.....	83
16.3	Planning for business continuity (ISO A.17.1.1 – ISO A.17.1.2) .....	83

16.3.1	Planning framework and individual business continuity plans (ISO A.17.1.1 – ISO A.17.1.2)	83
16.3.2	Testing and maintaining business continuity plans (ISO A.17.1.3)	84
16.4	Review of business continuity plans	84
16.4.1	Annual review	84
16.4.2	Ad hoc review	84
16.4.3	Elements of the review	85
17	Accessing the Internet	86
17.1	Objective	86
17.2	Security procedures	86
17.2.1	General statement	86
17.2.2	Access control	86
17.2.3	Internet usage	87
17.2.4	Prohibited content	87
17.2.5.1	Downloading files: software and executable code	87
17.2.5.2	Downloading files: static documents	88
17.3	Email protocols (ISO A.13.2.3)	88
17.3.1	Objective	88
17.3.2	General statement (ISO A.13.2.1 & A.13.2.3)	89
17.3.3	Monitoring of email	89
17.3.4	Business usage of the NCEPOD email systems – ncepod.org.uk and nhs.net (ISO A13.2.1)	90
17.3.5	Personal usage of the NCEPOD email system	91
17.3.6	Unsolicited emails (ISO A.12.2.1)	92
17.3.6.1	Reasons to be suspicious (ISO A.12.2.1)	92
17.3.6.2	Reporting of suspicious emails (ISO A.12.2.1 & A.16.1.2)	93
17.3.7	Attachments (ISO A.13.2.1)	93
18	Data Protection	95
18.1	Data Protection 2018 and the General Data Protection Regulation 2016	95
18.2	Subject Access	95
18.3	Data Protection Impact Assessment	95
19	Exchanges of information (ISO A.13.2)	96
19.1	Objective	96
19.2	Information Exchange/Data Sharing Agreements (ISO A.13.2.2)	96
19.3	Security of data/items in transit (ISO A.8.3.3)	97
19.4	Security of electronic mail (ISO A.13.2.3)	97
19.5	Security of electronic office systems (ISO A. 14.1.1)	98
19.6	Other forms of information exchange (ISO A.13.2.1)	98
19.7	Encryption	99
20	Network management (ISO A.9.1)	100

20.1	Objective .....	100
20.2	Network controls (ISO A.9.1.2).....	100
20.3	Network access controls (ISO A.9.1).....	100
20.3.1	Policy on use of network services (ISO A.9.1.2).....	100
20.3.2	Location of sensitive information .....	101
20.3.3	Enforced paths .....	102
20.3.4	User authentication for external connections.....	103
20.3.5	Node authentication ISO .....	103
20.3.6	Remote diagnostic port protection .....	103
20.3.7	Network connection control .....	103
20.3.8	Security of network services .....	104
20.4	Operating system access control (ISO A.9.4).....	104
20.4.1	Objective .....	104
20.4.2	Automatic terminal identification .....	104
20.4.3	Terminal log on procedures (ISO A.9.4.2).....	104
20.4.4.1	User identification and authentication (ISO A.9.2.1).....	105
20.4.4.2	Privilege control management (ISO A.9.2.3) .....	105
20.4.4.3	Privilege review (ISO A.9.2.5) .....	106
20.4.5	Password management system (ISO A.9.2.3).....	106
20.4.5.1	User password management (ISO A.9.2.3).....	106
20.4.5.2	System and service account password management.....	108
20.4.5.3	Management of other passwords .....	108
20.4.6	User of system utilities (ISO A.9.4.4) .....	109
20.4.7	Terminal time out (ISO A.9.4.2) .....	109
20.4.8	Limitation of connection time (ISO A.9.4.2) .....	109
20.5	Application access control (ISO A.9.4).....	111
20.5.1	Objectives.....	111
20.5.2	Information access restriction (ISO A.9.4.1).....	111
20.5.3	Protection of software configuration .....	112
20.5.4	Sensitive system isolation .....	112
20.5.5	Database controls.....	112
21	Monitoring system access and use (ISO A.12.4).....	113
21.1	Objective .....	113
21.2	Event logging.....	113
21.3	Monitoring of system use (ISO A.12.4.1).....	113
21.3.1	Procedures and areas of risk (ISO A.12.4.1) .....	113
21.3.2	Risk factors (ISO A.12.4.1) .....	114
21.4	Logging and reviewing events (ISO A.12.4.1) .....	114
21.5	Clock synchronisation (ISO A.12.4.4).....	114

22	Security of system files (ISO A.12.5) .....	115
22.1	Objectives.....	115
22.2	Control of operational software (ISO A.12.5.1) .....	115
22.3	Protection of system test data (ISO A.14.3.1) .....	115
22.4	Access control to program source library.....	116
23	Security in development and support processes (ISO 8.1 & A.14.2) .....	117
23.1	Objectives.....	117
23.2	Change control procedures (ISO 8.1 & A.14.2.2).....	117
23.3	Technical review of operating system change (ISO 8.1 & A.14.2.3) .....	117
23.4	Restrictions on changes to software packages (ISO 8.1 & A.14.2.4).....	118
23.5	Covert channels and Trojan code (ISO A.12.2) .....	118
23.6	Outsourced software development (ISO 8.1 & A.14.2.7) .....	119
24	Communications and operations management (ISO A.12) .....	120
24.1	Objectives.....	120
24.2	Documented operating procedures (ISO A.12.1.1) .....	120
24.3	Operational change control (ISO A.12.1.2).....	120
24.4	Separation of development and operational facilities (ISO A.12.1.4).....	121
25	System planning and acceptance (ISO A.12.1) .....	122
25.1	Objective .....	122
25.2	Capacity planning (ISO A.12.1.3) .....	122
25.3	Authorisation process for information processing facilities (ISO A.14 & A.11.2.4).....	122
25.4	System acceptance (ISO A.14.2.9) .....	123
26	Systems development and maintenance (ISO 14.1 & A.14.2) .....	124
26.1	Objective .....	124
26.2	Security requirements analysis and specifications (ISO A.14.1.1) .....	124
27	Security of system documentation.....	125
28	Compliance (ISO A.18).....	126
28.1	Objectives (ISO A.15.1).....	126
28.2	Identification of applicable legislation (ISO A.18.1.1).....	126
28.3	Intellectual property rights (ISO A.18.1.2).....	126
28.3.1	Copyright (ISO A.18.1.2) .....	126
28.3.2	Software copyright (ISO A.18.1.2) .....	126
28.4	Safeguarding of organisational records (ISO A.18.1.3).....	127
28.5	Data protection and privacy of personal information (ISO A.18.1.4) .....	127
28.6	Prevention of misuse of information processing facilities (ISO A.18.1.5).....	127
28.7	Collection of evidence (ISO A.16.1.7) .....	127
28.7.1	Rules of evidence (ISO A.16.1.7).....	127
28.7.2	Admissibility of evidence (ISO A.16.1.7) .....	128
28.7.3	Quality and completeness of evidence (ISO A.16.1.7).....	128

29 Personnel security (ISO 6) .....	129
29.1 Objective (ISO A.8) .....	129
29.2 Security considerations for personnel management (ISO A.6 & A7) .....	129
Appendix A - Information classification guidelines .....	130
Appendix B - Asset labelling and handling .....	132
Appendix C - Access control policy.....	134
Appendix D - Business Continuity Plan .....	137
Impact Analysis Table .....	138
Individual plans.....	140
Appendix E - Guidelines for Archiving.....	150
Appendix F – Day to day access to NHS.net/email/public folders/folders on intranet .....	151
F.1 Email - nhs.net .....	151
F.2 Email – study folders on Outlook’s public folders and personal mailbox.....	152
F.3 Case notes.....	152
F. 4 Excluded cases .....	153
F. 5 Data breaches and confidentiality.....	153
F.6 Importing spreadsheets .....	153
F.7 Reviewer CVs.....	154
F. 8 Back ups .....	154
Daily backups occur at 9pm .....	154
Appendix G - Cross reference of ISO 27001 controls to NCEPOD procedures.....	155

## **1. Information Security Policy**

### **1.1 Introduction**

As stated in the section 4.6 of the NCEPOD Staff Handbook (Information Security, Confidentiality and Data Protection Policy), NCEPOD is committed to ensuring the security of the information it holds, under all circumstances, and in all formats. In order to fulfil this commitment, it is essential that NCEPOD staff familiarise themselves with the parts of this document relevant to their particular duties and responsibilities. Equally important is an awareness of the overall aim of the Policy, an overview of which is included at the start of this document.

After the overview is a discussion of the responsibilities of staff members under the Policy, which relates them (via the individual roles and responsibilities of the staff members) to the security procedures that they will need in order to carry out those roles in a secure and controlled manner.

The bulk of the document then details the actual procedures, subdivided according to the broad areas of responsibility as laid out under the preceding section on staff responsibilities.

*All procedures laid out in this document are subject to further review and revision as and when necessary, in accordance with section 4.6.2.3 of the NCEPOD Staff Handbook.*

### **1.2 BS ISO/IEC 27001:2017 controls**

NCEPOD is committed to maintaining a recognised level of best practice for its information security procedures. To this end the NCEPOD procedures have been formulated in conjunction with the International Standard ISO/IEC 27001:2013 Information technology – Security techniques - Information security management systems - Requirements.

ISO/IEC 27001:2013 covers a wide range of security controls, designed to help an organisation ensure that risks are reduced to an acceptable level. Together, these controls provide a means for implementing industry recognised best practice. However, as not all of these controls are universally applicable, NCEPOD has selected for implementation only those controls that are relevant to its organisational structure, business functions and goals. An appendix (Appendix F) has therefore been included referencing those controls that have been incorporated into the NCEPOD Information Security and Confidentiality procedures. Where a control has not been considered appropriate, a brief justification is given.

By using ISO/IEC 27001:2013 to help assess, manage, and review the risks facing NCEPOD, NCEPOD demonstrates its commitment to information security and confidentiality.

### **1.2.1 The NCEPOD Information Security, Confidentiality and Data Protection Policy**

Before reading the sections of this document that detail specific staff responsibilities and procedures, each staff member should be fully conversant with section 4.6 of the NCEPOD Staff Handbook: Information Security, Confidentiality and Data Protection Policy.

In line with ISO/IEC 27001:2013, the policy outlines in clear detail the objectives behind the policy and procedures, emphasizing the commitment by NCEPOD to maintain its information assets in a secure manner. Staff members should therefore thoroughly familiarise themselves with the policy, to make themselves aware of the objectives, scope, importance and responsibilities attached to this commitment. The policy provides references to supporting security documentation and resources where necessary or helpful.

In brief, the overall objective of the policy can best be defined as an attempt to maintain the confidentiality, integrity and availability of all data held by NCEPOD in all situations. Quoting directly from the policy [4.6.1].

### **1.3 Purpose**

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy covers our data protection principles and commitment to common law and legislative compliance and procedures for data protection by design and by default.

### **1.4 Scope**

This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data. This policy applies to all staff, including temporary staff, clinicians and contractors.

### **1.5 Principles**

We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

We will undertake annual audits of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
- Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the GDPR;

- The right to be informed;

- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

In line with legislation we employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

### **1.6 Underpinning policies & procedures**

This policy is underpinned by the following:

- Data Quality Policy – outlines procedures to ensure the accuracy of records and the correction of errors;
- Record Keeping Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share;
- Data Security Policy – outlines procedures for the ensuring the security of data including the reporting of any data security breach;
- Network Management Policy – outlines procedures for securing our network;
- Business Continuity Plan – outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation.

### **1.7 Data protection by design & by default**

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>.

All new systems used for data processing will have data protection built in from the beginning of the system change.

All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

## 1.8 Responsibilities

Our designated Data Protection Champion is ***the Chief Executive***. The key responsibilities of the lead are:

- To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;
- To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.
- To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT.
- To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management and DPO to fulfil this work.
- Our designated DPO is Neil Smith, ***the Deputy Chief Executive***, they can be contacted via email: [nsmith@ncepod.org.uk](mailto:nsmith@ncepod.org.uk); phone: ***020 72519060***; or at the following address: ***NCEPOD, Ground Floor Abbey House, 74-76 St John Street, London, EC1M 4DZ.***

The key responsibilities of the DPO are:

- Overseeing changes to systems and processes;
- Monitoring compliance with the GDPR and the Data Protection Act 2018;
- Completing DPIA;
- Reporting on data protection and compliance with legislation to senior management;
- Liaising, if required, with the Information Commissioner's Office (ICO).

These Procedures are an attempt to put this Policy into action – to enable the full and efficient use of the information held by NCEPOD while at the same time guaranteeing that the data is held and handled in a secure manner. The Procedures are therefore an attempt to balance the security needs of the organisation (full compliance with ISO17799, the UK General Data Protection Regulation and an overall commitment to Information Security) with the business needs of the organisation (to be able to carry out our primary business functions).

To this end, it is an attempt to ensure that:

- Computer systems are properly assessed for security
- Paper records systems are properly assessed for security
- Computer systems are properly maintained and monitored
- Confidentiality, integrity and availability are maintained
- Staff are aware of their responsibilities, roles and accountability
- Procedures to detect, report and resolve security breaches are in place
- Procedures for enabling business continuity (under foreseeable situations) are in place
- Procedures for regular review of the policy, procedures and infrastructure are in place

The procedures ensure both that our Information Security responsibilities are enacted, and that the mechanism to review and monitor the procedures and practices employed (the management framework) is in place.

### **1.9 Review and evaluation (ISO A.5.1.2)**

In line with ISO27001 section A.5.1.2, both the Policy and these procedures are subject to regular review. Specified procedures are laid out within these Procedures governing this periodic review, along with any necessary change review processes (i.e. re-evaluation in response to changes affecting the current situation/controls).

Staff members are notified as and when changes to the Policy and Procedures occur and should ensure that these changes are understood and complied with from the time they are made.

### **1.10 Information security infrastructure (ISO A.5.1.1 – A.5.1.2)**

Section 4.6.2.2 of the Staff Handbook details the organisational infrastructure with regard to information security. The Chief Executive, on behalf of the Trustees, is responsible for the overall implementation and enforcement of the Policy. The IT Manager is, on behalf of the Chief Executive, and with the support of the Information Security Forum (see Section 2.3.1), responsible for the operational management of the IT security. Further details are given within section 4.6.2.2 of the Policy. Specific responsibilities, including those of all other staff and co-ordinators, are given within Section 4.6.3.2 of the Policy and are expanded upon in the next section of this document.

### **1.11 Individual responsibility under the Policy**

Each member of staff has a paramount responsibility for maintaining the security of all data, in all formats, at all times. By signing their formal contracts of employment, members of staff are confirming that they will read and abide by the requirements of the NCEPOD Information Security Policy.

The procedures in this document are intended as guidelines to facilitate Information Governance. As guidelines, they *must* be followed if security is not to be compromised, but there will inevitably be situations that fall outside the scope of these guidelines. When such situations occur, it is important that the aim behind the procedures is upheld. Following these guidelines should therefore be viewed as the *minimum* practice to be adhered to at all times. In this way it is intended that security is maintained during the ordinary day to day functioning of NCEPOD.

The Chief Executive has overall responsibility for the implementation and enforcement of the Policy. The Chief Executive should therefore be consulted on *any* matter concerning actual or potential breaches of confidentiality.

The responsibilities for other individuals within NCEPOD are fully laid out within section 4.6.3.2 of the Policy.

As the procedures in this document are built upon the responsibilities enumerated within 4.6.3.2, breaches of individual procedures are therefore breaches of the Policy itself and are dealt with accordingly.

### **1.12. Who should read which section of this document?**

The security procedures detailed in this document have been categorised according to the roles and responsibilities of NCEPOD staff members. Each member of staff will fall under one or more category in accordance with their duties, rather than their job title. In this way it is hoped that the procedures can be better matched with the working practices of all staff, present and future.

The categories listed are subject to further revision as and when necessary. Similarly, as the responsibilities of an individual member of staff changes, they must remain alert to the impact on the procedures they should be aware of.

The sections which should be read by each individual member of staff can be ascertained from Figures 1.1 & 1.3 (Definition of responsibilities and roles and Security responsibilities and staff roles – both overleaf).

**Failure to follow the procedures as laid out in this document, and in breach of the NCEPOD Information Security Policy, may result in disciplinary action being taken.**

**Figure 1.1: Areas of responsibility and roles:**

<b>Job title / area of responsibility</b>	<b>Access rights (see fig 1.2)</b>	<b>Should read sections in Figure 1.3 listed under</b>
Administrative Officers	Standard	<i>Administrative officer</i>
IT Manager	Higher-level: Network and Database	<i>Network administration, Security management, Data administration</i>
Network support staff (as defined under contract of employment).	Higher-level: Network	<i>Network administration</i>
Data support staff (as defined under contract of employment).	Higher-level: Database	<i>Data administration</i>
Clinical Co-ordinators	Co-ordinators	<i>Clinical Co-ordinators</i>
Chief Executive	Standard	<i>Security management</i>
Office Co-ordinator	Standard	<i>Administrative officer</i>
Research Staff	Standard	<i>Administrative officer</i>
Clinical Researchers	Standard	<i>Security management</i>
Project Manager	Standard	<i>Security management</i>

**Figure 1.2: Summary of access rights:**

Level of access rights	Definition	OBApplies to
Standard	Each individual has full control over files and folders within their designated home folder (the individual work space created for them on the NCEPOD network). They will also have limited access to shared resources based upon their specific role within NCEPOD (as defined in their job description). Access will only be granted to information necessary for fulfilling their job-specific tasks, with the type of access restricted to the minimum necessary to accomplish the tasks (read only, or ability to manipulate the data, as required).	All non-clinical staff without responsibility for administering the NCEPOD network or database.
High-level: Network	High-level access rights are granted for the purpose of authorised system administration and maintenance tasks.	Network administrators and support staff
High-level: Database	High-level access rights are granted for the purpose of authorised database administration and maintenance tasks.	Database administrators and support staff
Clinical Co-ordinators	<p>As with the Standard access rights, each Co-ordinator has full control over their own files and folders, and limited access to shared Co-ordinator resources based upon their specific role within NCEPOD.</p> <p>The Clinical Co-ordinator access level has additional restrictions/elevations, suited to the nature of their function within NCEPOD:</p> <p>No access to information held in administrative or managerial staff folders.</p> <p>Database access rights are limited to viewing &amp; manipulation of sanitised (non-identifiable) case data and anonymous/aggregated data only. They are locked out of database tables containing identifiable information, and tables that would allow them to track backwards to identify individuals or Trusts/hospitals involved in specific cases.</p> <p>Co-ordinator level accounts can be enabled for remote access, if authorised and necessary (see Section 10 of this document).</p>	Clinical Co-ordinators

**Figure 1.3: Security responsibilities and staff roles**

Staff should pay particular attention to sections that are more relevant to their role, as indicated in the following table.

<b>Sections</b>	<b>Staff role</b>	<b>Administrative Officer</b>	<b>Network administration</b>	<b>Data administration</b>	<b>Security management</b>	<b>Clinical Co-ordinators</b>
<b>1</b>	Introduction	Yes	Yes	Yes	Yes	Yes
<b>2</b>	Security Management		Yes		Yes	
<b>3</b>	Security Responsibilities	Yes	Yes	Yes	Yes	Yes
<b>4</b>	Risk Management		Yes		Yes	
<b>5</b>	Physical and environmental security	Yes	Yes	Yes	Yes	Yes
<b>6</b>	Computer equipment security	Yes	Yes	Yes	Yes	Yes
<b>7</b>	Security of paper records	Yes	Yes	Yes	Yes	Yes
<b>8</b>	Assets Register	Yes	Yes	Yes	Yes	
<b>9</b>	Security of third-party access	Yes	Yes	Yes	Yes	Yes
<b>10</b>	Security of remote access		Yes		Yes	Yes
<b>11</b>	User access	Yes	Yes	Yes	Yes	Yes
<b>12</b>	Security incident management	Yes	Yes	Yes	Yes	Yes
<b>13</b>	Housekeeping	Yes	Yes	Yes	Yes	Yes
<b>14</b>	Data validation	Yes	Yes	Yes	Yes	Yes
<b>15</b>	Software protection	Yes	Yes	Yes	Yes	Yes
<b>16</b>	Disaster recovery planning		Yes	Yes	Yes	
<b>17</b>	Accessing the Internet/email protocols	Yes	Yes	Yes	Yes	Yes
<b>18</b>	Data Protection	Yes	Yes	Yes	Yes	Yes
	continued over					

Sections	Staff role	Administrative assistant	Network administration	Data administration	Security management	Clinical Co-ordinators
19	Exchanges of information	Yes	Yes	Yes	Yes	Yes
20	Network Management		Yes	Yes	Yes	
21	Monitoring system access and use		Yes	Yes	Yes	
22	Security of system files		Yes	Yes	Yes	
23	Security in development and support		Yes	Yes	Yes	
24	Communications and operations management		Yes	Yes	Yes	
25	System planning and acceptance		Yes	Yes	Yes	
26	Systems development and maintenance		Yes	Yes	Yes	
27	Security of system documentation		Yes	Yes	Yes	
28	Compliance	Yes	Yes	Yes	Yes	Yes
29	Personnel security				Yes	
<b>Appendix-</b>						
<b>A</b>	Information Classification Guidelines	Yes	Yes	Yes	Yes	Yes
<b>B</b>	Asset labelling and handling	Yes	Yes	Yes	Yes	Yes
<b>C</b>	Access Control Policy	Yes	Yes	Yes	Yes	Yes
<b>D</b>	Business Continuity Plan	Yes	Yes	Yes	Yes	
<b>E</b>	Guidelines for archiving	Yes	Yes	Yes	Yes	Yes
<b>F</b>	Cross Reference of ISO 27001 controls to				Yes	
	NCEPOD Procedures					

## **The procedures**

## **2 Security Management (ISO A.6.1, A.5.1.2)**

### **2.1 Objective**

To establish the management structure for information security within NCEPOD.

### **2.2 Allocation of Information Security Responsibilities (ISO A.6.1.1)**

The Chief Executive, on behalf of the Trustees, is responsible for the overall implementation and enforcement of the Information Security Policy and will also act as the Caldicott Guardian and the Data Controller for NCEPOD. Responsibilities include:

- Ensuring compliance with relevant legislation
- Ensuring compliance with the Policy and procedures
- Responding to breaches of information security

The Information Security Forum (Section 2.3.1) is responsible for the operational management of the security system, including:

- Monitoring and reporting on the state of information security within NCEPOD
- Ensuring that the Information Security Policy is implemented throughout NCEPOD
- Developing detailed procedures to maintain security
- Ensuring that staff are aware of their responsibilities for information security
- Monitoring for actual or potential breaches of information security

### **2.3 Annual review, audit and the Management Information Security Forum**

#### **2.3.1 The Information Security Forum**

The Chief Executive, IT Manager, IG Lead and Clinical Researchers form the NCEPOD Information Security Forum. This Forum meets quarterly and has as its primary purpose to:

- a. review and approve information security policy and overall responsibilities,
- b. monitor significant changes in the exposure of information assets to major threats,
- c. review and monitor information security incidents,
- d. approve major initiatives to enhance information security.

The Forum is the body responsible for handling the annual review of security issues, as per Section 2.3.2.

#### **2.3.2 Annual review (ISO A.5.1.2)**

The Policy and Procedures, and their implementation in business systems and processes, are subject to annual review by the Information Security Forum (ISO A.5.1.2). The review process may utilise external support and advice where necessary, at the discretion of the Chief Executive.

The purpose of the review is to examine the existing Policy and Procedures for effectiveness and cost efficiency, and to react appropriately to any changes to the business practices of NCEPOD. To this end, security incident logs (compiled as under Sections 12.5) and fault logs (Section 13.3) for the previous year are reviewed as part of the full review process.

By this method - keeping a log of the nature, number and impact of all recorded security incidents - the effectiveness of the information security procedures can be accurately assessed during the annual review process.

NCEPOD may choose to seek external advice and support for such review, in order to build and maintain successful policy and practices (ISO A6.1.4, A.18.2.1).

### **2.3.3 Audit (ISO 18.2.1)**

As part of the quarterly review process, NCEPOD internally audits existing controls for compliance. Annually, actual practices are checked against the current Policy and Procedures to ensure compliance and identify any areas where remedial action will need to be taken, or where current Policy and Procedures have not adequately adapted to a change in business processes.

Annual audit requirements are set in advance, by using the previous annual review (scope and actions) as a template, incorporating any new procedures that are considered relevant (in the light of any changes over the previous year). The new requirements are then documented before the audit commences (ISO A.14.1.1).

IT resources (in terms of time and materials) are explicitly identified before the audit so that they can be made available for the necessary duration (ISO A.14.1.1). Similarly, requirements for any special or additional processing (by any member of staff) are identified and agreed beforehand. NCEPOD undergoes external assessment for Cyber Essentials certification.

Checks involving operational systems are carefully planned to minimise disruption to the work of NCEPOD. To minimise the danger of accidental changes being made during auditing, checks on operational system files are limited to read only access where possible (ISO A.14.1.1). Alternatively, checks may be made on a copy of the system file, isolated from the operational system (ISO A.14.1.1, A.6.2). For the latter, the copy is destroyed as soon as the audit is complete.

Data files checked during the audits are also protected via read only access, or by using an isolated copy, to prevent possible loss or alteration to the file. Access to sensitive and/or critical assets during the audit is monitored and logged, to produce a reference trail (ISO A.6.2, A.15.3).

The audit shall incorporate a review of the effect that technological changes have had or are likely to have on the effectiveness of the security procedures outlined in this document.

At the end of the audit, all findings are fully documented, with any necessary evidence (logs, reference trails etc.) appended, so that they can be assessed during the annual review.

All audit documentation, evidence and logs are protected as sensitive information. The audit material will contain information on security weaknesses, along with procedures for minimising those weaknesses, which could be instrumental in breaching security if they were to be accessed by unauthorised individuals.

Although NCEPOD at the moment uses no third-party auditing tools, use of any such tool would be protected to prevent the possibility of misuse or compromise of data (ISO A6.2, A.12.4). Access to the media would be restricted to authorised personnel only, and only the authorised (network support) personnel would install the utilities. They would be installed only for the duration of the audit, and then removed. While installed, they would be restricted from being run (via permissions/privilege settings, if possible, or simple physical location) from being run by unauthorised personnel.

NCEPOD may choose to seek external advice and support for such auditing, up to and including the utilisation of a fully independent audit (ISO A.6.1.4, A.18.2.1).

The Chief Executive will report any major issues of security arising from the audit to the Trustees.

#### **2.3.4 Technical compliance checking (ISO A.18.2.3)**

Specialist external agencies may be employed from time to time to provide technical compliance checking, using specialised software to actively test the security controls in place against security implementation standards. (ISO A.18.2.3)

### **3 Security responsibilities (ISO A.6.1.1)**

#### **3.1 Objective**

To ensure that NCEPOD staff are aware of security risks and their responsibilities to minimise the threats. (ISO A.6.1.1)

#### **3.2 Responsibilities**

Individual responsibilities under the Policy are fully laid out in section 4.6.3 of the Staff Handbook.

While NCEPOD adheres as much as possible to the principle of segregating the management, audit, and execution of duties/areas of responsibility to reduce opportunities for unauthorised modification/misuse of information (ISO A.8.2.3), this is not always possible in practice due to the size of the organisation.

To reduce the risks introduced where segregation of duties is not practical, a full review of all audit & monitoring documentation collected for each quarter occurs at the Information Security Forum. Where the monitoring of an area has to be carried out by the same person responsible for enforcing the procedures for that area (due to size of organisation and division of responsibilities) review documentation is reviewed by the whole Forum. In this way checks are in place to minimise the risk of abuse of position/accidental breaches and identify weakness in the manner in which the audits are carried out.

### **4 Risk Management (ISO A.8.2.1 & A.8.1.3)**

#### **4.1 Objectives**

To identify and counter possible threats to the security policy and standards (ISO Introduction, page ix). This is achieved by:

1. Assessing risk – Identifying threats to the security and of information stored and processed by NCEPOD, and consequently assessing the impact that such threats would have if realised and the probability that these events might happen.
2. Managing risk – The process of controlling and minimising or eliminating the identified security risks for an acceptable cost, given the potential impact and probabilities of occurrence calculated as part of the risk assessment.

#### **4.2 Methods**

All information systems are subject to annual risk management review by the Information Security Forum. This allows NCEPOD to react efficiently to changes in any aspect of the security environment

(changes to the level/nature of threats, to risk, to impact, or to cost/practicality of controls). The review includes:

- a. Identification and review of NCEPOD's information assets and the form in which they are held (ISO A.8.1.1)
- b. Identification and review of the systems or processes used to manage each asset
- c. Identification and review of the security classification of the asset (ISO A.8.2.1)
- d. Evaluation of potential threats
- e. Assessment of any changes in the risk of threat occurring
- f. Assessment of the impact on confidentiality, integrity and availability of data if the threat occurred
- g. Assessment of the overall level of risk
- h. Identification of practical and cost-effective counter measures
- i. Implementation programme for countermeasures

The process of ongoing review is used as the basis for selecting and maintaining appropriate controls. The benefit of bringing in new controls is considered, as well as the appropriateness of existing controls.

These reviews may, from time to time, be subject to independent scrutiny by Trustees or external advisors. (ISO A.6.1.4)

#### **4.2.1 Assessing security risks (ISO Introduction, ix)**

Security requirements are identified by the methodical assessment of security risks to NCEPOD.

Risk assessment is therefore applied to all areas of information processing within NCEPOD, as a whole and in its constituent parts. The results of this assessment help guide the selection (and maintenance) of controls employed within the NCEPOD Policy and Procedures.

#### **4.2.2 Selecting controls (ISO Introduction)**

Once the security requirements have been identified, controls are selected and implemented to ensure risks are reduced to an acceptable level.

Any controls that are essential from a legislative or regulatory point of view (data protection, safeguarding organisational records etc.) are identified and implemented.

Non-regulatory controls (i.e. best practice controls) are selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors (such as loss of reputation) are also taken into account.

#### **4.2.3 Best practice and successful implementation**

NCEPOD aims to provide a policy, and related procedures, which will not only conform to best practice but can be successfully implemented and adhered to.

#### **4.3.4 Reporting**

The results of the review by the Forum may be reported to the Trustees by the Chief Executive, if appropriate. Information Governance is a standing item on the Trustee agenda and reviewed quarterly.



## **5 Physical and Environmental Security (ISO A.11)**

### **5.1 Objective**

To prevent unauthorised access, damage and interference to business premises and information.

Covers physical access to areas containing sensitive information (paper based or electronic) and sensitive equipment. Areas with access restricted to NCEPOD staff in the day to day running of NCEPOD.

### **5.2 Secure areas and physical entry controls (ISO A.11.1.1 – A.11.1.6)**

The NCEPOD offices are considered as secure (restricted) areas for non-NCEPOD staff. As sensitive paperwork will be present on staff members' desks and computers throughout the day, care is taken when there are external visitors to NCEPOD. Specifically –

- a. Visitors to the NCEPOD offices are supervised during their time at NCEPOD. They are only granted access for specific, authorised purposes (for example, case reviewer meetings). (ISO A.11.1.2)
- b. Visitors are never left alone in an area where sensitive information is present in an unsecured state. If they must be present alone within an office, it must be one in which either no sensitive information or equipment is present, or one in which there is sensitive information and equipment has been adequately secured (ISO A.11.1.2).
- c. Access rights to secure areas are regularly reviewed and updated (ISO A.11.1.2)
- d. Staff are encouraged to challenge unescorted strangers, if the situation is one in which they feel comfortable doing so. If the staff member does not feel safe in making the challenge, they should immediately alert security to the presence of the potential intruder (ISO A.11.1.2)
- e. All staff are made aware of the importance of securing empty offices, with specific regard to unattended, sensitive information and equipment. (ISO A.11.1.3). All external doors to the NCEPOD offices are locked when unattended. The doors are locked and checked by the last staff key-holder to leave each evening.
- f. The office is protected by a security alarm system, monitored by GD Security Systems, including motion sensors for outside of office hours security (i.e. when the office is unattended overnight & at weekends). The alarm is activated by the last key holder to leave the office and deactivated by the first key-holder to arrive each morning. Only the non-clinical NCEPOD staff are recognised key holders.  
Any triggering of the alarm is routed directly to the company GD Security Systems both in and outside of office hours. If the incident is outside of office hours, the security company is an authorised key holders to the NCEPOD offices. This company will despatch staff to attend the scene to ascertain the appropriate action to be taken.
- g. Hazardous or combustible materials are stored securely at a safe distance from any secure area (ISO A.9.1.3)
- h. Third party support services personnel are granted access to secure areas and sensitive information processing facilities only when required (ISO A.11.1.4). This access, which is monitored, must be appropriately authorised, and is only given to organisations that have signed an agreement (as under Section 11)
- i. Visitor photographic, video, audio or other recording equipment is not allowed within NCEPOD's premises, unless authorised by the Chief Executive in writing (ISO A.11.1.4)

## 6 Computer equipment security (ISO A.11.2)

### 6.1 Objective

To protect computer equipment against loss or damage and avoid interruption to the work of NCEPOD.

Covers all items of computer equipment (including PCs, laptops, tablets, printers and peripheral devices) except those defined as Removable Media (see Section 6.8).

### 6.2 Equipment siting and protection (ISO A.11.2.1)

Equipment is sited to minimise unnecessary access into secured work areas (ISO A.11.2.1)

Information processing and storage facilities handling sensitive data are positioned to reduce the risk of overlooking during their use (ISO A.11.2.1)

Items identified as requiring special protection are, where practical, isolated to reduce the general level of protection required (ISO A.11.2.1). High-risk items are located separately from lower risk items wherever possible, to enable adequate physical security to be more easily matched to the level of risk.

Equipment is sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access. (ISO A.11.2.1)

During initial siting of the equipment, the impact/likelihood of a disaster happening in nearby premises is taken into consideration (floods, leaks etc.) (ISO A.11.2.1). Specifically, when siting sensitive/essential equipment, attention is paid to minimise the risk of potential threats including theft, fire, smoke, water (or supply failure), dust, vibration, chemical effect, electrical supply interference, electromagnetic radiation, and extremes of temperature and humidity (ISO A.11.2.1). By doing so, while such threats cannot be completely eliminated, they will be minimised.

Where practical, environmental conditions are monitored for conditions that could adversely affect the operation of sensitive equipment and information processing facilities (ISO A.11.2.1). The IT Manager shall perform the function of monitoring the environment, though staff are expected to report *immediately* any such conditions as part of the process for reporting security weaknesses. The IT Manager shall then deal with such conditions by reference to the procedures for handling security weaknesses.

NCEPOD operates a strict no smoking policy (ISO A.11.2.1).

Food and drink may be consumed at each staff members' desk, providing drinks are placed away from workstations. Food and drink may not be consumed near any item of equipment that has been classified as highly critical or highly sensitive in the Asset Register (server, etc.) (ISO A.11.2.1).

The main NCEPOD server(s) are secured in a lockable cabinet to minimise the risk of theft of either the server itself or the disks. The keys for this cabinet are held in the key safe. **The disks of the sever(s) are encrypted by using the BitLocker feature of MS Windows.**

Only the IT Manager and designated network support staff are permitted to remove or interfere with this cabinet.

Where necessary and practical, all other hardware containing sensitive data is similarly secured, and once secured must not be interfered with by any member of staff, aside from the IT Manager and designated network support staff. Items requiring special protection are those which have been classed as 'high risk' in the asset register.

No unsecured hardware may be used to store any sensitive information, unless that information is held in a secure, encrypted format (Section 6.7). Storage of information in this manner must be with the full knowledge and consent of the IT Manager. The IT Manager must be satisfied that sufficient attention has been paid to the security of the data before such permission can be given.

All essential computer equipment is security marked, providing that such marking does not invalidate any conditions of the equipment's warranty. This is the responsibility of the IT Manager.  
**All laptops for remote working are encrypted with Windows BitLocker.**

**Patient identifiable data must not be saved on local hard disks of the devices and NCEPOD staff must not save any sensitive data on local hard disks.**  
**Any files saved on local (office) computers are deleted automatically via scripts on shut down of the computer.**

It is the responsibility of the IT Manager to ensure that all items of computer equipment and/or peripheral devices are installed and sited in accordance with the manufacturer's specification.

Installation of all new hardware must be in full compliance with the manufacturer's instructions. This is in order to ensure that the full functionality of the equipment is utilised, and operating parameters are not compromised in such a way that would lead to the failure of the device, to the introduction of errors in the data held by NCEPOD or would invalidate any guarantee or warranty supplied with the product.

The relocation of existing hardware must be approved and performed by the authorised network support staff. No other staff member may attempt to install, move or any equipment, nor in anyway interfere with existing hardware connected to the network.

Installations outside of the capability of the network support staff are to be performed by staff from the designated IT support company retained by NCEPOD unless authorised by the Chief Executive.

Upon purchase, all new items of hardware will be registered with the manufacturer, to ensure that any direct support offered by the manufacturer, and any warranty included with the purchase of the item, is fully available.

### **6.3 Power supply (ISO A.11.2.2)**

Equipment is protected from power failures and other electrical anomalies according to the criticality of the equipment. While it is outside the control of NCEPOD to guarantee a consistent and steady power supply, the threat to sensitive equipment of spikes, surges and power-outs can be minimised (ISO A.11.2.2).

All sensitive computer equipment is protected from the effects of power surges by the use of, at a minimum, simple surge protectors.

In addition, a cost-benefit analysis with regard to the necessity for protecting particular sensitive items from power-outs is made, at the time of purchase, and reviewed at the annual review of the Information Security Forum (Section 2.3). Where it is viewed as essential that an item of equipment be protected in this way, that item is fitted with battery backup system (UPS) to ensure there is sufficient time to shut down the system in the event of mains power failure (ISO A.11.2.2). This ensures the protection of the sensitive equipment from, and any sensitive data held on that equipment that may become corrupted.

This cost-benefit analysis must take place before each new purchase of computer equipment. If the new item is considered essential to the functioning of NCEPOD, the cost of providing UPS battery backup will be factored into the purchase.

NCEPOD currently uses an APC Smart UPS to provide battery backup to the server in the event of a mains power out. This hardware comes with a software facility (PowerChute Business Edition) to enable automatic, safe shutdown in the event of a power outage lasting longer than a configurable period of time. The configuration of this facility is regularly reviewed as part of NCEPOD's disaster recovery planning (Appendix D), and also in the light of any changes to the software installed on the server, which may alter the time needed for a safe shutdown.

Regular, scheduled tests are carried out by the IT Manager to simulate the effect of a power outage (under business continuity plans in Appendix D). This is to ensure that in the event of a real power failure the system has time to shut the server down in a safe manner, avoiding the potential risk of damage to hardware, and the corruption of data held on the machine.

### **6.4 Cabling (ISO A.11.2.3)**

The IT Manager works with staff and appropriate third parties to ensure that power and telecommunications cabling carrying data or supporting information services are protected from interception or damage, wherever practicable/possible (ISO A.11.2.3).

Specifically, where possible, all cabling (electrical and communications) is sited within the framework of the building or housed within suitable conduits (ISO A.11.2.3).

The IT Manager also works with staff and third parties as appropriate in order to ensure that power cables are segregated from communications cables, to prevent interference (ISO A.11.2.3).

### **6.5 Equipment maintenance (ISO A.11.2.4)**

Equipment is maintained in accordance with the supplier's recommended service intervals and specifications (ISO A.11.2.4). External servicing, where it is viewed as both necessary and cost efficient to do so, may also be considered. The IT Manager is responsible for ensuring that service

intervals and specifications are considered as part of overall information security.

Only personnel authorised by the IT Manager may carry out repairs (ISO A.11.2.4). Authorised personnel would include support engineers employed by contracted third party support companies and engineers dispatched by the manufacturer/service provider (e.g. BT engineer, photocopy engineer).

All third-party support organisations are required to sign formal confidentiality agreements before starting any work (Section 9).

The IT Manager maintains records of all faults/suspected faults, and of any remedial work undertaken by a third party to the NCEPOD system (ISO A.11.2.4). These logs are maintained electronically, for easy reference, and are protected appropriately (Section 2.3.3, Section 27).

#### **6.6 Remote diagnostic services (ISO A.6.2.2)**

NCEPOD will permit remote access to the system by maintenance contractors only under direct supervision and monitoring by the IT Manager. The connection is physically broken when the fault is fixed/contractor ends the session (see also Section 10).

All arrangements involving third party access to organisational information processing facilities are based on formal contracts (Section 9). Such contracts require the contractor to commit to maintaining confidentiality of data and information and only to use qualified engineers.

#### **6.7 Security of hard disks containing sensitive data**

Any hard disks containing sensitive data are secured according to Section 5.2. The removal of hard disks off-site for repair is only done in exceptional circumstances, with the authorisation of the Chief Executive, in writing, and to a contractor who has signed a confidentiality agreement.

Unsecured PCs must never be used to store sensitive information unless, unless authorised in writing, by the Chief Executive (see also Section 20.3.2).

When the storage of information on an unsecured computer has been authorised by the Chief Executive, it becomes the responsibility of the IT Manager to provide the means with which the information can be held securely. Specifically, this entails the installation by the IT Manager of TrueCrypt encryption software, or alternatively PGP encryption software onto the target computer, and the creation of a securely encrypted volume. Once the user of the computer has been instructed in the use of the encryption software, the responsibility for encrypting ALL sensitive data (as authorised by the Chief Executive), and hence for keeping it in a secure format, passes to the individual staff member.

A copy of the information within the encrypted volume is to be maintained by the individual concerned on the NCEPOD server. This is to prevent complete loss of information if the encrypted volume on the individual's PC becomes corrupted or lost in any way, or the passphrase is forgotten. It is the responsibility of the individual to maintain the copy on the server as an up-to-date copy.

Secure destruction of out of commission hard drives is covered in Section 6.10.

#### **6.8 Security of removable media (ISO A.8.3.1 & ISO A.11.2.8)**

Removable media is defined as all disks, tapes, cartridges, USB sticks, removable hard drives including mobile phones and other storage media not permanently secured within the chassis of a

workstation, server, or other item of computer equipment. This includes now obsolete but for recognition one-time-use printer ribbons, carbon paper, optical storage media, and fax films.

Any removable media containing sensitive data must be securely stored in a locked drawer or cabinet when not in use (ISO A.8.3.1). Any data to be copied onto removable media, must be done so into an encrypted volume using TrueCrypt encryption software. The owner of the media (as defined in the Asset Register) is responsible for ensuring that the media is stored in a safe, secure environment. To protect the data contained on the media from corruption, the owner must also ensure the storage environment used is in accordance with manufacturers' specifications (if known) or is generally neutral (room temperature, free from dust or condensation etc.).

No removable media containing patient/clinician/hospital identifiable data to be left in an unsecured state in an unattended office (ISO A.11.2.8)

No removable media containing patient/clinician/hospital identifiable data – any information classified on the asset register as being highly sensitive, may be taken out of the NCEPOD office of any reason. See Appendices A & B (Information Classification, and Information Handling Guidelines).

Authorisation is required from the Chief Executive for all media removed from NCEPOD. Removal and return of the media is logged by the IT Manager (ISO A.12.4.1). These logs are kept for review at the Information Security Forum meetings.

#### **6.8.1 Secure destruction of removable media (ISO A.11.2.6 & ISO A.8.3.2)**

All removable media that has been used to store sensitive information will be securely destroyed at the end of its natural life by, or under the supervision of, the IT Manager.

It is the responsibility of each individual staff member to bring such media to the attention of the IT Manager. All staff will hand all such media to the IT Manager for secure destruction. Media that has contained confidential information may not be reused for any other purpose - they must be securely destroyed.

The IT Manager performs a quarterly check to ensure that all such media have not been overlooked. All removable media that has been used to hold project specific information is securely destroyed as part of the data destruction process outlined in Section 13.6.

Secure destruction is achieved by using Active Disk utility to securely overwrite the media in its entirety, configured for 30 overwrites (the standard for military use). The media is then kept in a secure environment until it is practical to arrange for an authorised third-party specialising in data destruction to physically destroy the media. All of this process is logged, including the initial overwrite, the location of the media while waiting destruction, and the date of the secure destruction. Certificates of destruction are required from the third-party and retained by NCEPOD indefinitely.

Where the facility does not exist to securely overwrite the type of media used the media is formatted, then physically destroyed on site. The remains of the tape will be held securely before handing to the authorised third party for secure destruction. The process is logged, as described above.

#### **6.9 Security of equipment off site (ISO A.9.2.5 & ISO A.10.7.3)**

Regardless of ownership, the use of any equipment outside of NCEPOD's premises for information processing must be authorised, in writing, by the Chief Executive. The security provided must be

equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside the organisation's premises (ISO A.11.2.6).

Information processing equipment includes all forms of personal computers used for home working, or that are being transported away from the normal work location (ISO A.11.2.6).

The Chief Executive must be made aware of the reason for the removal of any computer equipment, and also of the nature of any information that would need to be transferred to the equipment for purposes of working off-site. The Chief Executive reserves the right to deny permission for any information to be transferred to portable equipment if it is deemed too sensitive. Alternatively, permission may be given if it is feasible to encrypt the information in a secure manner (as under Section 19.3.2 of this document).

Authorisation is requested using a standard request form, including the above details, which the Chief Executive must review and authorise by signing off on the request. This is necessary in order to avoid any disputes or confusion about whether authorisation was granted or not.

Equipment owned by NCEPOD is not to be taken off site except with this authorisation. Laptop computers owned by Clinical Co-ordinators are to be kept in a secure place at all times and protected by strong passwords and up to date virus protection.

Equipment and media taken off the premises must not be left unattended in a public place at any time (ISO A.11.2.6).

Manufacturer's instructions for protecting equipment shall be observed at all times while the equipment is off-site (ISO A.11.2.6). Individuals are required to follow such instructions for protecting equipment (e.g. against exposure to strong electromagnetic fields or extremes of temperature/humidity) at all times.

Steps are taken to ensure that adequate insurance cover is in place to protect any equipment owned by NCEPOD while it is off-site (ISO A.11.2.4).

**All laptops for remote working are encrypted with Windows BitLocker.**

#### **6.10 Disposal of equipment (ISO A.11.2.7)**

Computer hardware disposal must be authorised, in writing, by the Chief Executive.

All storage devices (hard drives) that have been used to store sensitive information will have the data securely destroyed by the IT Manager. The data on the disks is overwritten using disk wiping software Active Disk, configured to overwrite the disk securely 30x to a standard for military use. The storage device is then removed from the rest of the hardware, and stored in a secure environment until it is practicable to arrange for an authorised third-party specialising in data destruction to physically destroy the drive. All of this process is logged, including the initial overwrite, the location of the media while waiting destruction, and the date of the secure destruction. Certificates of destruction are required from the third-party and held indefinitely.

Hard drives that cannot be overwritten due to hardware failure (rendering the drive inaccessible) are physically destroyed, as much as is possible, then retained in a secure environment until it can be arranged for an authorised third-party specialising in data destruction to physically destroy it properly (as above).

The remaining hardware (PC case, motherboard, memory etc.) can then, at the discretion of the Chief Executive, and according to its value and usefulness, be resold, donated to charity, donated to a staff member, or kept for spare parts.

#### **6.11 Unattended hardware (ISO A.11.2.8)**

All workstations, servers and laptops left temporarily unattended during the course of the day are to be left in a secure state. PCs are kept in locked cages fixed to the desk and laptops are secured with cables. This can be achieved by physically shutting the equipment down, logging it off the network, locking the session (Windows 10) or enabling a password protected screen saver by pressing the Windows key and L (according to the version of Windows in use).

All computer equipment, with the exception of the server, is to be shut down and switched off overnight and at weekends.

All offices are kept locked when the premises are unattended, at night and at weekends.

#### **6.12 Copying of electronic files**

All copying of electronic files must be done within the secure environment provided - original and copy must both reside within the folder structure provided on the NCEPOD server. No copies of information are to be made to locations outside of this, with the exceptions stated in Sections 6.7, 6.8 & 6.9 (for home/remote working etc.).

Copies of files that have been open may have been left in the Temp folder on a machine by the application or operating system (see Section 13.7). The user of each workstation (the asset owner) is responsible for regularly checking and cleaning out the Temp folder on their workstation. Full details of this are given in Section 13.7

## 7 Record keeping and data quality (ISO A.8.2.3)

To ensure the accuracy of information which we store and process, protect against loss or damage and avoid interruption to the work of NCEPOD.

Covers all instances of electronic or paper records containing patient identifiable, staff identifiable, clinician identifiable, or hospital identifiable information. Any documents relating to the financial or other sensitive business aspects of NCEPOD. All draft documents relating to reports in progress. Any documents otherwise classified as sensitive in the Asset Register.

### 7.1 Data accuracy procedures

We ensure accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

- Authentic – i.e. the data are what they claim to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed;
- Reliable – i.e. the data are complete and accurate
- Integrity – i.e. the data are complete and unaltered
- Useable – i.e. the data can be located when it is required for use and its context is clear.

All staff who record information - whether hardcopy or electronic - have a contractual responsibility to ensure that the data is accurate and as complete as possible. This responsibility extends to any system the staff member has access to.

### 7.2 Procedures for the correction of errors

In-line with national legislation, individuals have the right to have access to their personal data which we process and store. Citizens have the right to the rectification of said records in the instance that their records are inaccurate or incomplete.

Where at all possible, in the instance that we have appropriately shared that individual's records with any third-party we will inform this third-party of the rectification if appropriate.

In all cases we will respond to a request for rectification within one month. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.

To request for their records to be rectified service users or staff should contact us with the request for rectification either verbally or in writing. **Individuals can ask anyone in our organisation to request this, so staff should know their responsibilities to pass on requests to the Chief Executive.** If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.

While we are assessing the request to rectify records, we will restrict processing of the data in question.

In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received.

A record of all rectification requests and outcomes will be kept by the Chief Executive in line with timeframes outlined in NCEPOD's retention schedule.

All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO and to seek a judicial remedy;

### 7.3 Responsibilities

The Data Protection Champion **or equivalent job role** has overall responsibility for Data Quality policies and procedures being reviewed annually and for staff training in data quality and for monitoring data quality throughout the organisation. They also are responsible for responding to rectification requests and recording the outcome of any request.

Every member of staff is individually responsible for the quality of data they personally record – whether on paper or electronically. Additionally, they are responsible for reporting any mistakes they do notice to the Data Protection Champion **or equivalent job role**.

Staff are aware that data accuracy and security is a contractual and legislative requirement, and that breach of this policy might result in disciplinary action.

### 7.4 Physical security (ISO A.8.3.1)

- a. All staff members are expected to operate a clear desk policy at night and weekends in respect of any identifiable data (ISO A.8.3.1).
- b. All patient/clinician/hospital identifiable records are kept in locked cabinets when not in use (ISO A.8.3.1).
- c. Keys to these cabinets are stored in a digitally locked safe when the offices are unattended.
- d. No sensitive paperwork is to be left in an unsecured state. All such paperwork and/or folders is placed back into secure storage when unattended (ISO A.8.3.1). If for any reason this is not practical, the office itself is locked for the duration that it remains empty (ISO A.8.3.1).
- e. Attention is paid to the protection of incoming and outgoing mail points. Mail should not be left in the open in an unsecured office – the office should be locked, or the mail should be temporarily moved to a secure storage point (ISO A.8.3.1). Mail should not be left unsecured overnight.
- f. ~~Care is taken to site the fax machine to minimise the threat of faxes containing sensitive data being left on the fax machine in an unattended office (ISO A.8.3.1). Sensitive information should never be sent by fax (see Section 7.4 below). No longer applicable.~~
- g. Sensitive material should not be left unattended at the photocopier. The code should be cleared after each use to prevent unauthorised access. (ISO A.8.3.1)
- h. Sensitive information should be cleared from the printer immediately it has been printed (ISO A.8.3.1)

## **7.5 Access control**

Under normal circumstances, only those staff members who need access to identifiable (non-anonymised) data/records to fulfil specific business roles are authorised to handle such data. This includes the Administrative Officers, the Chief Executive, the Clinical Researchers, the Clinical Co-ordinators and the IT Manager.

Case reviewers do not have access to non-anonymised data/records, unless there are exceptional circumstances to warrant such access, and *only* when the express permission of the Chief Executive has been given. Such permission may be for short-, medium- or long-term access depending upon the situation, but must always be present, and can at the discretion of the Chief Executive be revoked.

Case folders are not to be removed from the NCEPOD offices at any time without the cases being fully anonymised, including but not limited to the patient/clinician and hospital/Trust/Board details. If removed this must only be for the purpose of reviewer training days and all case must be accompanied by at least two staff members and transported in boxes via taxi cab. Cases must be counted out during the meeting and counted back in at the end, before returning to the NCEPOD office by the same mode of transport.

## **7.6 Disposal of paper records (ISO A8.3.2 & A.13.2.4)**

Identifiable/sensitive paperwork (as identified by the Asset Register) which is no longer required is shredded on a weekly basis. All such paperwork is stored securely in a locked cabinet or draw before destruction.

All documents in case folders are shredded after publication of the relevant report. This is organised and overseen by the Office Administrator and the IT Manager.

Due to the volume of paperwork generated by each study undertaken by NCEPOD, the shredding is undertaken by an external organisation that specialises in secure destruction of data. This organisation is required to sign a confidentiality agreement, or formal contract, as outlined under section 9.3 of this document, before any shredding takes place.

Full documentation of the data destruction, including date and time of collection, and the Certificate of Destruction (if provided) will be retained by the Office Administrator. This information to be held indefinitely.

## **7.7 Copying of paper records**

Any copying of paper records is done in a secure and protected manner. All handling of sensitive paper records is performed within the protected environment of the NCEPOD offices.

Photocopiers are not left unattended while copying sensitive/confidential information.

~~The fax machine is sited to minimise the risk of any information sent to NCEPOD being seen by unauthorised individual. It is checked regularly for incoming faxes. No longer applicable.~~

~~No faxes containing sensitive information are to be sent by any member of NCEPOD. No longer applicable.~~

Any obsolete copies of sensitive information are shredded.

## **7.8 Anonymisation of medical case notes**

As part of its legitimate business functions, NCEPOD collects (and retains for the duration of the study) questionnaires that have been submitted by individual clinicians concerning cases identified by NCEPOD as falling within each studies' sample criteria. These questionnaires will contain information given by the clinician, along with copies of medical case notes relevant to the study (as supporting evidence). These case folders are held securely.

These case folders are used by the Co-ordinators in the formulation of each final report and are reviewed by panels of specially selected reviewers as an aid to this.

Before the case folders are given to the case reviewers for review, they are anonymised by the Administrative Officers. This involves the removal or obscuring of all identifiable information concerning patients. This is done by either cutting out the information or by using a thick black pen to hide the information or by covering sensitive information with a black box electronically before printing.

Whilst it may be possible to hold papers to the light to read some of the information thus obscured, this is treated as a breach of confidentiality by the reviewer and dealt with accordingly.

## **7.9 Reference numbers and codes**

In the process of conducting clinical studies NCEPOD makes use of its own reference numbers for the use in sending out questionnaires and requesting copies of medical case notes. These numbers are unique to each hospital/organisation and patient case within a study. Using these reference numbers NCEPOD limits the need for full names, addresses, or other details when sending out questionnaires or other correspondence.

## **8 Asset registers (ISO A.8.1.1)**

### **8.1 Objective**

To identify NCEPOD's information assets.

To enable NCEPOD to identify the relative value and importance of its assets and allow the process of risk management to be based on realistic foundations.

All information assets are listed in the asset registers and have a nominated owner. The asset register is maintained by the Information Security Forum and are stored within the NCEPOD Intranet (see Section 13.2).

Accountability for assets helps to ensure that the appropriate protection is maintained. While responsibility for implementing controls may be delegated, ownership of the asset may not - accountability for the asset will always remain with the nominated owner.

### **8.2 IT Assets**

#### **8.2.1 IT Hardware (ISO A.8.1.1)**

An up-to-date register of acquisitions and disposals of IT hardware is maintained by the IT Manager. This includes all physical items of computer equipment and peripherals, communications equipment, and magnetic and optical media.

Listed against each item is its location, owner, security classification (ISO A.7.1.1), purchase and manufacture dates, serial number, original purchase value, replacement value (updated at each review) and item cost of any third-party support.

Any new additions to the hardware assets of NCEPOD is documented at time of purchase by the IT Manager.

An annual review of hardware assets is undertaken by the IT Manager for presentation at the relevant Information Security Forum meeting. This review focuses on a revision of the estimated replacement cost of each item and assessing the suitability for continued third party maintenance (if present) for each item. The Information Security Forum discusses issues arising from the review, with any changes authorised by the Chief Executive.

#### **8.2.2 Software (ISO A.8.1.1)**

An up-to-date register of all proprietary software is maintained by the IT Manager to ensure that NCEPOD is aware of its assets and that licensing conditions are followed.

Listed against each item of software are - owner, security classification (ISO A.8.1.1), purchase date, version number, serial and/or license number, original purchase value, replacement value.

Any new software purchased by NCEPOD is added to the register by the IT Manager at the time of purchase.

An annual review of software assets is undertaken by the IT Manager for presentation at the relevant Information Security Forum meeting. This review focuses on a revision of the estimated replacement cost of each item and assessing the suitability for continued third party maintenance (if

present) for each item. The Information Security Forum discusses issues arising from the review, with any changes authorised by the Chief Executive.

### **8.2.3 Information assets (ISO A.8.1.1)**

An up-to-date register of all information assets, including databases, NCEPOD study documentation and system documentation is maintained by the Information Security Forum.

Listed against each item are – asset owners, security classification, location, and risk assessment (ISO A.8.1.2).

A quarterly review of information assets is undertaken by the Information Security Forum.

### **8.3 Information classification and handling (ISO A.8.2)**

All physical, software and informational assets are subject to a process of classification in order to ensure that the correct nature and number of controls are applied to each asset. By establishing the business need for sharing or restricting access to each asset and combining this with the value and sensitivity of each asset, NCEPOD can identify an overall security classification for each item. (ISO A.8.2.1)

This classification originates from, and is reassessed during, the annual review of assets as stated in the final paragraphs of Sections 8.2.1, 8.2.2 & 8.2.3 above. The classification process identifies each asset in terms of the level of its criticality to the organisation, the sensitivity of the data, and its risk in terms of loss to the organisation.

Procedures for the classification of information are found in Appendix A – Information classification guidelines.

Classification allows for appropriate procedures for information handling to be easily matched to the security needs of each asset (ISO A.8.2.2). Procedures can be maintained relating to the handling, copying, storage, transmission and destruction of data based upon the classification of the information, rather than the actual information involved. As the sensitivity or criticality of data can change over time, this allows information to be reclassified without having to change the published handling procedures.

It also allows for different informational assets with the same classification to be protected in the same way, simplifying the process of protection. For example, physical items with the same security classification can be stored in the same secured area; and informational (data) assets with the same classification can be stored within a single, strongly secured part of the network environment.

After classification has been undertaken, it is then the responsibility of individual asset owners to ensure that the control procedures applicable to their asset(s), as defined by the security classification (in conjunction with Appendix B) are being followed.

It is the responsibility of the asset's owner to inform the Information Security Forum of any changes in circumstances that impact on the asset, or changes to the asset itself, that may give rise for the need to reassess the classification of the asset. All changes that may lead to the need for re-categorisation or special handling / protection measures to be employed must be reported as soon as they are noticed.

It is also the responsibility of the asset owners to inform the Forum if at any point they feel that special protection or handling procedures over and above that described in the control procedures (Appendix B) for that particular asset's security classification are required.

It may be appropriate to label or mark physical documentation according to its classification, though of course this may be possible with electronically stored information. Whether it is labelled or not, and whatever its format, the classification should be documented within the assets register.

Information handling procedures for data held by NCEPOD are given in Appendix B –Information labelling and handling procedures.

## **9 Security of third-party access (ISO A.6.2)**

### **9.1 Objective**

To maintain the security of organisational information processing facilities and information assets accessed by third parties.

### **9.2 Identification of risks from third party access (ISO A.6.2.1)**

Where there is a business need for third party access to information assets, a risk assessment is carried out to determine security implications and control requirements. It takes into account the reason for the access (ISO A.6.2.3), the status of the third party, any controls employed by the third party, the value of the information, and the implications of this access to the security/confidentiality of the information.

Consideration is also be paid to the type of access required, as different controls are applicable depending upon whether the access is physical (i.e. on site) or over a network connection (VPN up support facilities) (ISO A.6.2.1 & ISO A.11.4.6).

Any necessary controls (within NCEPOD) are put in place before access is granted. The third party must sign a Confidentiality Agreement that binds them to handling the information in a secure manner (as specified in the Agreement) before access is granted. Where the third party is required to institute its own controls before access is granted, these will be agreed and defined in a contract that may accompany, or may incorporate, the Confidentiality Agreement. No access will be provided until any agreed third-party controls are met.

### **9.3 Security requirements in third party contracts (ISO A.15)**

Where NCEPOD requires specific controls to be put in place by the third party before access to organisational information, these arrangements will be based on formal agreements (contracts). These contracts must specifically refer to the security requirements placed upon the third party by NCEPOD, ensuring that there is an unambiguous understanding between the two parties involved as to acceptable usage of the third-party access.

The contracts may therefore include some, any, or all of the following, depending upon circumstances:

- a. a copy of the relevant sections of the NCEPOD Information Security and Confidentiality Policy (ISO A.5.1.1) concerning third party access, remote access, and any other section relevant to the reason for the access (e.g. for development of third-party solutions to data processing needs)
- b. agreed procedures to protect organisational assets (ISO A.13.2.1)
- c. agreed controls to determine compromise of any assets involved (ISO A.15.1.2, A.8.1.3)
- d. agreed controls to ensure the return or destruction of information and assets at the end of, or at an agreed point of time during, the contract (ISO A.15.1.2)
- e. agreed controls to ensure the integrity and availability of data (ISO A.15.1.2)
- f. restrictions on the use and disclosure of any information asset provided (ISO A.15.1.2)
- g. a description of each service, or asset, which is to be made available (ISO A.15.1.2)
- h. a target level of service and unacceptable levels of service (ISO A.15.1.2)
- i. provision for the transfer of staff (where appropriate – e.g. Co-ordinators) (ISO A.15.1.2)
- j. the respective liabilities of the parties to the agreement (ISO A.15.1.2)
- k. responsibilities with respect to legal matters (e.g. General Data Protection Regulation (ISO A.18.1.2)

- l. Intellectual Property Rights and copyright assignment (ISO A.18.1.2)
- m. access control agreement covering (ISO A. 15.1.2)
  - 1. permitted access methods, and use of unique identifiers
  - 2. an authorisation process for user access and privileges
  - 3. maintenance of a list of individuals authorised to have the agreed access
- n. the definition of verifiable performance criteria (ISO A. 15.1.2)
- o. the right to monitor, and revoke, user activity (ISO A. 15.1.2)
- p. the right to audit contractual responsibilities or have those audits carried out by a third party (ISO 8.1, A.15.2.1)
- q. the establishment of an escalation process for problem resolution (ISO A. 15.1.2)
- r. responsibilities regarding hardware and software installation and maintenance (ISO A. 15.1.2)
- s. a clear reporting structure and agreed reporting formats (ISO A. 15.1.2)
- t. a clear and specified process of change management (ISO A. 15.1.2)
- u. any required physical protection controls and mechanisms to ensure those controls (ISO A. 15.1.2)
- v. user and administrator training in methods, procedures and security (if appropriate) (ISO A. 15.1.2)
- w. controls to ensure protection against malicious software (ISO A.12.2)
- x. arrangements for reporting, notification and investigation of security incidents and breaches (ISO A.16.1)
- y. involvement of the third party with subcontractors (ISO A.15.1.2)

## **10 Security of remote access including mobile phones and tablets (ISO A.6.2)**

### **10.1 Objective**

To enable NCEPOD to control remote access to its systems.

To protect computer equipment used for remote connections to NCEPOD (laptops and desktops) against loss or damage and avoid interruption to the work of NCEPOD that would result from an unsecured laptop falling into the hands of unauthorised individuals.

Covers the use of connections by authorised staff members who need remote access to the NCEPOD network to pursue their legitimate roles and responsibilities. It also applies to the web access to email and the NCEPOD Social Media accounts. The use of remote connections by support staff from authorised third party organisations (as per Section 9).

### **10.2 Access controls**

No external agency is given access to any of the organisation's network, except on the written authority of the Chief Executive. External agencies will only be allowed access to hardware/systems for maintenance purposes. Such access will be restricted only to the item being repaired/maintained, in isolation from the NCEPOD network (if practical). All such access to be governed by formal contract or Confidentiality Agreement as under section 4.6.9 of the Policy.

Remote access to the system using VPN connections is monitored and controlled by the IT Manager.

### **10.3 Remote working (ISO A.6.2.1 & A.6.2.2)**

When using mobile computing facilities, special care needs to be taken to ensure that business information is not compromised. Controls are in place to reduce the risks of allowing remote connections to the NCEPOD network, but the mobile worker should be aware of the practical ways for reducing the risk of connecting from environments outside the direct control of NCEPOD, and act accordingly. This should be borne in mind when logging on to webmail as this will not be over a secure network and people may be able to see the password being typed in.

Permission for remote access by staff and Co-ordinators is at the discretion of the Chief Executive. Express authorisation must be given in writing by the Chief Executive before network staff set up the necessary remote connection facilities. Such permission may also be revoked at the request of the Chief Executive.

Requests for remote working are considered on the individual merits of each case and will only be authorised if the Chief Executive is satisfied that appropriate controls are in place to minimise the risk of compromise. Such decisions are based on factors including:

- a. The existing physical security of the site(s) that the remote user is connecting from (the physical security of the building(s) and room(s) involved) (ISO A. 6.2.2)
- b. The open nature of the proposed environment (open environment with many people, or closed environment) (ISO A. 6.2.2)
- c. The nature and classification of the information that the remote user is accessing (ISO A. 6.2.1)
- d. The threat of unauthorised access to information or resources from other people within the remote environment(s) (ISO A.15.1.2)
- e. The practicality of employing controls (physical, or software based) to minimise the impact of any of the above (see below)

Controls that will impact upon the decision (point e. above) may include:

- a. the presence of suitable (secure) storage at the remote site
- b. restrictions on the work permitted, the hours of work, the classification of the information to be handled, and the services the user can connect to
- c. use of secure communications equipment, channels, and methods
- d. the presence of strong physical security at the remote site
- e. the provision of rules and guidance (as laid out in this section)
- f. the provision of support and maintenance to ensure the equipment is not compromised
- g. procedures for back up and business continuity
- h. presence of security monitoring facilities with appropriate audit
- i. ability to easily revoke access rights when necessary and authorised by Chief Executive

#### **10.4. Equipment used for remote access (ISO A. 6.2.1)**

Laptop computers owned by Clinical Co-ordinators should be kept in a secure place at all times and protected by strong passwords and up to date anti-virus.

All laptops connected remotely to the network and left temporarily unattended should be left in a secure state. This can be achieved by terminating the remote connection, locking the session. The preferred option is to terminate the remote connection, but the situation may dictate otherwise (for instance, the user may lock the machine while a transfer of data is underway).

The protection of remote connections to the NCEPOD network is especially important, as with the connected machine being outside of the NCEPOD offices, NCEPOD will have no direct control over physical access considerations.

Remote access to the system using VPN connections is monitored and controlled by the IT Manager.

### **10.5 User account and password practices for remote users**

Passwords must never be stored on laptop computers.

Passwords must never be stored on any other computer equipment used for the purpose of connecting remotely to the NCEPOD network. This includes those for social media accounts.

Passwords may not be saved simply to facilitate automatic connections to NCEPOD. All remote connections to NCEPOD must remain password protected - the user must have to enter their password for each connection. To save a password would severely compromise the security of the NCEPOD network, as if the laptop were lost or stolen such automated connections could provide the basis for abuse or malicious behaviour.

Passwords should never be disclosed to any third party.

### **10.6 Storage of sensitive information on computers used for remote access**

No information containing patient-, clinician-, or hospital-identifiable information should have been passed to any Co-ordinator electronically so issues concerning the storage of such information on unsecured laptops does not arise.

All sensitive letters, documents and information held in an electronic format that would normally be stored within the authorised folder structure created and maintained on the NCEPOD file server must never be stored on a laptop. Files containing sensitive information must never be stored on the local hard drive of a laptop for any reason.

The manner in which such files are to be protected depends on how sensitive the data is considered to be:

1. the data is of low sensitivity or is not sensitive at all. Such material may be stored on the laptop without the protection of strong encryption.
2. The data is of medium sensitivity. Each item of data (or group of items, if similar) is judged individually with regard to whether strong encryption is required to hold it.
3. The data is highly sensitive. The data must be held in a file that is individually protected by strong encryption or held within an encrypted volume on a disk. This encryption is to be achieved with the PGP encryption software utility provided by the IT Manager. Use of other encryption software, if pre-installed by the owner or supplier of the laptop, may be used instead of PGP software at the discretion of the IT Manager.

It is not sufficient to use the password-protection native to Microsoft Office applications.

### **10.7 Software policy for remote access users**

NCEPOD has an obligation to ensure that software that it owns is installed and used in compliance with the law on licensed products. Any software purchased by NCEPOD for use on a laptop will therefore only be installed in accordance with the manufacturer's specifications, and only when that installation is covered by a valid license.

If the installation of software purchased by NCEPOD on a laptop/desktop involves furnishing the Co-ordinator with installation media, that individual must not make illegal copies of the installation media. Nor should they use the media to make illegal, unlicensed installations of the software. They must install the software only on the machine originally intended for installation by NCEPOD.

The IT Manager maintains an inventory of all software purchased by NCEPOD and installed on each laptop and desktop used to connect remotely to NCEPOD. In this way the IT Manager can ensure that all instances of software owned by NCEPOD, whether on local machines or machines connected via remote access, are legitimately licensed.

Software provided by NCEPOD to the Co-ordinators to facilitate their work for NCEPOD remains the property of NCEPOD. Upon ceasing to work for NCEPOD this software is removed from the laptop by the IT Manager.

### **10.8 Software support**

NCEPOD is only responsible for maintaining software owned by NCEPOD, or that is owned by an individual but used for NCEPOD business purposes. This entails the support of any software listed in the software register, including, but not limited to, Microsoft Office, Adobe Acrobat, Adobe Dreamweaver, Sage 50 Account software (if installed), and any other software installed on a laptop for the furtherance of NCEPOD's objectives.

From time to time, issues not directly related to NCEPOD oriented software may be looked at if the issue is impacting upon NCEPOD related work. This is entirely at the discretion of the IT Manager.

### **10.9 Anti-virus controls for remote users**

Users with the ability to connect remotely to the network should be aware that when they log in, they have the same responsibilities as if they were connected locally. They should therefore follow all of the same anti-virus precautions as local users, with exceptions as detailed in the paragraphs below.

Some procedures that are mandatory for staff using NCEPOD owned computers are not applicable in a situation where the laptop is owned by the individual – the prohibition from installing new software and executable code, for instance. In such circumstances, NCEPOD would request that remote users apply discretion when installing software that may have a negative impact when they next connect to the NCEPOD network.

In line with other users, the provision of anti-virus software for remote users is the first line of defence for the NCEPOD network. The configuration of the anti-virus software may not be tampered with nor altered without the knowledge and agreement of the IT Manager.

It is the responsibility of the IT Manager to ensure that the anti-virus software for all remote users is kept as up to date as possible. This will be achieved through dialogue with the asset's owner, who will be responsible for ensuring that any necessary actions to achieve this are taken.

Remote access users must never connect their laptop to the NCEPOD network if they know or suspect that they are harbouring a virus. The IT Manager must be informed that the remote equipment has/may have a virus. The IT Manager will revoke remote access rights for the duration of the incident.

Upon eradication of the virus, the laptop must be tested and passed as safe by the IT Manager before any new connections are allowed.

Any laptop that is suspected of being infected is disconnected immediately from the network and the remote access facility and rights are terminated for the duration. The right to reconnect to the network will not be re-instated until the IT Manager can verify that the virus has been removed, or the individual involved can demonstrate satisfactorily that effective remedial action has been taken.

#### **10.10 Use of other anti-virus software**

NCEPOD recognises that some of the laptops used to connect to NCEPOD are also used to connect to other networks related to the remote users' employment (e.g. hospital networks).

Where connection to these other networks require the mandatory use of a different anti-virus product than that used by NCEPOD, NCEPOD recognises that this may take priority. In such circumstances, providing that the IT Manager is happy that the other product is of sufficient quality, connections to the NCEPOD network may still be made.

In this circumstance, it becomes wholly the responsibility of the individual co-ordinator to ensure that his/her anti-virus protection is regularly and fully updated.

Situations where the use of other anti-virus software is not considered of sufficient quality, or conflicts with the NCEPOD software, or is not sufficiently regularly updated, is referred to the Chief Executive.

## **11 User access (ISO A.9.1 & A.9.2)**

### **11.1 Objective**

To restrict an individual's access to those systems and information required by their job function.

Covers the accounts used by staff members to logon to the NCEPOD network, and perform the duties required of them by their job description.

### **11.2 Access control policy (ISO A.9.1.1)**

Each staff member is provided with a user account with access privileges set according to their required roles and responsibilities, in line with business requirements. Likewise, each staff member will need access to specific kinds of information to enable them to fulfil their roles but should be blocked from information that they do not need access to, or should not have access to on grounds of confidentiality & data protection.

NCEPOD's access control policy is therefore an explicit attempt to lay out which categories of information each staff member (or group of staff members) should and should not have access to. Attempts by a staff member to access information that they are not authorised to access will be treated as deliberate breaches of confidentiality and dealt with accordingly. Appendix C details each user or user group against permitted types of information and permitted use of processing facilities (applications).

In general, an individual will only be given access to information that they require for the fulfilment of business roles, and only in a format for which they are authorised to see it.

All access to information is conditional upon a contract (staff members and third-party organisations (if appropriate), Confidentiality Agreement (co-ordinators, case reviewers, suppliers), and/or Data Exchange Agreement.

#### **11.2.1 Type of information vs. security classification of information**

Appendix C specifies *types* of information (financial, personnel, project planning & development etc.) that each staff member either should or should not have access to. It is NOT about controls for handling the information according to its *security classification*, which are laid out in Appendix B and throughout the rest of this document.

Appendix C therefore states whether a staff member is allowed access to the type of information *AT ALL*. If he/she is allowed access, then Appendix B (in conjunction with the Asset Register and the rest of the Procedures) provides the procedures necessary for handling that information in a secure manner, in line with its security classification.

**11.2.1.2 Location of the elements of access control (ISO A.9.1 & ISO A.9.2)**

The section of BS 27001 that deals with access control policies (ISO A.9.1.1) cuts across elements enumerated in Section 11.1, 11.2, 12.1, 7.2, and 10.1.1. The following table addresses this by indicating where information concerning each control can be found:

<b>Area</b>	<b>Addressed by section in Procedures</b>
Security requirements relating to individual business applications (ISO A.14.1)	Section 20.5, Appendix C
Identification of all information related to the business applications (ISO A.8.2)	Section 8 Asset Register, Appendix B Appendix C
Policies for information dissemination and authorisation (ISO A.12.1.1)	Appendix B Sections 7 & 19
Consistency between the access control and information classification policies of NCEPOD (ISO A.9.1.1)	Section 11.2.2.1
Relevant legislation and any contractual obligations regarding protection of access to data or services (ISO A.18.1.1)	Section 28
Standard user access profiles for common categories of job (ISO A.9.2)	Section 1.2 Appendix C

Similarly, the section dealing with access control rules (ISO 9.1.1) specifies considerations which cut across these Procedures as a whole. The table below indicates where information on each point can be found:

<b>Area (ISO A.9.1.1)</b>	<b>Addressed by section in Procedures</b>
Differentiating between rules that must always be enforced and rules that are optional or conditional (ISO A.9.1.1)	Individual requirements for rules and practices detailed throughout the Procedures
Establishing rules based on the premise “what must be generally forbidden unless expressly permitted” rather than the weaker rule “everything is generally permitted unless expressly forbidden” (ISO A.9.1.1)	Appendix C, Expressed throughout Procedures
Changes in information labelling/classification that are initiated automatically by information processing facilities and those initiated at the discretion of the user (ISO A.9.1.1)	Section 8.4, Appendix B, Asset Register
Changes in user permissions that are initiated automatically by the information system and those initiated by an administrator (ISO A.9.1.1)	Section 11.3
Rules which require administrator or other approval before enactment and those which do not (ISO A.9.1.1)	Individual requirements for authorisation detailed throughout the Procedures

### **11.3 User access management (ISO A.9.2)**

#### **11.3.1 Registering and de-registering users (ISO A.9.2.1, A.9.2.2)**

The Chief Executive will notify the IT Manager when a new user is to be registered. (ISO A.9.2.1)

Access to the NCEPOD network is controlled through a formal registration process, which will identify in written form the privileges and levels of access that each individual has been assigned. This written record forms the basis of any future auditing of privileges (Section 11.4) (ISO A.9.2.2).

The process of registering each user, creating a user account and assigning privileges to that account includes:

- a. using unique user IDs so that users can be linked to and made responsible for their actions. The use of group IDs should only be permitted where they are suitable for the work carried out (ISO A.9.2.1)
- b. checking that the user has authorisation from the system owner for the use of the information system or service (ISO A.9.2.2)
- c. checking that the level of access granted is appropriate to the business purpose and is consistent with the organisational security policy (ISO A.9.2.4)
- d. through induction and provision of the Policy and Procedures, giving the user a clear understanding of their access rights (ISO A.9.2.1)
- e. through the signing of a Contract of Employment, staff indicate that they agree to abide by the condition of access as laid out in the Policy and Procedures (ISO A.9.2.1 & A.7.2.2)
- f. maintaining a formal record of all persons registered to use the service (ISO A.9.2.1)
- g. immediately removing access rights of users who have changed jobs or left NCEPOD (ISO A.9.2.6)
- h. periodically checking for, and removing, redundant user IDs and accounts (ISO A.9.2.5)
- i. ensuring that redundant user IDs are not issued to other users (ISO A.9.2.5)

When a member of staff leaves NCEPOD, the corresponding user account is immediately disabled by the IT Manager/network support staff, pending removal from the system. Specific actions taken by the IT Manager are given in Section 20.4.4.2 of this document.

To ensure that all relevant issues are addressed, and all necessary actions are taken, a leaver's checklist is circulated by the Chief Executive prior to the staff member leaving. This checklist includes actions that have to be taken before, at the time of leaving, and after the staff member has left. While all the entries are not security related, all the steps that are involved for ensuring no breach of security takes place during/as a result of the staff member going are listed. The checklist is returned to the Chief Executive upon completion of all the tasks. This document is retained.

#### **11.3.2 User accounts and access privileges (ISO A.9.2.3)**

All staff members are assigned a network account when they join NCEPOD.

The necessary access privileges are granted to the user account according to the results of the formal registration process as governed by section 11.3.1. This will ensure that the staff member receives the correct privileges associated with each aspect of their work (ISO A.9.2.3).

It is the responsibility of the IT Manager to provide training to allow the secure and responsible use of this account. Once this training has been provided, it becomes the responsibility of the individual staff member to use the account in a secure and responsible manner.

Most staff members are also assigned a database account. It is the responsibility of the IT Manager to provide the necessary training to allow secure and responsible use of this account.

Each network and database account will provide only the privileges necessary to perform the users' assigned tasks (ISO A.9.2.3). Users should not attempt to increase or in any way alter the level of their own access privileges. Users should not attempt to increase or in any way alter the level of other users' access privileges.

Certain staff members (designated network and database support staff) will receive two sets of network/database account credentials. One of these will have the necessary extended privileges to perform the relevant network or database administration tasks, the other will have standard level privileges for all other daily activities (e.g. data input).

Where a staff member has more than one user account, they must log on with the appropriate account for each task undertaken (i.e. with the appropriate level of security privileges). For instance, if a person has both data input and network administration duties, the user should never log on with administrative rights if they are simply performing data entry tasks. To do so creates the potential for irreversible mistakes.

Access privilege is modified in line with any changes to the individual's roles and responsibilities. All necessary alterations to the account caused by a change in job description and/or responsibilities may only be made by authorised network and database support staff. Any change in job description or responsibility will have involved the input of the Chief Executive, and hence all corresponding changes to user privileges that flow from this are deemed to be authorised changes.

Access privileges are removed when an individual leaves (ISO A.9.2.3). As soon as the member of staff leaves NCEPOD, the IT Manager or other member of network support staff immediately suspends the corresponding user account. Once the IT Manager is satisfied that all resources linked to that account have been cleared of any NCEPOD relevant material, that account is deleted. Home folders belonging to that user are retained, with the information according to the usual schedule of retention. Any emails are likewise kept, but the email address is converted to automatically re-direct emails to an assigned individual (normally the staff members' replacement, Staff members' Manager or the CEO).

### **11.3.3 Review of access user rights (ISO A.9.2.5)**

Staff members' access rights are subject to annual review by the IT Manager, and to ad hoc review as part of the process change management for any changes in role / job description (ISO A.9.2.5).

Temporarily elevation of access rights (e.g. for special, time limited project working) are made by the IT Manager, who will document the nature of the change, and the time period at which the elevation is to be revoked. The removal (upon completion of the project/business need involved) is also logged by the IT Manager (ISO A.9.2.5)

Privilege allocations are checked at quarterly to ensure that no unauthorised privileges have been obtained (ISO A.9.2.5)

## **11.4 User passwords (ISO A.9.2.4 & ISO A.9.3.1)**

### **11.4.1 Objective**

To minimise the risk of unauthorised access to the network by enforcing a strong password policy. To minimise the risk of sustained unauthorised access to the network by ensuring passwords are changed on a regular basis.

Covers standards for creation and safeguarding of the passwords that, in combination with the assigned network and database user accounts, allow staff members to carry out their duties in a safe and secure manner.

#### **11.4.2 User password management (ISO A.7.1)**

No individual is given access to the system until they are properly trained and aware of their security and confidentiality responsibilities.

The allocation and use of passwords is fundamental to the security of the NCEPOD network. Staff members are therefore required to pay very strict adherence to the rules regarding the composition and use of passwords used for accessing the NCEPOD system and the information within it. Each member of staff is fundamentally responsible for the maintenance of their own password in a manner which conforms to the practices set out below.

#### **11.4.3 Password practices (ISO A.7.2.2, ISO A.9.3.1 & A.9.4.3)**

Passwords must never be disclosed (ISO A.7.2.2 & A.9.3.1). The password that enables a member of staff to access the NCEPOD network must NEVER be disclosed to an individual outside the organisation. To do so would render the staff member responsible for any damage or malicious activity following from this, and hence liable to disciplinary measures.

Similarly, the password should never be disclosed to another member of staff (ISO A.9.3.1), with one exception only. If it is essential for a password to be disclosed to a member of the network support staff to further a legitimate task, it may be disclosed. Such disclosure is to be treated as temporary, and only for the duration of the task. Immediately the task is completed, the network support staff will inform the staff member, and that staff member will generate a new password for their user account.

Standard user account passwords should never be written down or sent via email (ISO A.9.3.1). As all standard user account passwords can be over-ridden by the IT Manager in an emergency, there is no legitimate reason that these particular passwords should be written down.

For business continuity purposes, the top-level administrator account for the network and the database are recorded. These passwords are written down, stored in sealed envelopes (with the IT Manager's signature written clearly over the seal) and held securely with the monthly backup disks in the NCEPOD safe deposit company.

If at any time a user suspects that their password has become known to any other person, either within or without NCEPOD, they must *immediately* change their password, then inform the IT Manager at the earliest available opportunity (ISO A.9.3.1). Failure to change the password immediately would render the staff member responsible for any breaches that occur from the point of suspicion forward until the password is changed. Failure to notify the IT Manager at the earliest available opportunity would also constitute a breach of NCEPOD security procedures for reporting actual or potential security breaches.

Passwords should be chosen that maintain an appropriate balance between ease of usability (easy to remember) and security (complexity of composition) (ISO A.9.3.1). Care should be taken when selecting passwords, which should always conform to the following guidelines –

- a. Passwords should be unconnected with the individual and should be alphanumeric.
- b. To prevent security being compromised by the use of easy to guess passwords, certain categories of password are expressly forbidden. No passwords that relate to the work an

individual does, to their family life (including names of pets), or to their interests and hobbies are permissible. Such passwords provide weak security in that anyone who has knowledge of the individual's background, or has access to personal information, may (given time) guess such passwords correctly.

- c. For maximum security, passwords used to access the NCEPOD network should contain a minimum of eight characters and should be alphanumeric. The strongest category of password would be a random combination of letters and numbers, but NCEPOD recognises that due to the difficulty of remembering such a password, especially where a user's password is subject to regular change, this may not be practicable. It is therefore acceptable to use a combination of dictionary words and numbers or non-alpha characters. Dictionary words are, as the name implies, words that appear in a standard dictionary and will therefore be easier to remember than a string of random letters. Non-alpha characters comprise the set of symbols accessible from a standard keyboard by using the shift key in conjunction with one other standard key (keys 1 to 0 for instance, giving !"£\$%^&\*() as usable characters for a password).
- d. It is very important that where a dictionary word is used, it MUST be used in conjunction with numeric/non-alpha characters. This is because the most common (and quickest) automated cyber-attack on passwords is the dictionary attack. If your password is nothing more than a dictionary word, a dictionary attack (comparing your password to every single word in a dictionary, sequentially) would always succeed in cracking your password. Adding non-alpha characters to the password (or better still, splitting the dictionary word by inserting non-alpha characters within it) would prevent this.
- e. As even random string passwords containing non-alpha characters and no recognisable dictionary words are susceptible (eventually) to the slower brute-force password cracking software that is available, regularly changing passwords is very important.

Passwords should be changed every three months (ISO A.9.3.1) – this change is automatically enforced by the system policies configured for the NCEPOD network. This will lessen the chances of sustained abuse of a user account over any great length of time.

To prevent staff members recycling old passwords (ISO A.9.3.1), the system is configured to retain a list of each user accounts previous passwords, preventing a user from alternating between passwords.

Temporary passwords (used by the IT Manager to set up a user account for a new member of staff) should be changed immediately upon receipt of the account by the staff member (ISO A.9.2.4 & A.9.3.1). The system enforces this, by default, at the first log on by the staff member.

All temporary passwords (as above) should be communicated to the staff member verbally, and should never be written down for, or emailed to, the staff member (ISO A.9.2.4).

Passwords should never be stored on computer systems in an unprotected form (ISO A.9.2.4), or as part of any automated logon routines (whether protected or not) (ISO A.9.3.1).

The passwords to an individual's user account should never be shared with other users (ISO A.9.3.1).

The password for the NCEPOD social media sites is set by the Chief Executive and shared with limited staff tasked to manage them. As these sites (Twitter) are usually kept open, staff with access to these accounts, using them on their mobile phones must have a personal lock on their mobile phone. In the event of any breach such as phone access or loss then the Chief Executive must be notified immediately to change the password and check activity on the social media accounts.

#### **11.4.4 Considerations for other passwords**

For passwords other than user account passwords, it may be acceptable to keep a record of the password. Such circumstances are rare, are limited to situations where the password does not tie into the Windows Server security model (and hence cannot be over-ridden by the network support staff), and where it is known only to one person. In these instances the recorded password must be kept in a sealed envelope in a secured cabinet or safe. Situations where this is permissible would include, but are not limited to, the securing of sensitive information by strong encryption software.

If the information protected by any form of encryption is vital to the continuing functioning of NCEPOD, then the recording of the password and its secure storage becomes a requirement. In the event of the user's unavailability, for whatever reason, there must be a way in which the essential information can be recovered.

#### **11.5 User training (ISO A.7.2.2)**

All employees of NCEPOD will receive appropriate security training and regular updates concerning user access to the network.

This will include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, and the use of software packages in a secure and responsible manner.

## **12 Security incident management (ISO A.16.1)**

### **12.1 Objective**

To detect, investigate and resolve any suspected/actual security breach.

### **12.2 Security incidents (ISO A.16.1)**

Incidents affecting security are to be reported by staff members to the IT Manager immediately. In the absence of the IT Manager, another member of the network support staff (if IT related) or member of the Information Security Forum (if not IT related) should be informed.

A security incident is an event that could result in:

- a. Degraded system integrity
- b. Loss of system availability
- c. Disclosure of confidential information
- d. Disruption of activity
- e. Legal action
- f. Unauthorised access to applications

Security breaches may result in disciplinary action (ISO A.7.2.3).

### **12.3 Individual responsibilities (ISO A.16.1.1)**

Each member of staff and all Co-ordinators are personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

Each member of staff and all Co-ordinators are responsible for reporting any actual or potential security breaches to the IT Manager as soon as they occur.

A security breach is simply any event that has led to one of the situations defined under the Section 12.2 above or has the potential to cause one of those defined situations.

It is the responsibility of each member of staff to report any breach, (actual, suspected or potential) to the appropriate person (Section 12.4.1). Responsibility for investigating and documenting the incident is assigned according to Sections 12.4.1, 12.4.2 & 12.4.3, below.

Security breaches may result in disciplinary action (ISO A.7.2.3).

The failure to report a known security breach may also result in disciplinary action being taken.

#### **12.4 Reporting of security incidents (ISO A.16.1.2)**

A security incident is one in which the integrity, confidentiality or availability of data held by NCEPOD has been compromised, physically or electronically.

Incidents involving the NCEPOD network are the responsibility of the IT Manager and should be reported immediately so that the IT Manager (or other network support staff) can initiate the appropriate action (Sections 12.6.1 & 12.6.2). The Chief Executive will be kept informed throughout the investigation.

Incidents involving the functioning of the NCEPOD database are the responsibility of the IT Manager and should be reported immediately so that the IT Manager (or other database support staff) can initiate the appropriate action (Sections 12.6.1 & 12.6.3). The Chief Executive will be kept informed throughout the investigation.

Incidents involving errors in the NCEPOD project data are the responsibility of the Data Asset Owners and should be reported immediately to the Chief Executive so that they can initiate the appropriate action (as under Section 12.6.3).

Incidents involving breaches of confidentiality/related security breaches are the responsibility of the Chief Executive and should be reported immediately to the Chief Executive so that appropriate action can be initiated. (Section 12.6.4)

All data breaches must be added to the Breach of Patient Confidentiality Record spreadsheet. This is monitored to identify trends or organisations who repeatedly breach confidentiality. Data breaches can also be raised with any member of the Information Security Forum or in a PIMS meeting.

Incidents of sufficient severity may lead to the Chief Executive informing the Chair and Trustees, and the Information Commissioners Office as appropriate. Breaches of confidentiality must be reported to the Information Commissioner's Office without undue delay and within 72 hours. The controller should communicate a personal data breach to the data subject, without undue delay, if that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow them to take the necessary precautions.

It should be determined that all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform the Information Commissioner's Office and the data subject.

Failure to report a serious data breach or to protect against data breaches could result in administrative fines being applied by the Information Commissioner's Office, under the GDPR.

##### **12.4.1 Reporting of security weaknesses (ISO A.16.1.3)**

A security weakness is a situation where a member of staff has noticed that inadequate controls are in place, or adequate controls should be in place but have failed (e.g. software failure, broken locks). The end result of which is that the NCEPOD information systems are vulnerable, but no actual breach has occurred.

NCEPOD staff are required to report any observed (or suspected) security weaknesses or threats to the IT Manager (network or database related), Clinical Researchers or Project Manager (data related) or Chief Executive (breaches of confidentiality and all related issues).

The appropriate person (as above) will then investigate (or initiate an investigation into) the incident and take appropriate action. If necessary, the service involved in the incident and/or all services depending upon the actual service involved may be suspended or terminated for the duration of the investigation.

Under no circumstances should unauthorised staff members attempt to prove a suspected weakness, as this may lead to actual damage being caused, or an actual breach of security being created, and is therefore viewed as misuse of the system (with disciplinary procedures accordingly invoked).

Incidents of sufficient severity may lead to the Chief Executive informing the Chairman and Trustees, as appropriate.

#### **12.4.2 Reporting of software malfunctions (ISO A.12.4.1)**

As software malfunction raises the possibility of data corruption (and hence the integrity of the data) all software malfunctions are to be considered potential breaches of security (in its widest sense).

All users of the network should therefore report any suspected/actual malfunctioning of any software on the network. The symptoms and any error messages should be noted down and passed to the IT Manager as part of the standard incident reporting process (Section 13.3). The suspected malfunction will then be addressed as laid out in Section 12.6.1.

The IT Manager will consider any ramifications for system security as part of the incident handling procedure (13.3). Any software malfunction that may involve the compromise of the security of (or data held on) the network is logged as a security incident (as under Section 12.5)

Users must not attempt to remove suspect software or 'fix' software malfunctions unless authorised to do so.

#### **12.5 Logging security incidents (ISO A.12.4.1)**

All actual security incidents are formally logged by the IT Manager and categorised by severity. Any necessary action/resolution is also recorded, as governed here and in Section 13.3 (Incident Reporting).

These logs are maintained to provide a record of all incidents, actions taken, and successful or unsuccessful resolutions. The logs are held securely.

The logs are retained so that they can be used for:

1. Regular internal security reviews (as part of the annual review of security measures (see Section 2).
2. Internal problem analysis
3. Use as evidence in relation to a potential breach of contract, breach of regulatory requirements or in the event of legal proceedings
4. Negotiating for compensation from software and service suppliers

#### **12.6 Incident management procedures (ISO A.16.1.1)**

The precise steps to be taken in response to an incident cannot always be anticipated, but action taken should always conform to the guidelines below and should always be fully documented. This

documenting of the responses and solutions to each incident will enable NCEPOD to build up a body of information and expertise to

- a. prevent (or minimise) the likelihood of similar incidents occurring in the future, and
- b. provide a body of documentation to aid quick and appropriate response if the situation recurs (ISO A.16.1.1 & A.16.1.7)

Each incident will fall into one (or more) of four broad categories (see Sections 12.6.1 to 12.6.4), with different implications for handling and resolving the incident and any connected consequences. However, all incident handling will follow the same pattern of investigation, resolution, damage control and audit (as laid out below) to ensure that the incident is both handled in an appropriate manner, and that lessons can be learned from reviewing the incident.

Suspected incidents & weaknesses are handled as if they are actual incidents/weaknesses until they prove to be otherwise.

1. Initial reporting of the incident to the appropriate authority (Section 14.4.1)
2. Analysis and identification of the cause of the incident (ISO A.16.1.6)
3. Analysis and identification of any impact on/changes to related systems caused by the incident
4. Analysis and identification of any impact on data (errors, corruption etc.) caused by the incident
5. Analysis and identification of any impact on physical security measures (broken locks etc.)
6. For system failures (network and database incidents) isolation of the information and systems involved (until the incident is satisfactorily concluded) is essential. This may require terminating access to services, applications or information, or even physically isolating devices. Services should not be re-started, and information should not be released for use by staff, until the incident has been resolved, and the information processed by the system has been checked for its integrity (i.e. has not been corrupted)

7. Resolution of the incident at hand – including steps to
  - a. resolve any damage to information processing facilities and relates systems,
  - b. undo any corruption/errors within data caused by the incident,
  - c. resolve any other issues brought to light by the investigation
8. Resolution of the incident is overseen and carefully controlled (by the appropriate person, specified in Section 12.4) to ensure that
  - a. only authorised staff are involved in any investigation and repair of live systems and data (ISO A.16.1.1). For IT related incidents, this will be the IT Manager (and designated IT support staff). Incidents involving non-IT or general issues will be handled by the Chief Executive, or any other member of the Information Security Forum authorised to handle it by the Chief Executive's behalf (on a case by case basis)
  - b. if involved, only external support staff from authorised companies, with which NCEPOD has a Confidentiality Agreement, are used. Depending upon the criticality of the information/system involved, and the likely timescale for attempting to resolve the issue in-house, third-party support organisations may be called in to expedite resolution of the problem. Estimation of the timescales involved should include time taken to analyse and identify the cause of the problem, and likely time taken to plan and implement a resolution to the problem
  - c. all actions taken are documented in detail (ISO A.16.1.6 & A.16.1.7)
  - d. all steps to resolve the issue that will have an impact on other systems and/or data are authorised by the appropriate person before being taken (ISO A.16.1.1) and are checked to ensure effectiveness
  - e. the integrity of the systems involved, and the data held, is confirmed before the system/data is made available for general use again (ISO A.16.1.2). It is essential that after any incident, the integrity of the affected business system, relevant controls, and any information affected by the incident, be confirmed before the incident can be viewed as resolved
9. Planning and implementation of remedies to prevent recurrence of the problem, including any changes necessary to practices and procedures, including updating of Policy and Procedure documents to reflect this (ISO A.16.1.6)

10. Collection of audit trails and any other evidence necessary (ISO A.16.1.3 & A.16.1.7). This evidence will form part of the full record of the incident, but will also be necessary for
  - a. internal problem analysis at the next Information Security Forum, where all such breaches (including action taken to resolve, and changes to Procedures undertaken) are reviewed (ISO A.17.1.3),
  - b. use as evidence in relation to any potential disciplinary hearings (if appropriate), breaches of regulatory requirements, or any civil or criminal proceedings etc. (ISO A.16.1.7). If it is to be used as evidence, NCEPOD will collect and treat it in a manner laid out in Section 28.7.
  - c. negotiating for compensation from software and service suppliers (ISO A.16.1.7, 8.1)
  - d. evidence may also be needed for insurance claims
11. Reporting back any action taken, and any issues surrounding the resolution, to those involved in the incident. Debriefing of those involved with handling the incident, with any significant issues raised about the handling of the incident documented so that they can be considered at the formal review (see step 15)
12. Reporting the event (if necessary) to any appropriate authority (internal or external) (ISO A.16.1.3)
13. Completion of a fully documented incident report, including a report of the original incident plus relevant and explicit documentation of actions taken under all of the above steps (1 to 12). This documentation will be reviewed, and may also form the basis of a formal procedure for handling similar incidents
14. Formal signing off of the incident, once satisfactory resolution has been achieved
15. Full review of the incident itself, the manner in which it was handled, and any changes made to processes and procedures triggered by the incident, at the next Information Security Forum meeting.

#### **12.6.1 Information system failures and loss of service (ISO A.17.1)**

Incidents dealing with system and processing failures (e.g. loss of service, loss of power, malfunctioning of software) are treated as threats to the functioning of NCEPOD, and so are covered within NCEPOD's Business Continuity Plans (Appendix D).

These plans lay out all the steps necessary to identify, correct, and document such incidents. The Business Continuity Planning mirrors, in essence, the steps documented in Section 12.6

### **12.6.2 Denial of service (ISO A.16.1.2)**

Because denial of service incidents in effect means loss of processing power (complete or partial) and effect the functioning of NCEPOD, they are covered in NCEPOD's Business Continuity Plans (Appendix D).

### **12.6.3 Errors resulting from incomplete or inaccurate business data**

Incidents involving errors in the NCEPOD project data are the responsibility of the Project Manager and should be reported immediately so that the Project Manager can initiate the appropriate action (as under Section 12.6.3). The Chief Executive will be kept informed throughout the investigation.

As such matters involve live data, use of the data affected will be frozen for the duration of the investigation. If necessary, all staff apart from those authorised to investigate the matter will be locked out from the data by resetting the permissions on that database table. This may not be possible in all cases (where the data affected is only a small amount of data within a table) but will be done when necessary/

Investigation and resolution will proceed according to the steps documented in Section 12.6. As the investigation may reveal that the data was inaccurate at the point at which it was transmitted to NCEPOD by a third party (i.e. data as supplied was inaccurate), then resolution may be achieved by actions taken by that third party to re-send the information. Such a resolution must still be documented and signed off.

### **12.6.4 Breaches of confidentiality (ISO A.16.1.1)**

All incidents involving suspected/actual breaches of confidentiality or provision of inaccurate information to a third party are immediately referred to the Chief Executive (as under Section 12.4.1).

Incidents where confidentiality has been breached are very serious, as they have the capacity to damage the reputation, and impair the effectiveness, of NCEPOD.

The Chief Executive will therefore take any and all appropriate actions to contain and minimise the (potential) damage caused by any breach of confidentiality.

The Chief Executive will initiate an investigation, which can be assigned to any relevant member of staff (involving the IT Manager if the breach was caused by a system incident, for instance) but will retain ultimate authority at each step.

Investigation and resolution will proceed according to the steps documented in Section 12.6

## **12.7 Contacts with outside organisations (ISO A.15.1.2)**

Contact with appropriate third parties is maintained as a normal part of the NCEPOD security incident handling procedures. Contact details (including phone numbers, account managers, dedicated support line numbers etc.) are maintained for all companies that may need to be involved in handling a security incident. This includes (but is not limited to) computer & IT support companies with which NCEPOD has a contract, relevant telecommunications companies (BT), IT service providers (Easynet – for ADSL, BT N3 – for ASDL) etc. Contact numbers of organisations that may need to be informed of security breaches (landlord and/or police, if serious) are also maintained.

Before any confidential information is shared with these companies, the company must sign a data exchange agreement/confidentiality agreement, as outlined in Section 19.

## **13 Housekeeping (ISO 8.1)**

### **13.1 Objective**

To maintain the integrity and availability of computer and informational assets.

### **13.2 Data backup (ISO A.12.3)**

#### **13.2.1 The backup schedule**

NCEPOD employs a combination of daily (on site) and weekly (off-site) backups to ensure a solid basis for disaster recovery purposes.

Hard drives (NAS: Network attached Storage) are used for the daily backup, creating a rotation period of one working week. In this way, data can be restored from any prior day within a period of one week.

In addition, every week one of the daily backups is rotated with one stored in secure, off-site storage. Immediately after the backup is run, the disk used is taken to the secure deposit box, and the previous disk is brought back to the office for use next time. By rotating the disks, a backup is kept safely off site (in case of catastrophic disaster at the NCEPOD offices) that will contain information from a maximum of weeks prior to the disaster (worst case scenario, where the disaster happens on day of or one day prior to the monthly backup).

#### **13.2.2 Data that are backed up**

All information pertaining to the business functioning of NCEPOD is backed up on a daily basis, in accordance with the schedule in Section 13.2.1. This is regardless of the security category of the information.

All information pertaining to the projects run by NCEPOD is backed up on a daily basis, in accordance with the schedule in Section 13.2.1. This is regardless of the security category of the information.

To ensure that this is the case, all of NCEPOD's informational assets (in electronic form) are held within the designated home folder structure. All of the individual classes of informational asset are listed in the Asset Register, which specifies if they are backed up, and who is responsible to ensure that this actually happens.

It is the responsibility of the IT Manager to ensure that any changes to the NCEPOD folder structure are reflected in the daily backup script. It is essential that any new folder created should be accounted for and backed up accordingly. Any sub-folders within each user's individual home folder are automatically backed up by software.

All mailboxes are backed up on a daily basis, to insure against loss of important information transmitted by email. All public folders (NCEPOD calendar, contact lists etc.) are also backed up.

Non-critical system or application files are not backed up (i.e. files that can be replicated by re-installation of operating system or application).

All NCEPOD business or project related files are stored on the server, so no provision is made for backing up files on individual workstations.

All information on the backup drives (for all backups) is encrypted as part of the backup process.

### **13.2.3 Procedure for running backups**

To enable the backing up (and restoration) of data, NCEPOD uses an automated software solution – Altaro Virtualisation Backup. This software is configured and maintained by the IT Manager, assisted by the designated IT support staff.

The IT Manager is responsible for ensuring that the software is configured correctly to back up all the relevant information, and that changes to the folder structure are reflected in the backup script.

The software is configured to run the same backup script every weekday, at 21:00, and to email the results of the report to the IT Manager, the designated IT support company, and the IT support staff member. The software is also configured to verify the contents of the backup against the original files (on disk) and to report any discrepancies, which (if present) would need to be investigated, as they may be indicative of a failure to backup individual files.

Notification is emailed automatically to the IT Manager and the IT support company to identify when errors in the backup have occurred. The IT Manager will liaise with the IT support company to handle the issue and ensure the backup completes. The IT support member of staff is responsible for changing the backup media to ensure that the correct tape is in for the correct day. Each of the daily backups are marked according to their place in the schedule – from Monday to Friday. The relevant backup file is therefore indicated by the specific day of the week.

The weekly backup is stored in a safety deposit box (ISO A.12.3.1). The Balthorne Safe Deposit Centre Company is used, the contact details for which (including address and phone number) are maintained on the NCEPOD Contacts folder, accessible via Outlook.

The disks are held within a safety deposit box, but due to the nature of the information on the disks, they are first stored in a locked box accessible only with a key held by NCEPOD. This key is held securely within the NCEPOD office and accessible by designated members of staff authorised to access the locked box.

New backup media are formatted and dated when they are first used. To prevent the unavoidable degrading of the backup media (over time and with use) interfering with NCEPOD business continuity, the backup media is used and then retired in accordance with the manufacturer's specifications. The recommended life span of the media used is one year, so the tapes are replaced annually.

One-off, permanent backups of useful information are to be also made when necessary, preferably on optical media to preserve the information for longer periods. The content of these backups dictates the security and retention period for the media.

### **13.2.4 Procedure for restoring data from backups**

Restoration of data from backup media is only performed by the IT Manager or IT Support Company, and under authorised circumstances.

In most cases, this will be formally authorised, overseen and documented as part of a response to a security incident (Section 12).

Authorised individuals include only the IT Manager and officially designated support staff (and only where training has been given on the software used for backing up and restoring).

The data is restored using the restore function of the Altaro Virtualisation Backup software. Data can be restored in its entirety, or on a file-by-file basis, according to requirements.

As a safety precaution, individual files are restored to a different location to the original file (i.e. the later version of the file), unless that file is known to be corrupt, or is no longer present on the system. The files owner can then compare the backed-up file with the original of the file, before a decision is made to replace the newer file with the restored copy.

#### **13.2.5 Procedure for testing backup and restoration**

The backup and restore process are tested on a quarterly basis to ensure that they can be relied upon (ISO A.12.3.1). This involves testing the restore process against one example of the daily backup media, and one example of the weekly backup media stored in the safety deposit box (ISO A.12.3.1).

The NCEPOD main database, plus randomly selected files and folders from different areas are selected to test the restoration process. These files are then restored to a single location (NOT the original folders) and tested to ensure that they are intact. The testing process is logged, and any issues/errors addressed accordingly.

NCEPOD regards quarterly testing as adequate, due to the fact that backups are not used beyond the recommended time period given the manufacturer of the media. Backups are also held according to the environmental conditions specified by the manufacturer to ensure their good condition.

#### **13.3 Incident reporting (ISO A.16.1.2 & A.12.4.1)**

A log of all IT related errors and problems is maintained by the IT Manager, recording what happened, what was done and the final resolution.

This log is reviewed at the quarterly Information Security Forum meetings, to ensure that satisfactory action has been taken with regard to each incident (ISO A.12.4.1). It will also enable the network support staff to identify if there are long term, ongoing problems related to particular pieces of equipment, and to formulate more appropriate responses.

As part of the review, any corrective measures are audited to ensure that no action has been taken that has a negative impact on the security of the system involved, or on any systems/processes connected with that system (ISO A.16.1.1 & A.16.1.6).

#### **13.4 Media disposal (ISO A.10.7.2 & ISO A.10.7.3)**

All removable media are securely destroyed, as under section 6.8.2 of this document (ISO A.10.7.2).

The disposal of all removable media on-site is authorised by the Chief Executive and overseen & logged by the IT Manager (ISO A.8.3.1). An audit trail of all removable media destroyed in this way is kept by the IT Manager (ISO A.8.3.1 & ISO A.8.3.2).

The data on the media is first securely destroyed, then held securely pending destruction (Sections 6.8.2 & 13.6) (ISO A.8.3.2). The physical destruction of the media is carried out by arrangement with a legitimate company specialising in secure destruction of computer media (ISO A.8.3.2). Media is also defined by NCEPOD to include one-time-use printer ribbons, carbon paper, optical storage media and fax films.

### 13.5 Information handling procedures

Guidelines on the handling of information, in various formats and of various security classifications, are fully given in Appendix B.

### 13.6 Destruction of electronic data

All electronic data is retained (and archived/destroyed) in accordance with the data retention guidelines in Appendix E. This process is repeated quarterly by all staff members, who will archive/delete information according to the categorisation of the data, and the schedule of retention given in Appendix E.

Further to the archival/destruction of data by individual staff members, the formal, destruction of project data will be used to ensure complete destruction is achieved (by securely wiping the data).

After publication of a report all patient/clinician/hospital identifiable data relevant to that report held in an electronic format is securely deleted from the computer system. This includes all correspondence with clinicians directly related to individual case questionnaires, but not general information regarding the development and the running of the study, which may prove useful for future studies. Aggregated, non-identifiable data will similarly be retained for later use (but only after all patient/clinical/hospital identifiable coding has been removed).

This process is initiated and overseen by the Chief Executive. All staff are required to review their home folders for relevant correspondence to delete. The individual staff members will delete the correspondence – any material they are in doubt about is to be drawn to the attention of the Chief Executive, who will decide if it falls within the criteria for deletion.

All staff are required to delete identifiable emails relating to individual cases for the project from their mailboxes. Ambiguous emails will be brought to the attention of the Chief Executive, as above.

The IT Manager will remove all identifiable information from the project data in the NCEPOD database, retaining the aggregated, non-identifiable data for later use. No clinician, hospital or patient identifiable information is retained as part of the aggregated data, and no coding is left in to enable the process to be reversed in any manner or form. The Chief Executive will review the results of the aggregation to ensure the process has been carried out satisfactorily. All other information relating to the project held in the database will then be deleted.

Once all relevant information/correspondence has been removed from the server, and from the database and mailboxes, the IT Manager will complete the secure destruction of the deleted data. IT Manager will compact the Access database, to remove the empty space left over from deleting the data, which would contain traces of the deleted data. The email database (Exchange database) will similarly be compacted by the IT Manager. A full backup of the database, emails and home will then be made, before Active Disk software is used to securely overwrite all of the blank space on the server's disks (so that no recoverable residue of the deleted data is left). The software is configured to wipe the disks completely and overwrite the disk (to a military standard).

All of this process is logged by the IT Manager, including dates for the initial deletion of the information, the compacting of the relevant databases, and the secure overwriting of the free disk space. This information to be held indefinitely.

### 13.7 General housekeeping

Staff members are encouraged to practice good housekeeping with regard to the NCEPOD network's resources.

Staff members will regularly review the files held on the NCEPOD server as part of NCEPOD's data retention & archiving guidelines (Appendix E). Files no longer necessary are archived / deleted according to the retention guidelines. Archiving is achieved by moving the files to a pre-prepared (and protected) set of archive folder on the server.

Any files not covered by the guidelines (i.e. non project or business related) which may be useful for occasional reference but are not needed for the fulfilment of the staff member's day to day responsibilities, should also be archived.

Reasonable upper storage limits may be set and enforced on each of the home folders, at the discretion of the IT Manager, to maintain the amount of data contained on the system at a level appropriate, and practical, for ensuring all data can be backed up.

It is the responsibility of the IT Manager to ensure that the authorised folder structure on the NCEPOD file structure remains secure and up to date.

Staff members will similarly review emails held within the email folders provided for them on a quarterly basis. As disk space is quickly eaten into by the number of emails stored in an individual's mailbox, each staff member should show discretion when storing emails not related to the pursuit of their job functions within NCEPOD.

The IT Manager reserves the right to set upper limits on the size of mailboxes, and to enforce these limits accordingly. These storage limits are to be clearly indicated to the users.

Outlook provides the facility for archiving emails that are no longer needed for reference on a day to day basis but remain an important part of the documentation of the functioning of NCEPOD. The IT Manager can provide advice on the use of this feature if/when necessary.

The user of each workstation (the asset owner) is responsible for checking the Temp folder (created by default during installation of Windows) on their own Workstation on a weekly basis. Temporary files that the system has not automatically deleted after use (see below) should be deleted. The Temp folders will be checked on a quarterly basis by the IT Manager to ensure compliance.

While these files should be automatically removed by the application that created them, or the operating system, this does not always work. An example would be opening an attachment to an email - a temporary file might be created by the relevant application (e.g. Word) and stored in the Temp folder until the document is closed again. Word should automatically remove the temporary copy it stored in the Temp folder, but sometimes this does not happen, and the file is left in the folder. It is therefore important to check regularly to ensure that there are no such documents left in the Temp folder.

The Temp folder for each machine will be found either at the first level of the C: drive (C:\TEMP) or in the system root folder (C:\WINDOWS\Temp), depending upon the installation of the operating system.

Subfolders of the Temp folder should also be checked for files, but the folders should not be deleted (as they may have been created for the use of specific applications).

Some of the files in the Temp folder will be current (in use by the system) so you should order the files by date, then delete only files prior to today's date. This should ensure that you are not

attempting to remove files that may be in use. If while deleting a particular file you get an error or warning message (such as “Cannot delete, file in use”) seek advice from the IT Manager.

## **14 Data validation**

### **14.1 Objective**

To maintain confidence in data accuracy for use in decision making by using validation procedures to ensure accuracy of the data used by NCEPOD as the basis of analysis for each year's report. To maintain confidence in data accuracy for the processing of financial information, business-related information, and any other data when taken in the overall context of information processing within any sphere of NCEPOD's activity.

### **14.2 Data input validation**

While the majority of data processing that occurs within NCEPOD will relate to studies being undertaken, data throughout this section refers to any data/information that is being processed in any sphere of activity within NCEPOD (project data, financial data, business data etc.). The data handled by NCEPOD, in whatever capacity, is to be handled in a manner that protects its accuracy, reliability, and validity. Procedures specifically relating to the NCEPOD study database will be indicated explicitly.

Data accuracy is the direct responsibility of the person inputting the data, supported by their line manager. Within the NCEPOD study database, this is supported by validation processes put in place by the IT Manager (see below). Outside of the study database, the relevant line manager will provide support for staff appropriate to the processes involved.

The IT Manager will ensure that the NCEPOD study database incorporates validation processes at data input to check acceptability of key data. Such validation will include checks to detect, and thereby prevent, the following errors at the data input stage:

- a. out of range values
- b. invalid characters/invalid data types within data fields
- c. missing or incomplete data
- d. unauthorised or inconsistent control data

The NCEPOD study database will report all errors together with a helpful reason for the rejection to facilitate correction.

Error correction should be done at the source of input as soon as it is detected, and in accordance with defined reporting/correction procedures.

If considered appropriate, data may be inspected periodically to confirm the validity and integrity of the data, and the plausibility of the input data. This may involve random sampling of data against the original data source (on paper, or as originally supplied electronically).

Any suspected loss or corruption of data should be reported to the IT Manager (study database) or relevant line manager (other data) as soon as the suspicion arises. The IT Manager/line manager will then initiate an investigation into the source of the loss or corruption, involving other relevant staff as and when necessary.

Serious data validation errors (that have affected a whole range of data) along with suspected loss or corruption of data (for any other manner) will be treated as a security incidents, as they may well impact on the integrity of the data (Section 12).

### **14.3 Control of internal processing**

Data that has been correctly entered can become corrupted by processing errors, user mistakes (overwriting the data) or deliberate acts.

#### **14.3.1 Internal validation procedures and documentation**

Validation procedures are therefore not only enforced at the input stage (14.2) but throughout the life cycle of the data. The NCEPOD system, where appropriate, incorporates internal validation processes and audit trails to detect and record problems with processing and data integrity.

Validation processes are incorporated in the NCEPOD study database by the IT Manager and are reviewed/updated as and when necessary. They are specific to the format and content of the data set held for each project. They are fully documented as part of each project's data processing documentation.

This documentation, created by the IT Manager in conjunction with the Project Manager, includes the specifications for each database table required for the project, the validation rules built into each table, and any higher-level validation processes required, including sample of the coding involved (see Section 14.3.2). It also details the order in which the processes are run/or are triggered (if automatic), within the context of the whole flow of data for the project (from receipt of the data, through validation, sampling, and generation of questionnaires (if appropriate) to final data-cleaning before analysis.

While the majority of the above documentation will be in place before the data collection for the project is initiated (as part of the project planning process) further stages/validation may need to be added as the project develops. All such extra validation is documented and added to the main body of the project documentation by the Project Manager and/or IT Manager.

The design of data handling processes for specific business purposes/projects ensures that restrictions are in place to minimise, as much as is practical, the risk of processing failures, or of processing data in an incorrect order, which could lead to a loss of integrity.

Checks and controls that are considered for each data/data handling procedures within a project include:

- a. Session or batch controls, to reconcile actual results with expected results. Includes random sampling for verification of data on system against copy of data (paper based or electronic) as originally supplied
- b. Validation of system generated data
- c. Checks/procedures to ensure that application programs/processes are run at the correct time for the procedure involved
- d. Checks/procedures to ensure that application programs/processes are run in the correct order for the procedure involved

#### **14.3.2 High-level data manipulation and validation**

The use of high-level data manipulation functions within the database is strictly controlled.

Only designated support staff (IT Manager and support personnel) are authorised to add such code/procedures to the database. Restrictions on which staff may then run these processes are set in place (using staff member's access rights to objects within the database). Permission to run them is controlled strictly in accordance with an individual's roles and responsibilities (ISO A.6.1.1).

Explicit description of each higher-level validation procedure is to be documented as part of the overall project data processing documentation. This documentation may reside within the code/database itself, as long as a reference is included in the data process documentation of the project involved. The specification will include:

- What the validation does (including primary purpose)
- Why it is necessary to run the validation
- When it is to be run
- Who is authorised to run it
- At what point in the data processing timeline it is to occur
- Any procedures that have to be run before or after it is run
- Provision of fully annotated code for the procedure
- Any necessary roll back procedures for undoing the results of the validation, in the event of an error (including whether or not to freeze activity on the database until rectified)

#### **14.3.3 Reporting of processing errors and suspected errors**

Any suspected errors in the processing of the data, or as a result of erroneous processing of data, are to be reported immediately to the IT Manager.

Any loss or corruption of data is to be reported to the IT Manager immediately.

Procedures for handling failures within the database application, and for ensuring that such failures and the steps taken to recover from them has not compromised the integrity of the data, are documented in Section 14.5.

#### **14.4 Data output validation**

Procedures are in place to prevent the presentation of data, for internal or external use, which has not been passed as clean (i.e. fully validated and logically consistent). Such checks are integral to the work of NCEPOD, enabling NCEPOD to have confidence in the data that each published report is based on.

While most of the data validation checks happen during data input and internal processing (Sections 14.2 & 14.3), procedures are in place to ‘sanity check’ the resultant data.

For project data (held within the NCEPOD study database), these procedures are the responsibility of the IT Manager in conjunction with the data asset owner. The IT Manager is responsible for implementing any specific mechanisms required by the data asset owner (if possible, within the constraints of Access).

These checks are performed by the IT Manager and data asset owner and occur at appropriate stages throughout each project. The nature of the checks will vary depending upon the format and content of the particular project’s data set, and any background reference data publicly available to use as control data (for plausibility checks). They may also include a random sampling of cases for testing of the data within the database with the data as originally supplied (whether on paper or electronically).

Plausibility checks are checks designed to test that the data is both logically consistent and reasonable in the context within which it has been collected/for which it is to be used. An example would be comparing numbers of specific procedures reported to NCEPOD, along with death rates from those procedures, compared with the publicly available control information provided by the HES database for the same procedures.

Failure of sample data to meet any of these checks will result in a larger scale checking of the data held. Further analysis of the data and inputting/importing of the data effected will be put on hold until the issue of the validity of the data is resolved. This may include large-scale comparison exercises with the original data supplied, which may be carried out either by the IT Manager or the individual staff member responsible for the data involved, or both. This is at the discretion of the Chief Executive.

All checks to be undertaken, along with procedures for handling data that has failed output validation, are documented within each project's documentation, by the IT Manager in consultation with the Chief Executive.

The format/content of output data may need to provide sufficient information for a reader to determine the accuracy, completeness, precision and classification of the information. Where this is the case, NCEPOD will endeavour to provide this contextual information.

#### **14.4.1 Data usage validation (case reviewer meetings and report drafts)**

Any implausible data discovered by/with the aid of the Advisors used by NCEPOD to help analyse project information for the report is to be addressed by the Chief Executive, if necessary, with the input of the IT Manager.

Any issues of implausibility raised by the clinical co-ordinators during the drafting of the report will be addressed by the Chief Executive, if necessary, with the input of the IT Manager. This includes issues with data analysis provided by the IT Manager and issues raised when draft chapters are reviewed by the other co-ordinators.

All serious issues will be brought to the attention of the Chief Executive.

#### **14.5 Handling of database errors**

If the suspected error or corruption is within the NCEPOD study database, it should be reported immediately to the IT Manager (Sections 14.2 & 14.3) as well as the appropriate line manager (where appropriate).

The IT Manager will immediately advise all current staff to log out of the database, to allow unhindered investigation, and prevent propagation of existing errors (if present). The IT Manager will then check the suspected error/corruption to confirm if it is an actual corruption or error. If it is, then the Database Administrator will attempt to find out the cause, and if there is any action that can be done to recover from the situation.

If the suspected error turns out not to be actual, the suspected breach will still be logged (as below). Staff can then be allowed back into the database.

If the error is small-scale, and it can be recovered by amending individual records, or deleting and re-entering/re-importing the information, then the IT Manager will proceed accordingly.

If it is not a small-scale error, or is not recoverable in any other way, then the IT Manager will restore the database, but into a different folder than the existing database. The restored database will then be checked to ensure that the same error/corruption is not present. If it is not, then the corrupted database will be moved and the restored one put in its place. An attempt will be made to identify any information that can be re-entered/re-imported to bring the restored database back into line

with the corrupted database (by comparing, if possible, the contents of the corrupt database with the newly restored database).

If the restored database shows the same errors/corruption as the current database, it may be necessary to restore earlier backups until the source of the corruption is removed.

All steps taken to identify and resolve the problem are fully documented and entered into the error logs kept for review at each Information Security Forum quarterly meeting.

## **15 Software protection (ISO A.12.5.1)**

### **15.1 Objective**

To comply with the law on licensed products and minimise risk of computer viruses and malicious code through education, good practice/procedures and anti-virus software.

The NCEPOD software policy is designed -

1. To ensure that NCEPOD complies with the law on licensed products by controlling the installation and use of all software on the NCEPOD network.
2. To provide a policy that will minimise the risks of virus infection and the introduction of malicious code into the NCEPOD network. Strict controls over software installation and usage, when combined with full implementation of up-to-date anti-virus software and the NCEPOD email and Internet protocols, provides the most effective way of protecting the network.

### **15.2 Licensed software (ISO A.12.5.1 & ISO A.18.1.2)**

The IT Manager is responsible for ensuring that only licensed copies of commercial software are installed on the NCEPOD system (ISO A.12.5.1). It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action (ISO A.18.1.2).

Authorised network support staff are the only individuals mandated to install software onto the NCEPOD network. As such they are responsible for ensuring that all software installed is

- a. a licensed copy (ISO A.18.1.2)
- b. installed in accordance with the manufacturer's instructions and licensing restrictions (ISO A.18.1.2)

The IT Manager is responsible for maintaining an inventory of all software owned by NCEPOD and installed on the network (ISO A.18.1.2). The information in this inventory includes all relevant Product IDs, license and registration/serial numbers, and dates of purchase.

The IT Manager is responsible for maintaining proof of ownership of licensed products (including licenses, licensed media, and copies of invoices and evidence of payment) (ISO A.18.1.2).

The IT Manager is responsible for ensuring that the maximum number of permitted users (concurrent or numeric) for each product is not exceeded (ISO A.18.1.2). The IT Manager is also responsible for ensuring that no other licensing conditions for any product are breached (ISO A.18.1.2).

It is expressly forbidden to remove from the NCEPOD premises any CDs, disks or other installation media that are the property of NCEPOD, for the purpose of installing illegal copies of the software or making illegal copies of the media.

Any software that is disposed of, transferred or donated in any way must be done in a legal manner, in a way that does not breach terms of the license (ISO A.18.1.2). An audit trail of any transferred software must be kept by NCEPOD. All relevant licensing documentation must be passed to the party the software has been transferred to. This party must agree (in writing) to retain all necessary licenses and documentation before the transfer can be authorised.

If necessary, automated auditing may be considered to control software use (ISO A.18.3.1). At the moment, however, all audits are manual.

### **15.3.1 Software standards (ISO A.12.5.1)**

Only authorised network support staff are mandated to install software on the NCEPOD system (as above in Section 15.2).

No other staff member is allowed to install software of any kind to the network under any circumstance. This includes full software applications, games, screensavers, utilities, patches, on-line updates to licensed software, and any other executable code.

The installation of any software or executable code to the network without the permission of the IT Manager will render the staff member liable to disciplinary action.

Only software listed in the official inventory should be present on each workstation. The installation of unauthorised software by individual staff members is a disciplinary matter and is referred to the Chief Executive by the IT Manager.

Six-monthly checks of all computers owned by NCEPOD and connected to the network are conducted (ISO A.11.2.4 & ISO A.12.7.1). This audit is performed either by the IT Manager or delegated to authorised network support staff. The result of the audit is documented and then presented at the next Information Security Meeting.

If a breach of procedures has occurred, it is handled as a security incident (Section 12.4).

The date of the inspection is updated on the Asset Register, in the appropriate column, at the time of inspection.

### **15.3.2 Authorisation for software purchase & software installation**

If a member of staff considers it necessary for the legitimate pursuit of their roles and responsibilities within NCEPOD that they need access to a new piece of software, they should approach the IT Manager with this requirement. The IT Manager, if authorised to proceed by the Chief Executive, will obtain costings for purchasing the software, or for purchasing a license to install an existing piece of software to the new machine. The final decision as to whether the purchase is made rests with the Chief Executive. In this way, no unlicensed software is installed onto the NCEPOD network.

Patches and upgrades to existing licensed software may only be undertaken by the IT Manager and authorised network support staff. This includes both upgrades downloaded for later implementation and instant on-line updates. All such patches regarded as necessary must be applied as soon as practicable.

No games, screensavers or any other software unrelated to the business purposes of NCEPOD is installed on the network under any circumstances. There are numerous examples of software utilities and screensavers (especially those downloadable from the Internet) hiding Trojan horse programs and malicious code. To minimise the exposure of the NCEPOD network to these risks, no software in any form that does not contribute to the functioning of NCEPOD is installed.

## **15.4 Anti-virus controls (ISO A.12.2.1)**

### **15.4.1 Objective**

To minimise the risk of computer viruses and malicious code through education, good practice/procedures and anti-virus software.

Reliance is placed on users remaining vigilant, adhering strictly to the procedures outlined in this section, and reporting all incidents and suspected incidents immediately to the appropriate network staff.

Includes procedures relating the automatic and user-based aspects of the anti-virus software, covering transmission of files via the network, email, and the Internet. Places emphasis on the human aspect of any virus protection policy.

#### **15.4.2 Anti-virus education**

It is the responsibility of the IT Manager to provide adequate education about the ways in which a network can become infected with a virus (ISO A.7.2.2). This instruction takes place when each new member of staff joins NCEPOD. Specific attention is paid to the most common means of infection that a user would be vulnerable to during their day-to-day work (via email, the Internet and the use of removable media etc.).

This instruction includes an overview of the practices they must follow in order to reduce the threat of virus infection to the absolute minimum practicable. The IT Manager ensures that the staff member is aware of the relevant guidelines contained in this document, and that they appreciate the importance of abiding by them.

Such education will ensure that the user knows how to react to a virus incident on their workstation, both in the presence and in the absence of an available network support staff.

#### **15.4.3 Virus prevention**

It is the responsibility of the IT Manager to ensure that there is a coherent and integrated anti-virus strategy (ISO A.12.2.1).

This strategy involves all of the different strands of protection recommended by the IT support company. These include Webroot for servers, EST (latest version) and Norton Symantec (latest version) for desktop PCs and Microsoft threat protection ATP Plan 1 for email scanning. This software is updated on a daily basis to ensure the optimum level of protection (ISO A.12.2.1). The updating is automatically carried using the scheduling functionality of the software. The updates are set to occur on an hourly basis for all server anti-virus software. Clients are updated from the server immediately the next time they are connected to the network and switched on, before the user logs on to the network. If a user is logged on when the update is received, the computer is patched immediately.

Documentation relating to this strategy, including configuration decisions made and implemented, is maintained by the IT Manager, and reviewed regularly in the light of the threats from constantly evolving virus technology.

All configuration of anti-virus software is controlled from the server. Clients do not have access to disable or alter the settings of the anti-virus software.

Configuration of the anti-virus client software is controlled from the server when logged in as administrator. This ensures that it is not possible for unauthorised staff to disable the client or alter the configuration from the client computer.

In accordance with the policy on licensing and software standards, no unauthorised user is allowed to install any software, or run any unauthorised executable code, on any computer within the

NCEPOD network. This will dramatically reduce the opportunity for malicious code to infiltrate the NCEPOD network (ISO A.12.2.1 & A.13.1.1).

The IT Manager and appropriate network support staff should ensure, as far as is practical, that they are aware of emerging threats (new viruses and vulnerabilities) (ISO A.12.2.1). This may involve periodic checks of leading (trusted) anti-virus sites assess current threats, and the taking of any action necessary to protect against those threats. This is over and above ensuring that the software remains up to date (with the latest information files installed). It may also involve subscribing to trusted anti-virus alert services to enable the automatic receipt of alerts via email.

The IT Manager must be aware of, and use, trusted sources to gain specific information on specific viruses, as and when necessary, and to enable the separation of hoax alerts from real threats (ISO A.12.2.1)

Procedures to minimise the risk of email-borne infections are dealt with in section 17.3 of this document.

#### **15.4.4 Virus detection**

NCEPOD is protected from viruses on CD/DVDs, USB sticks and other removable media by the automatic scanning capabilities of up-to-date antivirus software. This intercepts requests to open files on any media (removable, hard drive or network drive) and scans them for viruses before allowing them to be opened or run. The software quarantines files it cannot disinfect and alerts the user to the situation. Staff should report virus incidents to the authorised network support staff.

As the on-access component of the software is the first line of protection, its configuration must never be altered or in any way interfered with by unauthorised personnel.

All anti-virus Software used at NCEPOD have the tamper protection enabled.

#### **15.4.5 Incident reporting**

Users should report any viruses detected/suspected on their machines immediately to the IT Manager (ISO A.12.2.1)

In the absence of the IT Manager the staff member should immediately notify a member of the network support staff. The IT Manager and/or network support staff will then take appropriate action.

#### **15.4.6 Virus removal**

Any machine that is suspected of being infected is disconnected immediately from the network. The machine will not be reconnected to the network until the IT Manager can verify that the virus has been removed (ISO A.12.2.1).

#### **15.4.7 Recovery from a network wide virus incident**

All virus incidents shall be handled as security incidents. Following a network-wide virus incident, the IT Manager will make full use of data backups, the Asset Register, and any necessary documentation to restore the network to working order, with the data restored (as near as possible) to its state before the incident (if it had been compromised) (ISO A.12.3.1). See also Sections 8, 13.2 & 16 of this document.

## **16 Business continuity planning (ISO A.17)**

### **16.1 Objective**

To be able to restore computer facilities and information to allow NCEPOD to continue essential activities following a major failure or disaster. To allow NCEPOD to deal quickly and effectively with such disasters, with minimum disruption to business goals.

### **16.2 Need for an effective plan**

NCEPOD recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its work. These plans arise out of the formal planning process documented in 16.3.1 and are included in Appendix D of this document. The Information Security Forum is responsible, supported by the owners of each individual plan (see Appendix D), is responsible for ensuring that all the elements for these plans are in place, and that they are regularly tested and maintained.

Because of NCEPOD's limited size and resources, it is not possible for NCEPOD to maintain standby equipment or offices. A mainstay of all business continuity plans is therefore that all essential processing equipment be insured (for replacement if lost) and on an IT maintenance contract (on a repair/replace basis, for replacement due to faults/failure).

### **16.3 Planning for business continuity (ISO A.17.1.1 – ISO A.17.1.2)**

#### **16.3.1 Planning framework and individual business continuity plans (ISO A.17.1.1 – ISO A.17.1.2)**

The business continuity framework seeks to cater for escalating levels of disruption to the functioning of NCEPOD – from minor incidents (e.g. loss of individual workstation), through loss of a key part of the system (e.g. database), to complete loss of processing power and/or processing facilities (e.g. devastating fire). For each scenario, NCEPOD has a fully documented set of procedures, which can be found in Appendix D of this document. These individual plans, in their totality, make up the NCEPOD Business Continuity Plan.

While each individual plan therefore fits into the NCEPOD Business Continuity Plan at a certain level, they are all based on a consistent approach to business continuity. Each individual plan follows the same pattern, and includes the same elements:

- a. Precautions that must already be in place to prevent/minimise the impact of the event on other sensitive systems/processes
- b. The conditions for activating the plans giving the process to be followed (ISO A.17.1.1)
- c. Emergency procedures covering *immediate* actions to be taken in response to an incident (ISO A.17.1.1)
- d. Steps to be taken to resolve the event that triggered the plan, including an escalation procedure for handling the event, with a timescale for bringing in outside support (if appropriate) and invoking fall-back procedures (below).
- e. Fall-back procedures describing the actions to be taken to allow NCEPOD to continue in the face of an unresolved event, including any contingency plans necessary (or practical) for NCEPOD to continue functioning effectively. May include provision of contingency devices defined in the disaster recovery plan (ISO A.17.1.2)
- f. Resumption procedures describing the actions to be taken to return to full normal service (ISO A.17.1.2)
- g. A maintenance schedule which specifies how and when the plan is tested, and the process for maintaining the plan (ISO A.17.1.2) – see Section 16.3.2 below.

- h. Any necessary educational issues, to ensure all staff involved are aware of the procedures and their responsibilities (ISO A.17.1.2)

Each plan has a specific owner, who is responsible for the relevant business process involved and its continuity. Individual responsibilities for specific steps within the plan (where different from the plan owner) are also fully documented. (ISO A.17.1.2 & A.17.1.3).

### **16.3.2 Testing and maintaining business continuity plans (ISO A.17.1.3)**

Business continuity plans are tested according to the schedule laid out within each individual recovery plan. A timetable documenting, at a glance, which plan is to be tested when is given at the start of Appendix D and is maintained by the IT Manager. In this way, NCEPOD attempts to ensure that all plans are both effective and practical. Such tests will also ensure that all members of the recovery team and other relevant staff are aware of the procedures and their part in them. (ISO A.17.1.3)

The testing process involves –

- a. Simulations of the scenarios, if practicable (ISO A.17.1.3).
- b. Complete rehearsals (testing that the organisation, personnel, equipment, facilities and processes can cope with the interruptions) if practicable (ISO A.17.1.3).
- c. Technical recovery testing (ISO A.17.1.3).
- d. Debriefing of parties involved in the plan (discussion to identify if any of the steps in the procedure need to be altered, or if any of the risks involved have altered (ISO A.17.1.3).
- e. Documented evidence of the success of the testing, or (if failure) of changes to plan implemented to resolve the failure. Any changed procedures to be re-tested immediately, until success achieved.

## **16.4 Review of business continuity plans**

### **16.4.1 Annual review**

NCEPOD reviews all plans for disaster recovery on an annual basis. This review includes:

- a. a review of existing disaster recovery plans
- b. a review of new factors/new equipment, leading to the inclusion of new plans to the existing body of plans.
- c. a review of the impact analysis documentation

The review will take place in accordance with the process outlined in section 16.4.3 below.

### **16.4.2 Ad hoc review**

Any significant change to the situation of NCEPOD (change in location, change in processing equipment etc.) will prompt an immediate review of business continuity plans. An initial assessment (documented) is made to decide if any of the plans are affected by the change.

This initial assessment is triggered in the following circumstances –

- a. Changes in personnel (ISO A. 17.1.3)
- b. Changes in operational addresses or telephone numbers (ISO A. 17.1.3)
- c. Changes in business practices, strategy or goals (ISO A. 17.1.3)
- d. Changes to location of the business (ISO A. 17.1.3)

- e. Changes in legislation (ISO A. 17.1.3)
- f. Changes in contractors, suppliers or support companies (ISO A. 17.1.3)
- g. Changes to information processing facilities or processes (ISO A. 17.1.3)
- h. Changes in identifiable risks (ISO A. 17.1.3)
- i. Failure of plan undergoing scheduled testing (as under Section 16.3.2)

All business continuity plans identified as being affected by the change will undergo a full review, as outlined in Section 16.4.3.

#### **16.4.3 Elements of the review**

The main elements of each review (annual or ad hoc) are:

- a. Identification of critical systems (existing and new) (ISO A. 17.1.1)
- b. Identification of areas of greatest vulnerability based on risk assessment (ISO A. 17.1.1)
- c. Review of the impact of failure in each system
- d. Mitigation of risks by developing resilience
- e. Consideration on the purchase of suitable insurance which may form part of the business continuity strategy (ISO A. 17.1.1)
- f. Review of documentation and testing of disaster recovery plans - identifying tasks, agreeing responsibilities and defining priorities (ISO A. 17.1.3)
- g. Ensuring that the management of business continuity is incorporated in the NCEPOD's processes and structures (ISO A. 17.1.2).
- h. All plans are developed to restore business operations within specified time scales following interruptions to critical business processes (ISO A. 17.1.2).

To enable full communication of disaster continuity plans regarding specific assets, the review (and initial planning process) is carried out with full involvement from the owner of the business resource and process being investigated. (ISO A. 17.1.1)

## **17 Accessing the Internet**

### **17.1 Objective**

To reduce the risk of security breaches by providing a secured means of access to the Internet. To ensure appropriate standards of behaviour are adhered to and prohibited material is not downloaded onto the NCEPOD network.

Covers use of an open connection to the Internet from anywhere within the NCEPOD network.

### **17.2 Security procedures**

#### **17.2.1 General statement**

NCEPOD provides Internet access for business purposes. You may use it in performing your assigned job duties. Inappropriate use of the Internet access provided by NCEPOD may result in disciplinary action being taken. NCEPOD reserves the right to monitor Internet usage patterns, in terms of time spent online and websites viewed, to ensure that no contravention of the NCEPOD Internet policy takes place. Logs of Internet usage may be archived for future reference or destroyed at the discretion of the Trustees.

#### **17.2.2 Access control**

Internet access is restricted to full time staff members and Clinical Co-ordinators. Use of the Internet by unauthorised, temporary staff is not permitted unless authorised by the Chief Executive, IT Manager, or a Clinical Researcher who may disclose a temporary password.

NCEPOD reserves the right to monitor Internet usage to ensure that official NCEPOD policy is not contravened or abused.

All Internet access must pass through the authorised, protected gateway. Attempts to circumvent access controls by use of personal modems attached to workstations are treated as a disciplinary offence.

Access control software is installed to prevent users from connecting to sites with prohibited content. NCEPOD is aware that access control software, no matter how efficient, will never be able to filter prohibited sites 100% effectively. It is therefore the responsibility of the individual not to actively pursue links, or search for content, which would lead to the viewing of prohibited content.

No staff member, with the exception of the designated network support staff, will for any reason attempt to alter the configuration of the access control software. To do so could significantly reduce the security of the NCEPOD network and would be viewed as a disciplinary matter.

No staff member, with the exception of the designated network support staff, may attempt to disable or interrupt the necessary functioning of the access control software. Attempting to remove, circumvent, or disable the software in any way will render the staff member subject to disciplinary proceedings. Network support staff may themselves only disable or interrupt the necessary functioning of the software under carefully controlled conditions, and for legitimate, authorised reasons.

The Chief Executive reserves the right to revoke access privileges for individual staff members.

### **17.2.3 Internet usage**

The Internet, where authorisation has been given, may be used for purposes relating to the functions and interests of NCEPOD. This would include (but is not limited to) the viewing of NHS, clinical, and health-related websites.

The Internet access granted by NCEPOD must not be used to view or actively pursue prohibited or offensive material, as detailed below (Prohibited content).

Users may not use the Internet connection provided to sign up for or utilise anonymous emailing or browsing facilities.

Users may use the Internet connection to access legitimate web-based email accounts. A legitimate account is one set up by the individual under their own name, using accurate and truthful information. While such an account is not directly under the control of NCEPOD, use of the Internet connection provided by NCEPOD to access the account is. As such, complaints against an individual arising from their use of a personal web email account on NCEPOD time, using the NCEPOD connection, is dealt with as a disciplinary offence in exactly the same way as if the email originated from within the NCEPOD network.

Personal usage of the Internet is subject to the same limits of reasonable usage as the telephone.

### **17.2.4 Prohibited content**

The Internet connection provided by NCEPOD may not be used to view material that is illegal or offensive.

It is not practical for NCEPOD to provide detailed information regarding the legality of particular types of content on the Internet. Common sense should be applied when using the Internet to avoid material that the staff member knows to be, or suspects to be, illegal.

It is similarly not practical for NCEPOD to provide a comprehensive list of material deemed to be offensive. Such a list would include, but not be limited to, material that is pornographic in nature, or that is racially, religiously or ethnically offensive and/or discriminatory in any way.

Common sense should be used at all times when using the Internet connection provided by NCEPOD. All usage can be traced back to the NCEPOD network, and you should consider this while you are using the connection. No usage should be made of the Internet that has the potential to harm NCEPOD, or the reputation of NCEPOD.

NCEPOD is aware that the accidental loading of web pages with prohibited content can and does occur in the course of legitimate Internet usage. This may happen by the accidental mistyping of Internet addresses (URLs), or as the unexpected results of searches on innocuous sounding key words. It is the responsibility of the individual staff member to leave such sites immediately.

If sites whose names or addresses suggest that they contain prohibited material are noticed in the logs, time spent at the site is taken into account when deciding if the staff member has contravened the NCEPOD policy on prohibited matter. Occasional, accidental contact with such sites is treated accordingly – i.e. as accidents. Repeated or sustained connections to web sites with prohibited content are dealt with as disciplinary offences.

#### **17.2.5.1 Downloading files: software and executable code**

Under no circumstances may any member of staff download and install any software or other executable code from the Internet, with the exception of the designated network support staff (see below). This includes any shareware, freeware, screensavers, or trial versions of recognised software. If any member of staff feels that there is a benefit in downloading a specific piece of software, they must consult the IT Manager.

If the IT Manager agrees that the software is necessary or helpful for the carrying out of the staff members' roles and responsibilities, and that it comes from a reputable source, then they will authorise the downloading of the software. This is done on the staff member's behalf by the designated network support staff. The software or code is checked before installation by the authorised network support staff, if it is within their capability to do so. The IT Manager and/or network support staff, in line with NCEPOD regulations, will perform all such installations.

There are very few circumstances where executable code will need to be downloaded and installed. All such installations are restricted to software and executable code only where it furthers the legitimate interests of NCEPOD. No software for personal usage may be installed on the network under any circumstance.

#### **17.2.5.2 Downloading files: static documents**

Full time staff members and Clinical Co-ordinators may download static documents (defined below) as and when necessary. Such documents will have been automatically scanned by NCEPOD's anti-virus software as they are downloaded (and will again be automatically scanned when they are opened) so there is no need for the user to manually scan them.

Static documents, consisting of non-executable code, include Word files, Excel files, Adobe Acrobat files and other common word processing, spreadsheet and presentation files. If you are at all unsure as to the nature of the file you are downloading, you must consult the network support staff before downloading the file.

Some static documents may contain small, self-contained pieces of executable code called macros. While most macros are benign, some are either malicious in their entirety, or can be used to hide malicious code routines. There are an expanding number of macro-based viruses that can be contained in otherwise harmless documents, and triggered to run automatically when the document is opened.

The anti-virus software is configured to scan for, and block, macros when documents are being downloaded, but like all such software, it is only as good as the latest update. Therefore, if after downloading a document and attempting to open it you receive a prompt stating "This document contains macros", you should immediately seek the advice of the network support staff. It may be that the macro is benign, but it could be that the macro contains virus code that is unrecognised by the anti-virus software.

### **17.3 Email protocols (ISO A.13.2.3)**

#### **17.3.1 Objective**

To ensure proper and responsible use of the NCEPOD internal and external email systems, safeguarding the integrity of the ncepod.org.uk domain name. To minimise the risk of email-borne viruses infections, and protect the network from email-borne Trojans and malicious code.

Covers all communications (emails and attachments) sent and received via the NCEPOD email system.

### **17.3.2 General statement (ISO A.13.2.1 & A.13.2.3)**

NCEPOD provides electronic mail for business communications, to be used in performing assigned job duties. Inappropriate use of email may result in disciplinary action being taken. Electronic mail may be monitored in transit or stored on disk by network personnel for later review. Email may be archived for future reference or destroyed at the discretion of management. The sending of emails with content liable to tarnish the reputation of NCEPOD is treated as a disciplinary matter.

Flagrant abuse of NCEPOD's email policy is treated as gross misconduct. The sending of offensive, abusive, threatening, discriminatory, inflammatory or libellous material is treated as gross misconduct. The sending of such material clearly tarnishes the reputation of NCEPOD, and in addition has the potential to fall within the definition of criminal conduct under current UK legislation, including (but not restricted to):

- section 43 of the Telecommunications Act 1984
- section 1 of the Malicious Communications Act 1988
- sections 4&5 of the Public Order Act 1986
- sections 1&2 of the Protection from Harassment Act 1997
- section 28 of the Crime and Disorder Act 1998 (racially aggravated offences)

Agreement to abide by the NCEPOD email policy forms part of the standard Terms and Conditions of the staff member's contract of employment. All staff, whether on a permanent or temporary contract, are bound by this policy.

### **17.3.3 Monitoring of email**

A distinction is to be made between the monitoring of the volume of email traffic, and the content of email traffic.

The volume of emails sent and received may be monitored on a day-to-day basis, with no extra authority needed over and above the initial nomination of the specified network support staff by the Chief Executive (as above). If necessary, the destination address of emails may be monitored in the same way, with the same implied authority.

NCEPOD reserves the right to monitor the content of email usage to ensure that official NCEPOD policy is not contravened or abused. Personnel with the authority to perform monitoring tasks are restricted to the Chief Executive only, who must notify the Chair in writing if they plan to access someone's email and the reason why this is being undertaken. All authorised staff are expected to handle the task of monitoring usage with integrity, confidentiality and discretion at all times.

No attempt may be made to monitor the content of emails unless specifically authorised by the Chair. Such authorisation is to be specific to each case, and may only be given if the Chair:

- a. has good reason to suspect, or has evidence of, misuse of the NCEPOD email system by a particular individual, or
- b. is pursuing a legitimate complaint, from inside or outside the organisation, relating to a specific individual's usage of the email system to send material that contravenes these guidelines.

In all circumstances where the content of a person's emails is being examined, that individual is notified, and will have all the same rights as guaranteed by the official NCEPOD disciplinary procedure regulations.

#### **17.3.4 Business usage of the NCEPOD email systems – ncepod.org.uk and nhs.net (ISO A13.2.1)**

All emails originating from within the ncepod.org.uk email system have a company disclaimer automatically attached. The text of the disclaimer is fixed, and no staff member is authorised to make any additions or amendments to this text, aside from the designated network support staff.

Emails are a notoriously insecure method for transmitting information. It should never be assumed that information sent via email is read only by the person for whom it is intended.

As such, users must not transmit confidential, personal or other sensitive information relating to NCEPOD via email without adequate precautions. No sensitive information may be sent in the body of the email – it must be sent as a password protected and/or encrypted attachment to the email using the nhs.net address, not the NCEPOD.org.uk domain. All usage of email to send sensitive information is at the discretion of the Chief Executive. See section 19.4 for detailed policy and procedures on use of email to send confidential information.

Emails should be filed in a logical manner in Outlook. Users should regularly go through and delete emails in their inbox and sent items. Critical Attachments should be stored on the file server not in an email inbox.

Emails are not guaranteed to reach the destination that they are intended for. If the content of the email is important, and requires a response, it may be wise to follow up the email with a phone call, or to send a copy of the information sent via email in the regular post.

Emails should be retained according to exactly the same principle that governs the retention of other electronic & paper-based information – if the email contains important information concerning any aspect of NCEPOD business, it should be retained for further use / reference.

In some circumstances shared email folders called (Public Folders) will be set up to allow many staff to access email to a common email address. In this case there needs to be a named manager who is responsible for procedures for checking the email and who has access to the shared email folder.

Emails may be printed, and the copy filed with related correspondence (e.g. in a local reporter file), but only if it is viewed important enough to do so. It is up to the individual receiving the email to decide when this is justified, but for the vast majority of emails, it is enough to retain the email in your mailbox / in a sub-folder within your mailbox.

Such emails (printed or in electronic format) form part of the business records of NCEPOD and must be treated as such (for legal and decision-making reasons). NCEPOD's rules governing the retention period for business information (Appendix E) apply equally to email messages.

Users must make sure that the appropriate authority has been obtained before transmitting any company information or advice. Where appropriate, hard copies of such emails must be retained, as they form part of the official record of correspondence with the other party involved.

If a user receives an email in error, they must inform the sender immediately and delete the message from their mailbox.

It is an offence to send emails containing offensive imagery or statements, as defined in the preceding General Statement. It is an offence to use the email system to send attachments containing offensive imagery or statements. The sending of such material will result in an

investigation of the alleged misconduct, and disciplinary action may be taken commensurate with scale of the misconduct.

The nhs.net email must never be used for personal email transmission, or any use other than transmitting data between NCEPOD and healthcare organisations.

### **17.3.5 Personal usage of the NCEPOD email system**

All emails that originate from within NCEPOD carry the ncepod.org.uk domain address and have the NCEPOD disclaimer attached. Care must therefore be taken that the content of any personal email does not diminish or harm NCEPOD's reputation in any way.

Personal communications originating from the NCEPOD email system are subject to the same conditions regarding content as for business communications (above).

Specifically, while the content of the email and the intended recipient may be unconnected with NCEPOD, the use of the NCEPOD email system to send personal communications containing offensive imagery or statements is still a disciplinary offence, being an action likely to tarnish the reputation of NCEPOD. The sending of such material will therefore result in an investigation of the alleged misconduct, and disciplinary action may be taken commensurate with scale of the misconduct.

Users may not use their NCEPOD email account to sign up to Internet news groups, or discussion groups, without first consulting the IT Manager. This is to minimise the number of unsolicited emails (spam) being received by the NCEPOD mail server. Internet News Groups are regularly scanned by companies to extract email addresses, which then become targets for persistent spamming. This in turn puts an unnecessary burden on the email system.

If in the opinion of the IT Manager the news group will prove to be a useful resource for the carrying out of the individual's role in NCEPOD, then the IT Manager will consult the Chief Executive before giving/withholding permission. Such permission may only come from the Chief Executive, and in all cases the judgement of the Chief Executive is final.

Users may not use their NCEPOD email account to sign up to automated mailing lists without first consulting the IT Manager. Automated mailing lists are generally more secure than open Internet news groups (entailing the provision of an email address to one specific company – for instance to enable the receipt of automated security alerts and patches released by one specific company, for one specific product)

If in the opinion of the IT Manager the mailing list is secure, and will prove to be a useful resource for the carrying out of the individual's role in NCEPOD, then the IT Manager may authorise subscription to the list without consulting the Chief Executive.

If the IT Manager views the subscription to the service as unlikely to further the interests of NCEPOD, or has doubts over the level of trust engendered by the company involved, the decision is referred to the Chief Executive. Again, in all such cases the judgement of the Chief Executive is final.

In each case, the company involved should have a privacy policy detailing the use to which they will put the users' data (including email address). If the company does not have a privacy policy, permission will not be given.

If a user receives an email in error, they must inform the sender immediately and delete the message from their mailbox.

Personal usage of the email system is subject to the same limit of reasonable usage as the telephone.

### **17.3.6 Unsolicited emails (ISO A.12.2.1)**

All unsolicited emails are to be treated with extreme caution (see also the Anti-Virus procedures in section 1.3.2). Email-borne viruses have now become the most prevalent means of infection and are most commonly triggered by the simple act of opening the email to read it.

Although the anti-virus information files are updated on an hourly basis, and all known instances of email viruses will therefore be quarantined automatically, users must remain vigilant to prevent the spread of new and unknown viruses. The procedures for dealing with unsolicited emails are simple. Action to be taken depends on the circumstances surrounding the particular email:

1. You do not recognise the sender, and the sender appears to be unrelated to any aspect of NCEPOD's business practices, or to belong to any organisation that you feel would have a legitimate reason for communicating with NCEPOD: **delete the email without opening it.**
2. You do not recognise the sender, and the subject line appears to be unrelated to any aspect of NCEPOD's business processes: **delete the email without opening it.**
3. You recognise the name of the sender, or the sender seems to belong to an organisation that would legitimately be communicating with NCEPOD, but you are suspicious of the subject line text: **do not open the email - contact the IT Manager immediately (or at the first possible opportunity).**

A discussion of possible reasons for being suspicious is given below Point 4.

4. If you are at all unsure as to the origin and purpose of an email: **do not open the email - contact the IT Manager immediately (or at the first possible opportunity).**

#### **17.3.6.1 Reasons to be suspicious (ISO A.12.2.1)**

The propagation mechanism for most email viruses involves emailing a copy of itself to every address in an infected machines address book. This means that often you will know the name of the person who is sending you the virus and would therefore not naturally be suspicious. This makes it doubly important to scan the text in the subject line for suspicious material before you open any email. While it is not always possible to detect the presence of an infected email from the subject line, there are several circumstances that should arouse your suspicion –

- a. If the subject line is blank, you should be suspicious.
- b. If the subject or the body of the email refers(via a link) to any Facebook, Instagram or social network account
- c. If the subject line seems vague in nature yet is couched in the language of a response to an unmade request (such as "here is that file you asked for", or "Re: the information you requested"), you should be suspicious.
- d. Similarly, the one of the most common hooks used by virus writers is an appeal to human curiosity, with subject lines following the pattern of “wow – you have to see this”, “check this out – you will not believe it!!!” etc. Such subject lines, combined with the fact that the email

often purports to come from someone the victim knows, explains (but does not excuse) why people still fall for such tricks.

- e. If the subject line is garbled, you should be suspicious. One of the easiest mechanisms to spot is the garbled or nonsensical subject line. This is caused by email viruses that capture random strings of text from the infected host's files. If the subject line doesn't make sense (or does make grammatical sense but doesn't make sense to you) then be suspicious.

#### **17.3.6.2 Reporting of suspicious emails (ISO A.12.2.1 & A.16.1.2)**

The reporting of emails with suspicious subject lines to the IT Manager is essential, as the subject text used by particular viruses is published as part of the service of most anti-virus sites. Network support staff are in a better position to check the text against known viruses than the individual user.

If for any reason you cannot contact a member of the network support staff immediately, you may continue to send and receive other items of mail *so long as you do not open the suspected email itself*. It is safe to do this as any potential virus within the email will remain dormant until triggered by user intervention - specifically, by the user opening the email in an attempt to read it.

**Remember:** These guidelines are an attempt to provide best practice advice on virus avoidance. As viruses become more technically sophisticated (as do the tricks used to get people to open them) there will inevitably be instances where viruses get through no matter how vigilant the individual user is. Do not feel therefore that if a virus enters the NCEPOD network through an email you have opened, it will necessarily be treated as a disciplinary matter. If it is clearly demonstrated that you were vigilant and did not contravene these guidelines, there is no blame to be attached.

#### **17.3.7 Attachments (ISO A.13.2.1)**

No executable attachments of any kind to be sent or received, with the exception of the two following circumstances –

1. Executable code can be sent and received by network support staff in the necessary pursuit of their role (for example, to receive software patches for specific problems from the manufacturer of an application).
2. Where NCEPOD related files (data from local reporters, for instance) are received by email in the form of self-extracting archive files. These are created by compression utilities and can be run by the recipient to allow decompression of the files without the need for the recipient to have the same software installed on their computer.

In both cases, the attachment itself is automatically stripped from the email as it passes through the email gateway. You will therefore have to request that the file be passed to you by the network support staff, who will ensure that the file is virus free before releasing it.

All file attachments that contain macros are routinely quarantined upon receipt at the email gateway, due to the threat of malicious code. There is a whole strain of virus development that utilises the coding facilities built into Microsoft products (particularly Office applications) to inflict malicious damage on a victim's system and/or network. During the course of a staff member's day to day activities, there are very few circumstances where the receipt of files containing macros would be necessary. If you are expecting such a file, inform the appropriate network support staff. They will then be able to retrieve the file from quarantine, test it, and pass it on to the intended recipient.

The file itself is passed to the staff member in a form depending on the criteria outlined below –

- a. If the macro is found to be both necessary and benign, the file is passed on to the recipient intact.
- b. If the macro is found to be benign but unnecessary, the macro is removed before the file is passed to the intended recipient.
- c. If the macro is found to contain malicious code, and the file is related to the legitimate interests of NCEPOD, the macro is removed, and the file itself is thoroughly tested for infection before being passed to the intended recipient. If the file cannot safely be disinfected, it is destroyed. In the meantime, the intended recipient should contact the sender of the document and inform them that their computer may be harbouring a virus.
- d. If the macro is found to contain malicious code, and the file is unrelated to the legitimate interests of NCEPOD, the whole file is destroyed. The intended recipient is informed so that they can notify the sender of the document.

It is possible that you may receive emails with embedded hypertext links (text or images that when selected cause your Internet browser to open a specific web page). You should treat such links with extreme caution. If you know that the email is from a legitimate source (for example in response to a request for information from an individual or a company) the link is probably safe.

However, you should be extremely wary of links contained in unsolicited emails, even if the email appears to come from a legitimate company. Fake emails with embedded links have been used to direct users to spoof websites. These are sites created to mirror the website of a known (trusted) company, carry all the necessary corporate branding, and to all intents and purposed look fully legitimate. Such sites have been used both for malicious activity (transmitting malicious code over the Internet connection) and for fraudulent activity (tricking the unwary into providing personal and financial information). Company websites known to have been spoofed in this way include Microsoft.

If you have any doubts about the validity of an email with a hypertext link or any social network account like Facebook, Instagram etc. you should seek advice from the IT Manager.

## **18 Data Protection**

### **18.1 Data Protection 2018 and the General Data Protection Regulation 2016**

The General Data Protection Regulation gives certain rights to individuals about whom information is held (manually or electronically). Individuals may ask for information about themselves, challenge it if appropriate, and in certain circumstances can claim compensation. The Regulation places obligations on those organisations or individuals who record and use personal data (data users). They must be open about that use by registering all systems containing personal data and must follow sound and proper practices.

The risk to the organisation of failing to comply with the Regulation is clear. Not only is there risk of criminal sanctions but also the risk of public embarrassment over failure to comply. It is also worth remembering that where an offence under the Act is committed by an organisation any employee is personally liable if the offence is attributable to neglect on their part.

The concept of data protection by design and default is central to the GDPR. This means that data protection should be included in studies from the beginning and in all policies and templates, not as an additional function. Studies are designed to only collect personal data that is absolutely necessary to be able to carry out the work. IT and physical security procedures are in place from the beginning of each study. Data to be collected and security measures are specified in the Study Protocol early in the study's development and this is used to obtain Section 251/PBPP approval to collect data without obtaining consent from patients. Any identifiable information must only be kept as long as it is needed. Patient details are anonymised within 2 months of being received and completely destroyed 3 months.

### **18.2 Subject Access**

All subject access requests should be referred to the Chief Executive. Responses will be made within 30 days of request.

### **18.3 Data Protection Impact Assessment**

A Data Protection Impact Assessment (DPIA) is available and should be updated at least twice a year for submission to HQIP. Any new data collections should be addressed in the DPIA.

## **19 Exchanges of information (ISO A.13.2)**

### **19.1 Objective**

To prevent loss, modification or misuse of information exchanged between organisations, whether in an electronic or paper format.

### **19.2 Information Exchange/Data Sharing Agreements (ISO A.13.2.2)**

NCEPOD will undertake to facilitate formal information exchange agreements, if required by any of the participating Trusts/organisations that contribute to NCEPOD. The content of any such agreement should consider the sensitivity of the material involved, and may also include consideration of any/all of the following, from the point of view of both parties to the agreement –

1. Management responsibilities for controlling and notifying transmission, despatch and receipt of the information (ISO A. 13.2.1)
2. Procedures for notifying sender, transmission, despatch and receipt (ISO A. 13.2.1)
3. Minimum technical standards for packaging and transmission (ISO A. 13.2.1)
4. Courier identification standards (ISO A. 13.2.1)
5. Responsibilities and liabilities in the event of loss of data (ISO A. 13.2.1)
6. Use of an agreed labelling system for sensitive or critical information (ISO A. 13.2.1)
7. Responsibilities (on both parties) for data protection, copyright compliance and similar legal or regulatory considerations (ISO A. 13.2.1)
8. Technical standards for recording and reading the information (ISO A. 13.2.1)
9. Any special controls that may be required to protect the information (ISO A. 13.2.1)

NCEPOD will attempt to meet any requirements of the other party to the agreement, where they are reasonable and practicable.

In the absence of any Information Exchange Agreement being requested by the third party, NCEPOD still provides advice and guidance to help individuals within the third party transmit data to NCEPOD in a secure manner.

This advice is included in the formal Guidelines for Local Reporters issued to the nominated reporter within each NHS Trust and Independent organisation that sends data to NCEPOD. It is also included (from time to time) within the NCEPOD Newsletter that goes out to local reporters and Medical Directors (or equivalent) of each organisation.

All business suppliers and support companies used by NCEPOD, whether they have a contract or not, is required to have signed a confidentiality agreement with NCEPOD (Section 9) which will cover all information needed for that supplier/company to provide the service contracted for.

NCEPOD does not use external companies to process sensitive data (i.e. no data is outsourced for processing). Were NCEPOD to use such third parties, that company would be required to sign an Information Exchange Agreement (as above) on top of the Confidentiality Agreement. This is to protect the data being processed, over and above the information about NCEPOD that the company may need to hold.

It is important to note, however, that some of the Information Exchange Agreements already signed by NCEPOD to allow transfer of project related data specifically prohibit the use of outsourcing/subcontracting to process the data provided.

### **19.3 Security of data/items in transit (ISO A.8.3.3)**

When sending sensitive or confidential information, a method of despatch should be chosen commensurate with the sensitivity of the information and the perceived risk. If necessary, registered post or couriers should be considered. (ISO A.8.3.3)

Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit. (ISO A.8.3.3)

### **19.4 Security of electronic mail (ISO A.13.2.3)**

Users must not transmit confidential, personal or other sensitive information relating to NCEPOD via email without appropriate controls. Emails are notoriously insecure. Email can very easily be sent to the wrong address, and once sent, is impossible to recall. It is also open to very simple interception methods (ISO A.13.2.3).

All sensitive or confidential information sent via email must therefore be in the form of a protected attachment to the email (see below) and sent via the NCEPOD nhs.net address connected to the Health and Social Care Network (HSCN). No sensitive material of any kind may be sent in the body of the email itself.

For organisations that have a formal Information Exchange Agreement with NCEPOD (18.2), the transmission of the information must take place according to the controls specified in the agreement. Note that it is possible for an agreement to prohibit the sending of confidential material by email at all (in favour of other means of exchange), or to require strong encryption.

For all other organisations (those that NCEPOD does not have a formal agreement with) all attachments containing sensitive information must be password protected. The provision of the password to the recipient of the email must be by phone. Under no circumstances should the password be sent via email.

The Chief Executive reserves the right, for any highly sensitive material, to require information to be sent via the regular (or registered) postal service.

In certain circumstances, highly sensitive or confidential information may need to be sent in the form of a self-decrypting file. Advice on achieving this level of security should be sought from the IT Manager.

NCEPOD undertakes to support all requests for secure flow of data both to and from the external organisations. In the absence of any formal agreement with an organisation, although the onus for securing incoming material is on the sender (the external organisation), NCEPOD encourages other organisations to send material in a password protected format wherever possible. Any sensitive information arriving not via the nhs.net or not password protected are placed on the breach notification spreadsheet and the sender notified.

Guidelines on the content, handling and retention of business emails are found in section 17.3 of this document.

Internal directories of email addresses are confidential and should not be disclosed.

Internal email addresses of staff are provided for business use, so may be disclosed according to the everyday necessity of business use (in much the same way as the public, NCEPOD phone number may be disclosed).

External email addresses of staff, co-ordinators, and other people related to NCEPOD are confidential, and must *not* be disclosed without the permission of the individual involved (in the same way that personal telephone numbers should not be disclosed without permission from the individual concerned).

Remote users may dial in for the purpose of picking up email from the NCEPOD mailbox provided for them (ISO A.11.7.2). Such usage is governed by the controls on remote users in general.

### **19.5 Security of electronic office systems (ISO A. 14.1.1)**

Electronic office systems and the interoperability and ease of data exchange between applications poses a risk that NCEPOD recognises and seeks to limit. A combination of secure operating system, secure (password protected) resources, and tightly controlled user access policy, is used to minimise the risks while retaining the benefits of the modern electronic office.

Areas that are looked at during the formulation/review of appropriate policy and controls include –

- a. policy and appropriate controls to manage information sharing (security on the NCEPOD Intranet and public folders) (ISO A. 14.1.1)
- b. excluding categories of sensitive information systems from areas that do not provide an appropriate level of protection (ISO A. 14.1.1)
- c. restricting of access to diary information and mailboxes on a user-by-user basis, with the exclusion of specific, shared calendars and mailboxes (ISO A. 14.1.1)
- d. categories of staff and external contractors allowed to use the system and the locations from which it may be accessed (ISO A. 14.1.1)
- e. restricting selected facilities to specific categories of user (ISO A. 14.1.1)
- f. retention and backup of information held on the system (as under disaster recovery plans) (ISO A. 14.1.1)
- g. fall-back and recovery arrangements (as under disaster recovery plans) (ISO A. 14.1.1)

### **19.6 Other forms of information exchange (ISO A.13.2.1)**

Staff members should be aware of the danger of being overheard when discussing confidential or sensitive information over the phone, at either end of the conversation, (particularly when there are visitors to the NCEPOD offices), and act accordingly.  
(ISO A.13.2.1)

Staff members should not have conversations involving confidential or sensitive information in public places or open areas outside of the NCEPOD offices, or where there are visitors within the NCEPOD offices (ISO A.13.2.1).

Staff members should not leave messages containing confidential information on answer phones, since these may be played by people other than the intended recipient, or may be left on a wrong or communal answer phone (ISO A.13.2.1)

Staff members should not send confidential information by fax, since the fax could easily be read by someone else apart from the intended recipient or could be faxed to an incorrect number. (ISO A.13.2.1)

## **19.7 Encryption**

Where appropriate, methods of encrypting data will be used to protect confidential information. This may be for transmission of data or for storing identifiable information and will be defined on a study-by-study basis. Encryption of data will be done using software like TrueCrypt, PGP software, or 7zip. Authorisation is further required from the Chief Executive for all media transmitted from NCEPOD. Transmission of any media is logged by the IT Manager (ISO A.12.4.1).

## **20 Network management (ISO A.9.1)**

### **20.1 Objective**

To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

### **20.2 Network controls (ISO A.9.1.2)**

A range of controls, covering a variety of areas, are needed to achieve and maintain an acceptable level of security in a networked environment. These controls are enumerated fully under Sections 20.3 (network access controls), 20.4 (operating system access controls), 20.5 (application access controls), and 21 (monitoring system access and use) of this document.

In general, though, NCEPOD aims to ensure that:

- Operational responsibility for networks is separated from computer operations where appropriate (ISO A.9.1.2, A)
- Responsibilities and procedures for the management of remote equipment are established (ISO A.9.1.1 & A 9.1.2)
- Special consideration is given to safeguarding the confidentiality and integrity of data passing over public networks (ISO A.9.1.1)
- Management activities are closely co-ordinated to optimise the service to the business and to ensure that controls are consistently applied across the information processing infrastructure. (ISO A.9.1.2)

The focus of these procedures is twofold.

1. To enable the NCEPOD network to function in a secure and reliable manner, with particular attention to its interconnections with the world outside. Failure to follow the procedures in this section would create the potential for abuse of the NCEPOD network (and the data contained within that network) by unauthorised individuals.
2. To prevent behaviour originating from within the NCEPOD network that is abusive, illegal, negligent, or would damage the reputation and functioning of NCEPOD, or lead to external investigation or prosecution.

### **20.3 Network access controls (ISO A.9.1)**

#### **20.3.1 Policy on use of network services (ISO A.9.1.2)**

Access to both internal and external networked services are controlled and monitored, to ensure that users who have access to networks and network services do not compromise the security and integrity of the network and the information held on the network by NCEPOD.

Wireless networks may not be attached to the NCEPOD domain under any circumstances. Virtual Private Networks (VPNs) may only be installed by the IT manager.

You must never use open Wi-Fi (on the train or airport etc.) to log on to the NCEPOD server via VPN, or to email copies of the report/data that you might be working on through any other email system.

For safer internet access when travelling you can setup your own hotspot using your mobile phone. Costs will be covered by NCEPOD.

The IT Manager is responsible for

- a. ensuring that adequate controls are in place to protect and regulate the use of any interface between the internal NCEPOD network and any external networks (ISO A.9.1.2)
- b. ensuring that there are appropriate authorisation procedures for determining who is allowed access to which networks and networked services, and that these are followed. See also Section 11.2.1.
- c. ensuring appropriate controls for user access to network and information systems are in place (ISO A.9.2 & ISO A.9.1.2). See also Section 11.2.2.

### **20.3.2 Location of sensitive information**

To ensure that all sensitive information held in digital format is stored in an appropriate, secure, environment, the IT Manager maintains a suitable, secure, folder structure on the NCEPOD file server.

All sensitive information held in digital format is to be stored within this secure environment.

Sensitive information includes (but is not limited to) all documents and information, stored in a digital format, containing patient identifiable, clinician identifiable, or hospital identifiable information. Any documents relating to the financial or other sensitive business aspects of NCEPOD, or in any way marked as confidential on the information asset register.

The security in place upon this folder structure allows staff members to store information in a secure and stable environment that is tailored to the particular data held and the business needs of NCEPOD.

By requiring all NCEPOD related information to be held within this folder structure, NCEPOD also ensures that all information that is necessary to the functioning of NCEPOD is included in the scheduled backup process that is an essential component of the disaster recovery procedures.

It is the responsibility of the IT Manager to ensure that the security in place on the folder structure, combined with the access privileges of the various classes of users within NCEPOD, provides a robustly secure environment. Access permissions for each folder are specifically tailored to providing secure access (or blocking access) based on the defined individuals and user groups. Access to any network resource is restricted solely to those who need access to carry out their assigned roles and responsibilities.

Special care is taken to remove all unnecessary default user groups that appear in system folders under a Windows operating system installation, and the default “Everyone” group that appears for all newly folders created.

Only the IT Manager and network staff have access rights to alter permissions and create new subfolders directly under the root folder. However, all other users have full rights to create, manipulate and delete sub-folders within their own home folder. These permissions do not extend to any folder outside of their own home folder, with the exception of appropriately secured communal folders.

It is the responsibility of the IT Manager to assess the need for changes to the root folder structure requested by other staff members. If such a request is legitimate, and will not compromise the underlying security considerations, the IT Manager will create the requested folder. Access

permissions is granted according to the purpose for which the folder was created.

Any changes in staffing are reflected by changes in the root folder structure.

The IT Manager can, if authorised by the Chief Executive, use cryptographic software and controls to provide designated users with the means to store sensitive information outside of the secured folder structure on the NCEPOD network (Sections 6.7 and 10.6).

Data may be stored outside of the NCEPOD folder structure for any reason determined as legitimate by the Chief Executive but must be authorised in writing. Legitimate reasons would include, but not be limited to, the protection of sensitive personal data relating to staff members. In such circumstances the data may be held on a machine other than the NCEPOD file server, but only if one of the two following conditions are met:

1. The data is held in a file that is individually protected by strong encryption. It is not sufficient to use the password-protection native to Microsoft Office applications – the file **MUST** be password protected as part of the strong encryption process.
2. The data is held within a volume on a disk that has been set up as an encrypted volume using the PGP Disk software utility provided by the IT Manager.

In either case, the IT Manager will provide access to these tools when authorised to do so by the Chief Executive. No other member of staff may under any circumstance attempt to install encryption software on any workstation.

Once the user of the computer has been instructed in the use of the encryption software, the responsibility for encrypting all sensitive data (as authorised by the Chief Executive), and hence for keeping it in a secure format, passes to the individual staff member.

In circumstances where the encrypted files are to reside on a machine that is not owned by NCEPOD (i.e. one of the Co-ordinators laptops), and the laptop user already has a preferred encryption solution resident on the laptop, the pre-existing software may be used. This will only be allowed if the IT Manager agrees that the alternative encryption solution is of sufficient quality, the final decision to involve the approval of the Chief Executive.

In a situation where the encryption utility proposed is of a lower standard than the PGP software, the IT Manager (in conjunction with the Chief Executive) reserves the right to refuse permission for sensitive information to be held on the laptop until such a time as the approved PGP software has been installed.

### **20.3.3 Enforced paths**

Access to resources within the NCEPOD network is controlled. Along with controls enumerated under other sections (e.g. restricted user access rights) this may include the use of enforced paths as and when appropriate.

Where appropriate, and practical, this may take the form of

- a. allocating dedicated lines or telephone numbers for remote users.
- b. automatically connecting ports to specified application systems or security gateways
- c. limiting menu and submenu options for individual users (for instance, using Active Directory Group Policies within Windows server (ISO A.9.2.5)
- d. preventing unlimited network roaming (ISO A.11.4.5)

- e. enforcing the use of specified application systems and/or security gateways for external network users (ISO A.13.1.3)
- f. actively controlling allowed source to destination communications via security gateways (e.g. forcing all Internet connections to go through the NCEPOD firewall). See also section 19.3.7 of this document.
- g. Using DMZ(Demilitarised Zone)

Where appropriate, these controls will be written into specific business procedures and processes. They will form part of the process.

#### **20.3.4 User authentication for external connections**

A suitable level of user authentication for remote access connections is enforced. Authentication is of the same level and strength as a standard internal logons.

Security of remote access connections is reviewed six monthly, specifically with a view to individual usage patterns of remote working that may indicate the need for an elevated level of protection in certain cases, and the options (cost/benefit) of strengthening such authentication processes.

#### **20.3.5 Node authentication ISO**

In addition to the presence of user authentication techniques (20.3), the possibility of node authentication as a means of strong protection may be considered. This would enable the NCEPOD network to check access both against the user credentials (the user logon account) and against the hardware used to make the connection (computer account) to ensure that the connection is originating from the expected computer (i.e. the user's laptop).

It is currently viewed as not necessary to enforce node authentication.

#### **20.3.6 Remote diagnostic port protection**

All remote diagnostic facilities pre-installed as part of the operating system are shut down. No connections/ports from any other diagnostic based software (e.g. LogmeIn) are left open unless they are in use for legitimate business purposes (below).

When such access is needed, for instance so that an IT support company can perform remote diagnostics, the port is opened under the direct supervision of the IT Manager. The IT Manager will monitor all access from the support company for the duration of the dial-in, and immediately shut down the port when the session has concluded.

The use of the dial in connection will be logged by the IT Manager, giving the time of start and finish, the reason for the connection, and any actions taken/files looked at by the support company.

#### **20.3.7 Network connection control**

All communications between the NCEPOD network and the outside world will go through the designated gateways (email, Internet, and remote user access). This ensures that appropriate controls can be implemented to govern access to, and use of, the facilities (if necessary/practical on a user-by-user basis). Also, that the activity can be monitored for security breaches.

All Internet traffic, including email, is filtered through a router (with Network Address Translation enabled) and a firewall (Cisco Meraki) between the network and router). The firewall is set to deny all incoming packets on all TCP/IP ports (by default) with the exception of port 25 (SMTP email) and port 80 (HTTP) for Internet connections (initiated from inside trusted network only). The firewall allows blocking of individual addresses, if necessary.

### **20.3.8 Security of network services**

Care is taken that any networked service running within NCEPOD that communicates with other networks/machines is adequately secured. As such services bridge the gap between the external world and the NCEPOD network, and could potentially be open to exploitation, steps are taken to secure them, and they are closely monitored.

All non-essential services are disabled or blocked. At present, the only services allowed a connection to outside networks are email (MS Exchange Server), the HTTPs service (allowing use of the Internet) and HTTPs service to access the NCEPOD Online Questionnaire service is isolated in the implemented DMZ. All other services are blocked at the firewall (Section 19.3.7).

The Exchange server is set up to refuse requests to relay email (to prevent it being used as a spam relay) and runs inside the protection of the NCEPOD firewall. It is configured to log both standard and unusual email events (including attempts to relay) to the Server Event logging service.

This log is reviewed on a weekly basis (as part of the standard IT housekeeping routine) in an attempt to identify any suspicious activity/breaches. Attempts to pass malicious code (viruses) into the NCEPOD is protected against by use of anti-virus (MS Exchange based anti-virus software) – see Section 15 for further details.

Connections to the Internet are only allowed if initiated from within the NCEPOD network. Anti-virus software is used to scan all Internet traffic and block malicious scripts/code from being executed or downloaded during the Internet session. See Section 15.4 for further details.

## **20.4 Operating system access control (ISO A.9.4)**

### **20.4.1 Objective**

To prevent unauthorised access to computer resources that could enable the compromising of the networked operating systems within the NCEPOD network. To enable full logging of system events to provide an audit trail for any attempt (successful or unsuccessful) to compromise system stability and integrity.

### **20.4.2 Automatic terminal identification**

Each computer on the network has a unique computer ID that is recorded as part of the logon procedure, along with the credentials of the logon account used. In this way each logon can be tracked back both to a unique user account, and to the equipment that person used to log on with.

### **20.4.3 Terminal log on procedures (ISO A.9.4.2)**

The NCEPOD network provides access within a secure environment, which can only be reached by successfully completing a network logon process. This process is in itself designed to be secure, and to disclose the minimum of information about the system needed to log on.

The NCEPOD log on procedure conforms to best practice under ISO 27001:2013 in that it:

- a. does not display system or application identifiers until the logon process has been successfully completed (ISO A.9.4.2)
- b. displays a general notice warning that the computer should only be accessed by unauthorised users (ISO A. 9.4.2)

- c. does not provide help messages of any kind during logon that would help an unauthorised user (ISO A. 9.4.2)
- d. validates the log on information only on completion of all input data. When a logon failure occurs, the system does not identify which part of the credentials is incorrect (ISO A. 9.4.2)
- e. limits the number of unsuccessful logon attempts (ISO A. 9.4.2) to five before locking the account (for a set period) so that no further log on attempts can be made until the period has timed out or been reset by a member of the network support staff.  
The network also logs all unsuccessful (and successful) logon attempts for later audit.

#### **20.4.4.1 User identification and authentication (ISO A.9.2.1)**

The NCEPOD network employs a combination of unique user identification and authentication to restrict an individual's access to those systems and information required by their job function only.

All access to the system is based on this system of unique user identification, to enable fine control of access rights and proper auditing. Under exceptional circumstances, where there is a clear business benefit and no negative impact upon the security of the network, the use of a shared user logon may be authorised. Such authorisation will only be given for single, specific tasks, usually time limited and project based, and the group account access rights is tightly controlled and bound to this specific task.

The IT Manager is responsible for maintaining the system of user identification and authentication.

The Chief Executive will notify the IT Manager when a new user is to be registered. The Chief Executive will inform the IT Manager of the new staff members roles and responsibilities, and any necessary access privileges are granted as a result of that discussion (see under 4.6.19.4.4.2.)

#### **20.4.4.2 Privilege control management (ISO A.9.2.3)**

Access privileges are granted according to the requirements of the individual's job.

Most privileges are assigned as standard, in line with a user's job title and assigned roles and responsibilities (administrative assistant, network support staff, database support staff, clinical co-ordinator etc.). These privileges are assigned by the IT Manager according to the pre-specified user categories.

Privileges above and beyond these standard privileges may be implemented as a result of discussion with the Chief Executive, reflecting unusual fine-tuning of access privileges to fulfil specific roles. The privileges must be documented by the IT Manager, and the authorisation must be explicit, not implied.

Changes in access privileges that flow from a clearly defined change in the role of an individual, in accordance with the pre-set categories (for example from administrative assistant to database support staff) may be made without formal consultation with the Chief Executive. Authorisation for such changes is implied by the Chief Executive's prior involvement in the change in job title/description.

Any alterations in access privileges resulting from changes to job title, job description or responsibilities that fall outside the scope of these standard roles must have explicit authorisation from the Chief Executive.

When a permanent member of staff leaves NCEPOD, the IT Manager disables the corresponding user account immediately. The staff member is deemed to have had enough time to remove any

personal files (letters, emails etc.) from the server. Their home folders and mailbox will be checked by the CEO or the IT Manager, and any files and emails relating to NCEPOD are retained (personal files and emails being deleted). The staff member's folder will be retained, until the files within have all been deleted/archived according to the standard data retention guidelines (Appendix E).

The mailbox will similarly be kept, but the address will be used to re-direct fresh emails to another, appropriate member of staff (which may be the replacement for the leaver). The user account may be deleted only *after* the mailbox has been assigned to another user account (i.e. as the primary account for that mailbox). Deletion of the user account without reassigning the mailbox would result in the deletion of the mailbox, and NCEPOD could lose valuable emails & information.

When a temporary member of staff leaves NCEPOD, the procedure depends upon how their user account was set up. If an individual, new user account was set up specific to that person, that procedure is the same as for when a permanent staff member leaves. If they have home folders and a mailbox, these is scanned for content that should be retained (if any), then deleted. If the temporary member of staff was using the standard temporary staff member account (created for temporary staff with low access privileges) then the account will simply be disabled. If they have home folders and a mailbox, these is scanned for content that should be retained (if any), then deleted.

To ensure that all relevant steps are taken, a leaver's checklist is circulated by the Chief Executive prior to the staff member leaving. This checklist includes actions that have to be taken before, at the time of leaving, and after the staff member has left. While all the entries are not security related, all the steps that are involved for ensuring no breach of security takes place during/as a result of the staff member going are listed. The checklist is returned to the Chief Executive upon completion of all the tasks. This document is retained.

If a member of staff has been suspended for any disciplinary matter, their user account is disabled immediately. Such an account will not be deleted until the disciplinary matter has been resolved. If the user is re-instated, the account is unfrozen on the authority of the Chief Executive. If the user is dismissed, their user account is deleted after their home folders (on the network) and mailbox had been checked for NCEPOD related information (with all relevant information/emails kept, as above). Such information that is necessary to NCEPOD is retained. Files that are clearly personal are forwarded to the individual. Everything else is deleted from the server.

#### **20.4.4.3 Privilege review (ISO A.9.2.5)**

Staff member's access rights annually reviewed by the Information Security Forum. Ad hoc review, as part of the process of any change in role / job description, may also take place (ISO A. 9.2.5).

Temporarily elevated access rights (e.g. for special, time limited project working) are removed upon completion of the project (ISO A. 9.2.5).

Privilege allocations are checked at quarterly to ensure that no unauthorised privileges have been obtained (ISO A. 9.2.5).

#### **20.4.5 Password management system (ISO A.9.2.3)**

A strong policy for password management is enforced within the NCEPOD network.

##### **20.4.5.1 User password management (ISO A.9.2.3)**

The use of individual passwords to maintain accountability is paramount. (ISO A.9.2.3) No individual is given access to the system until they are properly trained and aware of their security and confidentiality responsibilities.

Where appropriate, users are responsible for selecting their own passwords, and for following the relevant guidelines to select strong passwords (ISO A.9.2.3 & A.9.3.1). These guidelines are found in section 11.4.4 of this document. The importance of following those guidelines to the letter cannot be over-emphasised when it comes to the setting of passwords on higher level user account (i.e. administrator accounts). Breaches of these accounts pose the greatest threat, as the increased access rights magnify the damage that could be done over the network.

It is the responsibility of the IT Manager to ensure that new staff members are aware of the reasons for operating in a secure environment and have accordingly read the required sections of this document. Once the IT Manager is satisfied that the staff member has received sufficient training, it becomes the responsibility of the individual staff member to continue to act in a responsible manner, following all necessary guidelines.

Staff members are required to change passwords every three months (ISO A.9.3.1). The IT Manager is responsible for providing an appropriate mechanism for enforcing this change, utilising either the functions built into the operating system to enforce the change or providing a suitable alternative method (depending upon the circumstances/practicalities) for each group of users.

Where users are granted a temporary password, they are required to change it to one they have selected themselves at the first logon (ISO A.9.3.1). This action is the default behaviour of the system (of Windows 2012 Active Directory) so is enforced automatically.

The NCEPOD system is set up to maintain a record of each users 12 previous account passwords, against which new passwords can be tested to ensure that staff members are not simply alternating between passwords (ISO A.9.3.1). This is configured using the Windows 2012 domain security policy and is fully automated (no user intervention required).

The NCEPOD logon procedure does not display password on the screen in clear text, either for the network or database logons (ISO A.9.4.3).

Password files (encrypted) are stored separately from application system data, and so are logically separate by default (ISO A.9.4.2).

Passwords are stored in encrypted form (ISO A.9.4.2). The logon procedure within Windows 10 itself uses hashed algorithms derived from the password, rather than the password itself, to compare and authenticate logons. This ensures a high level of security during logon.

Default vendor passwords for all installations of software are changed as soon as the installation is complete (ISO A.9.4.3).

Passwords must never be disclosed to another individual.

There are no circumstances under which the password for an administrative account should be disclosed to any staff member, not even to another member of the network support staff. Provision of the password for one administrator account to another network administrator would never be necessary, as no increased access rights would be conferred. All that would be achieved is that the audit trail of network events would be compromised, as one individual could now log in as another staff member and perform actions untraceable back to that individual.

#### **20.4.5.2 System and service account password management**

It is necessary for the correct functioning of the NCEPOD network and information processing facilities to have several automated service accounts present within the network. Such accounts only have the level of privilege assigned necessary to ensure that the automated functions they govern can occur.

As with all Windows 2012 Server installations, the NCEPOD server runs certain services as local accounts (called service accounts). These service accounts are like other user accounts, in that they have a user name (the account name) and a password. Some of these service accounts necessarily have higher-level access privileges in order for them to carry out the process for which they are used.

For instance, the Altaro Virtualization Backup software runs using a backup service account. In order to gain access to all of the user and system files that the backup is configured for, it necessarily has to have access rights that override the user-level security set up by the IT Manager.

As a consequence of this, it is just as important to protect these service accounts from being breached as to protect the administrator accounts assigned to individual staff members. However, there are three major differences in the way that the passwords for these accounts are handled:

1. Rather than being advice for best practice, it is mandatory that these passwords are strings of non-dictionary alpha characters combined with numbers and/or other non-alpha characters. This is made practical by the other two differences below.
2. As some service accounts are used to perform system tasks at certain scheduled intervals, the process is often started by one piece of software (responsible for the scheduling) logging on using a system account to run the task. This requires the password for the account to be stored in the scheduling software, to enable an automated logon with no user intervention. This being the case, there are no problems associated with human failure to remember complex strings of alpha and non-alpha characters.
3. Also, as the maintenance of service accounts fall under the remit of the network support staff, and there is no guarantee that both are present for each change of passwords, all passwords for these accounts are logged. This log details all service accounts and passwords and is kept securely in the fireproof cabinet. A copy of the latest (current) account details and passwords is taken to the bank with the monthly off-site backup media. Password change is synchronised with the schedule for backup to aid this process.

#### **20.4.5.3 Management of other passwords**

For passwords other than user account passwords, it may be acceptable to keep a record of the password. Such circumstances are rare and are limited to situations where the password does not tie into the Windows 10 security model (and hence cannot be over-ridden by the network support staff) and is known only to one person. In these instances the recorded password must be kept in a sealed envelope in a secured cabinet or safe.

Situations where this is permissible would include, but are not limited to, the securing of sensitive information by strong encryption software.

If the information protected by any form of encryption is vital to the continuing functioning of NCEPOD, then the recording of the password and its secure storage becomes a requirement. In the event of the user's unavailability, for whatever reason, there must be a way in which the essential information can be recovered.

#### **20.4.6 User of system utilities (ISO A.9.4.4)**

Whenever possible, restrictions are put in place to prevent the unauthorised use of system and network utilities that are capable of compromising the integrity and security of the NCEPOD network. Access controls are utilised to ensure that only necessary individuals (network support staff) can gain access to, and utilise, such utilities.

While it is not always possible to remove Operating System based utilities from machines (where they are not an optional part of an OS installation), it may be possible to prevent unauthorised users from running them by setting the correct permissions level on the machine. Where this is the case, it is done.

Third party utilities are restricted by installation only on specific machines (used by administrators only).

A combination of methods is therefore used to remove access to such utilities, to minimise the dangers caused by the presence of such utilities:

- a. Where possible, authentication procedures are used to govern access to system utilities (ISO A.9.4.4). Only staff with the appropriate access levels (see Appendix C) shall have access to keys, codes or system passwords required to access system utilities.
- b. Segregation of system utilities from application software is achieved by limiting installation of utilities to specific machines (ISO A.13.1.13). Media for utilities to be securely held, to eliminate possibility of unauthorised installation.
- c. Limitation of the use of system utilities to the minimum practical number of authorised, trusted users (ISO A.9.4.4), as defined in Appendix C.
- d. Authorisation for ad hoc use of system utilities (ISO A.11.5.4) to be given to the appropriate network support staff by the IT Manager
- e. Limitation of the availability of system utilities, where practical, to the duration of an authorised action (ISO A.9.4.2) – i.e. they are removed/uninstalled after use.
- f. Logging of all uses of such system utilities, as part of the logging process for network events (ISO A.9.1.2)
- g. Defining and documenting of authorisation levels for system utilities (ISO A.9.4.4)
- h. Removal of all unnecessary software-based utilities and system software (ISO A.9.4.4)

#### **20.4.7 Terminal time out (ISO A.9.4.2)**

Unattended terminals on the network (including computers logged on over a remote access link) should never be left in an open state. As specified elsewhere, all unattended terminals should be locked (if the operating system allows this) or the session should be logged off completely.

Password protected screensavers are not used, as staff must lock all unattended Workstations (allowing all network connections and work in progress (application sessions) to remain open while the computer is locked) or completely log off for the duration (closes all open connections).

#### **20.4.8 Limitation of connection time (ISO A.9.4.2)**

To restrict the opportunity for breaches of the NCEPOD network, all user accounts have set hours when they can be used to log on to the network.

The hours involved will vary with the job functions of the staff member but are based around the premise that (for most staff) access will only be needed during the working week (Monday to Friday)

and within reasonable office hours (7am to 5:30pm, allowing for flexi-time). Remote users have extended log on hours (weekends and evenings) to allow for out-of-hours working patterns.

Attempts by a user to log on outside of permitted hours is rejected by the NCEPOD server. Connections remaining open at the expiry of permitted hours are terminated by the server. Users get a warning that their permitted hours are about to expire, so that they can save their work and log off safely.

Remote connections are timed out after 15 minutes of inactivity (set universally as a property of the modem used to answer RAS connections).

Requests for extended/alternative working hours are judged on a case-by-case basis, with the final decision at the discretion of the Chief Executive.

Permitted log on hours for each individual are recorded by the IT Manager and checked on a 6-monthly basis.

## **20.5 Application access control (ISO A.9.4)**

### **20.5.1 Objectives**

To control user access to information and application system functions, in accordance with the NCEPOD access control and user privilege procedures (ISO A.9.4)

To provide protection from unauthorised access for any application that is capable of overriding network, system or application controls (ISO A.9.4.4)

To ensure that no application is used in a way that could compromise the security of the NCEPOD system, or of applications and data within the NCEPOD system (ISO A.9.1.1)

To restrict access to information, through controls on application use, to authorised individuals and user groups (ISO A.9.4.1)

To restrict the use of application software to users / groups of users who are authorised to access, and have a business need to access, the application in question.

### **20.5.2 Information access restriction (ISO A.9.4.1)**

Where necessary (and possible) users of application systems are only provided with access to functions within applications, and to information accessible through applications, in accordance with their job functions, and their access rights (ISO A.9.4.1).

For instance, controls are in place within the NCEPOD database that allow for the provision of different access rights to the data for different users, in accordance with the nature of their work, and the sensitivity of the data held. Also, to restrict the running of higher-level application functions to the database administrators group (ISO A.9.4.1).

Sensitive system documentation that could provide information on restricted functions to users who have no need to use those functions is considered sensitive information and marked accordingly on the Asset Register. Such information is therefore subject to the same handling procedures as other sensitive information (Appendix B) and is therefore stored securely. (ISO A.9.4.1)

Access rights to information accessible through applications, where that information is stored within the secure folder structure of the NCEPOD network, are controlled through the security integral to the folder structure itself, rather than the application. (ISO A.9.4.1)

If data is to be provided to a third party, then that information must contain only what they need, they must be authorised to have that information, and it must be transmitted to them in a secure manner (ISO A.13.2.1). The Information Security Forum reserves the right to carry out periodic spot checks on any data sent out from NCEPOD to satisfy itself that procedures are being followed.

Data movements within NCEPOD are governed by the same principles. All information passed to coordinators and case reviewers comprise only what they need, and only in a format in which they are authorised to see it (i.e. anonymised, non-identifiable data). See Section 7.3.

Where information is generated by an application for output (e.g. printing), care must be taken to ensure that the information is secure at the point of output (ISO A.8.2.3). Once printed, the printout must be removed from the printer immediately, so there is no danger of it being forgotten and left unsecured.

### **20.5.3 Protection of software configuration**

Certain applications (e.g. anti-virus software with tamper protection) give the option to have their configuration pages password protected. Whenever this is the case, password protection is utilised. Procedures relating to the handling of passwords for these applications follow exactly those practices detailed under Section 20.4.5.2.

### **20.5.4 Sensitive system isolation**

A review is made of each new application or service that processes sensitive information, and of the information being processed. If it is decided that the sensitivity of the information processed is sufficiently high that it needs to be run in isolation from other information processing tasks, then the application, and the information it is handling, will be hosted on a dedicated machine so that it is not sharing resources with other processes.

To this end the review will identify and document the sensitivity of the data, the feasibility of the data and application being hosted in an isolated computing environment, the impact on the overall functioning of the business, and the final decision as to whether it will actually be isolated.

The owner of each system (and/or of the information being processed) is consulted as part of the process (ISO A.8.1.2). Once the system/information has been assessed for sensitivity/criticality, and has been documented in the information asset register, it is the responsibility of the asset's owner to bring to the attention of the Information Security Forum any change in the type of data (criticality/sensitivity) being processed by that asset.

### **20.5.5 Database controls**

Suitable controls are maintained on the database used by NCEPOD. These controls are the responsibility of the IT Manager.

Controls are enforced that allow each user of the database to have a uniquely identifiable User Account, to which suitable privilege levels are attached. Data within the database is classified according to who should or should not have access, and the user privileges granted reflect this accordingly.

## **21 Monitoring system access and use (ISO A.12.4)**

### **21.1 Objective**

To detect, and record, unauthorised access to the network, and unauthorised use of applications and / or access to information within the network. To provide a suitable audit trail for investigation of security incidents.

### **21.2 Event logging**

Audit logs are retained to assist access control monitoring. The logs are archived on a regular basis to prevent event log overflows.

System audit logs are set up to record:

- a. user IDs (ISO A.12.4.1)
- b. dates and times of logons and logoffs (ISO A.12.4.1)
- c. the ID of the machine where the logon event is originating (ISO A.12.4.1)
- d. the success or failure of each logon event (ISO A.21.4.1)
- e. where possible, attempts to access other resources and information on the network (ISO A.12.4.1)

### **21.3 Monitoring of system use (ISO A.12.4.1)**

#### **21.3.1 Procedures and areas of risk (ISO A.12.4.1)**

The Information Security Forum undertakes an annual review of the monitoring and auditing of information processing facilities. This meeting does not concern itself with the results of the monitoring/auditing (which is reviewed as a matter of course at each quarterly meeting) but with the *level* of auditing being undertaken. All processes currently being monitored are audited for the appropriateness of monitoring, and for the level of monitoring (too stringent, not stringent enough etc.).

For each process, four areas are considered for monitoring, one or more of which may be considered appropriate. A suitable level and method of monitoring is then adopted as the basis of monitoring.

The four areas considered are:

- a. Monitoring of authorised access (success or failure) including information on user ID, date and time of access, type of access, the files accessed, the programs / utilities used (if possible). (ISO A.12.4.1)
- b. Monitoring of the running of a privileged operation, such as use of administrative account, system shut down and re-start, I/O device attachment/detachment (ISO A.12.4.3)
- c. Monitoring of unauthorised access attempts (success or failure) such as failed attempts, access policy violations (ISO A.12.4.1)
- d. Monitoring of system alerts or failures such as console alert messages, system log exceptions, network management alarms (ISO A.12.4.1)

A decision as to the applicability of each area for monitoring against each process is made, along with the extent of the monitoring employed within each area (if employed). This is then documented accordingly at the end of the review and forms the basis of the monitoring schedule & procedures over the next year (i.e. until the next annual review).

The documentation specifies explicitly which of the four methods will be used, and what information will be monitored (i.e. what markers are to be used to identify breaches of security). It also specifies the person to be responsible for the monitoring, and the frequency of the monitoring.

### **21.3.2 Risk factors (ISO A.12.4.1)**

The frequency of monitoring for each activity/process depends upon the risk factors involved. The annual review of monitoring/auditing that is carried out by the Information Security Forum (under Section 21.3.1 above) is used to decide this frequency.

The frequency will depend upon:

- a. the criticality of the application process (ISO A.14.1.1)
- b. the value, sensitivity or criticality of the information involved (ISO A.14.1.1)
- c. the past experience of system infiltration and misuse (ISO A.16.1)
- d. the extent of system interconnection (with public networks) (ISO A.13.1.1)

The results of the monitoring are reviewed at each quarterly Information Security Meetings.

### **21.4 Logging and reviewing events (ISO A.12.4.1)**

All automatically generated system logs are reviewed and archived weekly, to identify any actual/suspected breaches to security. A record of any actual/suspected breaches is kept, and appropriate action taken based on the incident.

Use of the system log viewer is restricted to authorised network support staff. Controls are in place to prevent:

- a. the logging facility being de-activated (ISO A.12.4.2 & A.12.4.3)
- b. alterations being made to list of system events that are recorded (ISO A. 12.4.2 & A.12.4.3)
- c. editing or deletion of the log files (by using the access controls within Windows to block unauthorised access to the folders containing the files) (ISO A. 12.4.2 & A.12.4.3)
- d. log overflows, causing the logs to stop recording new events (ISO A. 12.4.2 & A.12.4.3).

### **21.5 Clock synchronisation (ISO A.12.4.4)**

To ensure the accuracy of audit logs, the internal clock of each computer logging onto the network is synchronised with the server clock at logon.

The server clock is checked monthly, and adjusted as necessary, by the IT Manager.

## **22 Security of system files (ISO A.12.5)**

### **22.1 Objectives**

To ensure that the NCEPOD network is not compromised by unauthorised access to system files. To ensure the integrity of the functioning and integrity of the system and data.

### **22.2 Control of operational software (ISO A.12.5.1)**

Installation of new operational software (applications and utilities), along with the upgrading of existing software, is only performed by the authorised network support staff. No other member of staff may install any software or executable code under any circumstances (see section 4.6.15.3).

Authorised installation of is tightly controlled -

- a. the updating or installation of software is only performed by the authorised network support staff, and only upon appropriate management authorisation (ISO A.12.5.1)
- b. where possible, operational systems only hold executable code (ISO A.12.5.1). All data is held only within the designated NCEPOD folder structure on the server, allowing operational re-installations (or installation of new software) on the client machines to progress without the worry of having to backup / restore data.
- c. where possible, executable code is not implemented on an operational system until evidence of successful testing and user acceptance is obtained (ISO A.12.5.1)
- d. an audit log is maintained of all updates to operational machines (ISO A.12.5.1)
- e. previous versions of software are retained as a contingency measure (ISO A.12.5.1). All such media is stored securely, in NCEPOD's fireproof filing cabinet.

All software is maintained in compliance with the manufacturer's advice and specifications. All necessary upgrades and patches released by the manufacturer are applied, in accordance with any instructions given.

### **22.3 Protection of system test data (ISO A.14.3.1)**

Where the testing of an information processing facility is required, neutral test data is used wherever possible (i.e. data that is invented, but that fits the structure and requirements of the data for which the process is used).

Where this is not possible, and actual live data is to be used to test the new processes/facilities, the following controls are used –

- a. the same access control procedures that would apply to a fully operational process/the data contained within the process are matched by the test facilities (ISO A.14.3.1). The physical equipment used to test the new facility is either inside the NCEPOD network (if appropriate) or set up to match the security on the NCEPOD network (if outside/isolated from the existing network).
- b. there should be separate authorisation each time operational information is copied, if the test environment is outside of the existing (operational) NCEPOD network (ISO A.14.3.1)
- c. all test data is erased from the test environment immediately a specific test (or round of testing) is complete (ISO A.14.3.1)
- d. the copying and use of test data is logged to provide an audit trail (ISO A.14.3.1)

## **22.4 Access control to program source library**

In order to reduce the potential for corruption of computer programs, control is maintained over application source libraries.

- a. Program source libraries are protected from network users as much as practical by using access control procedures for sensitive folders
- b. IT support staff will not have unrestricted access to program source libraries, where possible (ISO A.9.4.5)
- c. Programs under development should not be commingled with operational program source libraries wherever possible (ISO A.9.4.5). This is to be accomplished by utilising separate operational and development environments where possible.
- d. The updating of program source libraries (through upgrades or any other method) is only performed by the authorised network support staff (ISO A.9.4.5). An audit log is maintained of all updates to program source libraries (patches etc.).
- e. Old versions of source programs (i.e. old media) are archived within the fireproof filing cabinet (where appropriate, and until stability of the new program has been tested over a satisfactory period of usage (ISO A.9.4.5).
- f. Maintenance and copying of program source libraries are subject to strict change control procedures (ISO A.9.4.5) as under Section 21.2.

## **23 Security in development and support processes (ISO 8.1 & A.14.2)**

### **23.1 Objectives**

To maintain the integrity and security of the NCEPOD network when implementing new procedures or integrating new software

### **23.2 Change control procedures (ISO 8.1 & A.14.2.2)**

In order to minimise the corruption of information systems, the process of implementing changes to operational procedures (whether supported by new applications or existing applications) is strictly controlled.

Operational changes that will have a great impact on NCEPOD's information processing will be investigated by the Information Security Forum before decisions are made as to how (and if) the proposed changes are to be made. The review process includes:

- a. reviewing the necessity of changes to any agreed authorisation levels (ISO A.14.2.2)
- b. ensuring changes are submitted by authorised users (ISO A.14.2.2)
- c. reviewing controls and integrity procedures to ensure that they will not be compromised by the changes (ISO A.14.2.2)
- d. identifying all computer software, information, database entries and hardware that require amendments (ISO A.14.2.2 & A.14.2.3)
- e. obtaining formal approval for detailed proposals before work commences (ISO A.14.2.2)
- f. ensuring that any relevant, authorised user accepts changes prior to any implementations (ISO A.14.2.2)
- g. ensuring that implementation is carried out in a way that minimises business disruption (ISO A.14.2.2)
- h. ensuring that the system documentation is updated to reflect the new situation, and that the old documentation is disposed of to avoid confusion (ISO A.14.2.2)
- i. maintaining a version control for all software updates (ISO A.14.2.2)
- j. maintaining an audit trail of all change requests (ISO A.14.2.2)
- k. ensuring that operational documentation and user procedures are changed to reflect that new situation, and that old documentation is disposed of to avoid confusion (ISO A.14.2.2)
- l. ensuring that the implementation of the change takes place at a time that causes the minimum of disruption to the continued functioning of NCEPOD (ISO A.14.2.2)

Some changes to information processing functions result from a change in operational (information handling) procedures. In these circumstances, the review of the necessary changes to the applications should be integrated with a review of the procedural change (see 24.3)

### **23.3 Technical review of operating system change (ISO 8.1 & A.14.2.3)**

Periodically, it may be necessary to change or update the operating system. When such change is necessary, a technical review of the change takes place prior to implementing any changes.

The effect on the type and version of application systems currently running on the existing operating system should be reviewed to ensure that no adverse reaction in any of the business functions of NCEPOD can be expected upon upgrading/changing the operating system.

Where the change takes the form of a patch to the current version of an operating system, a technical review of documentation from the manufacturer(s) of all applications involved as to the effect of the change in the OS on the application software is usually sufficient. Such a review will usually identify whether the upgrade will negatively impact on the application software, and whether it will (in turn) lead to the necessity of upgrading the application software.

If satisfied that the application of the patch will not compromise the security and integrity of the NCEPOD network, or that any compromise is remediable by upgrading the application software (taking into consideration the cost of the upgrades involved) then the patch upgrade can go ahead.

Where the change takes the form of a complete OS version upgrade, the feasibility of fully testing the effects of the upgrade is looked into (ISO A.14.2.3). Full OS version upgrades will usually (but not always) lead to the necessity for upgrading some of the current application software. Due to the cost implications of this, it may be deemed cost effective to create an environment in which to test existing applications against the new operating system and (if it proves necessary) to test newer versions of the application software. In this way the implications for security and integrity (ISO A.14.2.3) and any hidden costs can be assessed before committing NCEPOD to the upgrade.

Any change should be handled to ensure that there is adequate time for review and planning (ISO A.14.2.3), and that there is adequate funding for any testing, if considered necessary (ISO A.14.2.3).

As part of the change control procedure, any necessary changes to the business continuity plans must be considered (ISO A.14.2.3).

#### **23.4 Restrictions on changes to software packages (ISO 8.1 & A.14.2.4)**

Modification to software packages, through alteration of source code, patches and upgrades, or in any other manner, may only be carried out by authorised network support staff, and only when the following points have been reviewed.

- a. the risk of existing controls and processes being compromised (ISO A.14.2.4)
- b. whether the consent of the supplier should be obtained (ISO A.14.2.4) or the support company informed
- c. the possibility of obtaining the required changes from the vendor as standard program updates (ISO A.14.2.4)
- d. the impact if the organisation becomes responsible for the future maintenance of the software as a result of the changes (ISO A.14.2.4)

If changes are essential, the original software is retained (for roll back purposes, if necessary), and any changes fully tested and documented before being applied to the operational environment.

#### **23.5 Covert channels and Trojan code (ISO A.12.2)**

The likelihood of penetration by Trojan code is significantly reduced by NCEPOD's policy of prohibiting any staff member apart from network support staff to install any executable code, in any form, to the network (see Section 17).

It is further reduced by the use of anti-virus software to protect the network (specifically, to block downloads of malicious code from the Internet, and by email attachments). See Section 15 on anti-virus controls for further information.

Network support staff may only install software from a reputable source (ISO A.12.2.1).

### **23.6 Outsourced software development (ISO 8.1 & A.14.2.7)**

Where software development is outsourced, the following points must be considered, and NCEPOD must be satisfied by any agreement reached with the third party, before the third party can be utilised to develop or configure the product.

- a. licensing arrangements, code ownership and intellectual property rights (ISO 8.1 & A.14.2.7)
- b. certification of the quality and accuracy of the work carried out (ISO 8.1 & A.14.2.7)
- c. rights of access for audit of the quality and accuracy of the work done (ISO 8.1 & A.14.2.7)
- d. contractual requirements for quality of code (ISO 8.1 & A.14.2.7)
- e. testing before installation to detect Trojan code (ISO 8.1, A.14.2.7& A.12.2.1)

NCEPOD must be satisfied by any agreement reached with the third party before the third party can be utilised to develop or configure the product.

In addition, the software developed is subject to review and testing to ensure that it does not compromise existing security controls.

## **24 Communications and operations management (ISO A.12)**

### **24.1 Objectives**

To ensure the correct and secure operation of information processing facilities

### **24.2 Documented operating procedures (ISO A.12.1.1)**

The operating procedures identified by the Policy, and throughout the various sections of the Procedures, are fully documented and maintained.

Operating procedures are formal documents relating to the information processing performed by NCEPOD, and therefore changes to the documentation need to be authorised by the Information Security Forum. Such authorisation will normally be given as part of the change control procedures when the process that the documentation refers to is being revised/alterd (Section 24.3).

The procedures specify the instructions for detailed execution of each job, including:

- a. processing and handling of information (ISO A.12.1.1)
- b. scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times (ISO A.1.1.1)
- c. instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (ISO A.12.1.1)
- d. support contacts in the event of unexpected operational or technical difficulties (ISO A.12.1.1)
- e. special output handling instructions, such as the management of confidential output, including procedures for secure disposal of output from failed jobs (ISO A.12.1.1)
- f. system restart and recovery procedures for use in the event of system failure (ISO A.12.1.1)

### **24.3 Operational change control (ISO A.12.1.2)**

Changes to information processing facilities and systems within the NCEPOD network are tightly controlled. Each proposed change to the way in which NCEPOD handles data is discussed within the context of NCEPOD's existing security controls, and any change managed in a way to minimise the disruption to NCEPOD.

Some changes to operational procedures will necessitate changes to information processing applications. In this circumstance, the review of the procedural change will be integrated with a review of the necessary changes to the applications.

In particular, the review of each proposed operational change will include:

- a. Identification and recording of every significant change (proposed and implemented) in writing, so that any implications can be taken into consideration (ISO A.12.1.2). This to be undertaken prior to the review by the Chief Executive (for changes to information handling on an organisational/project-based level), and/or the IT Manager (changes to information processing facilities), and/or other personnel relevant to the situation.
- b. Assessment of the potential impact of every significant change (ISO A.12.1.2), to be documented in writing as part of the review. Initial assessment of the impact to be done by the relevant staff members (as above) and presented to the Information Security Forum for discussion/amendment at the review proper. This will include impact on other information processing systems/procedures, and on existing Policy & Procedures (i.e. to ensure non-contravention, or necessary amendments before acceptance can be given).

- c. Formal approval (or rejection) for the proposed change is given in writing at the end of the review period. Acceptance/rejection by the Information Security Forum to be formally signed off by the Chief Executive (ISO A.12.1.2)
- d. As part of the acceptance documentation, the circumstances for aborting unsuccessful changes will be explicitly stated (as agreed at the review stage). This will include documentation of the responsibilities and methods for recovering from such unsuccessful changes (ISO A.12.1.2)
- e. Communication (and discussion) of change details with all relevant staff (ISO A.12.1.2) is made prior to commencement of work.

#### **24.4 Separation of development and operational facilities (ISO A.12.1.4)**

Where possible, facilities for testing and development of new software and operational procedures will take place outside of the main NCEPOD operational environment. This may involve complete physical isolation from the NCEPOD network, or it may involve the use of an environment logically separate from the operational environment, but still situated within the same NCEPOD network.

In order to minimise the chances of operational processes and data becoming corrupted, the practicalities of using the following controls are considered in the review for each individual development project.

- a. development and operation software should, where possible, run on different computers, or in different domains (or directories, if necessary) (ISO A.12.1.4)
- b. development and testing activities should be separated as far as possible (ISO A.12.1.4)
- c. compiler, editors and other system utilities should not be accessible from operational systems when not required (ISO A.12.1.4)
- d. different log on procedures (and accounts, if necessary) should be used for operational and test systems to reduce the risk of error (ISO A.12.1.4)

## **25 System planning and acceptance (ISO A.12.1)**

### **25.1 Objective**

To minimise the risk of system and business failure by adequately planning ahead to ensure future need for additional capacity are anticipated and met.

### **25.2 Capacity planning (ISO A.12.1.3)**

It is the responsibility of the IT Manager to monitor network capacity, and to ensure that adequate processing power and storage are available. A monthly log of server capacity (used vs. free space) is kept by the IT Manager.

This monitoring enables pro-active management of the capacity of the NCEPOD network in the most efficient manner, and helps avoid bottlenecks in, or disruptions of, information processing systems.

Regular review of the log will also allow projections to be made concerning future increases in demand for capacity resulting from any operational change, or from the day-to-day expansion of the information held within the NCEPOD network.

Any projections which indicate a need for expansion of capacity are brought to the attention of the Chief Executive.

### **25.3 Authorisation process for information processing facilities (ISO A.14 & A.11.2.4)**

The introduction of new information processing facilities must be authorised by the Chief Executive. Consultation occurs with the IT Manager to enable the implementation of any security controls necessary for integrating the new facility in to the existing framework without impacting negatively on security. (ISO A.14.1.1)

Where necessary, hardware and software are checked to ensure that they are compatible with other system components (ISO A.14.3.1)

The use of personal information processing facilities (e.g. laptops) to process business information must be authorised by the Chief Executive, after the IT Manager is satisfied that sufficient controls are in place (ISO A.14.1)

The use of personal information processing facilities in the workplace may cause new vulnerabilities, and must be authorised by the Chief Executive, after the IT Manager is satisfied that sufficient controls are in place (ISO A.14.1)

#### **25.4 System acceptance (ISO A.14.2.9)**

Acceptance criteria for new information systems, upgrades and new versions of application software are established before embarking on the upgrade. Suitable tests of the system are designed and must be concluded satisfactorily before acceptance and rollout. These criteria are clearly defined and documented before the process of testing begins. A standard template is used, to ensure that each of the categories below is taken into account (i.e. the criteria set for each category, along with evidence of being met (or not met)) and to provide a means for official sign off by the Chief Executive to be documented.

Acceptance criteria considered for each project may include any or all of the following:

- a. performance and computer capacity requirements (ISO A.12.1.3)
- b. error recovery and restart procedures, and contingency plans (ISO A.14.2.9)
- c. preparation and testing or routine operating procedures to a defined standard (ISO A.14.2.9)
- d. agreed set of security controls in place (ISO A.14.2.9)
- e. effective manual procedures (ISO A.14.2.9)
- f. business continuity arrangements (ISO A.14.2.9)
- g. evidence that installation of the new system will not adversely affect existing systems (ISO A.14.2.9)
- h. evidence that consideration has been given to the effect the new system has on the overall security of NCEPOD (ISO A.14.2.9)
- i. training in the operation of the new system (ISO A.14.2.9)

NCEPOD shall only proceed with the implementation or use of the new information systems, upgrades or new versions of application software once the acceptance criteria have been met.

## **26 Systems development and maintenance (ISO 14.1 & A.14.2)**

### **26.1 Objective**

To ensure that security is built into all new information processing systems, including infrastructure (hardware), operating system, and business applications.

### **26.2 Security requirements analysis and specifications (ISO A.14.1.1)**

Any review of business requirements for new systems, or enhancements to existing systems, must include discussion of appropriate security controls that would need to be updated or introduced to integrate the new system/enhancements without compromising security.

All new controls necessary for successful integration are considered indivisible from the installation of the enhancement in itself – installation should not proceed without them.

Security requirements should therefore reflect the business value of the information assets involved, and the potential damage that would result from a failure or breach of security.

NCEPOD acknowledges that controls introduced at the design stage are often considerably more effective, and cheaper to implement and maintain, than those introduced retrospectively.

## **27 Security of system documentation**

System documentation may contain a range of sensitive information concerning NCEPOD business practices and information processing practices. They are therefore treated as sensitive material, and subject to the appropriate security controls for their classification (as detailed throughout this document, specifically within Sections 5, 6 & 7).

In summary:

- a. all system documentation is stored securely
- b. access to system documentation is granted only to authorised personnel (network and database support staff)
- c. system documentation held in electronic format on the NCEPOD network is protected by user access controls

## **28 Compliance (ISO A.18)**

### **28.1 Objectives (ISO A.15.1)**

To comply with all appropriate criminal and civil law, regulations or contractual obligations. To ensure that the design and functioning of NCEPOD's information processing facilities, and all NCEPOD's data handling, complies with all appropriate regulations.

The Chief Executive, on behalf of the Trustees, is responsible for ensuring compliance with all relevant legislation.

### **28.2 Identification of applicable legislation (ISO A.18.1.1)**

All relevant statutory, regulatory and contractual requirements are explicitly taken into account when designing and documenting information systems and processes. The specific controls and individual responsibilities to meet these requirements are similarly defined and documented.

All new legal, regulatory and contractual agreements are reviewed for any necessary changes to the security policy.

### **28.3 Intellectual property rights (ISO A.18.1.2)**

#### **28.3.1 Copyright (ISO A.18.1.2)**

NCEPOD complies with the legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, and trademarks.

Any staff found breaching copyright legislation will be subject to a disciplinary process.

#### **28.3.2 Software copyright (ISO A.18.1.2)**

NCEPOD complies with legal restriction on the use of licensed software and promotes an internal policy of legal usage (Section 8 (Assets Register) and Section 15 (software protection)).

NCEPOD endeavours, within its Information Security and Confidentiality Policy and these procedures, to:

- a. maintain and promote a formal software copyright compliance policy (ISO A.18.1.2)
- b. issue standards for the procedures for acquisition of software products (ISO A.18.1.2)
- c. maintain and promote awareness of software copyright and acquisition policies, including the intent to take disciplinary action in the event of breaches (ISO A.18.1.2)
- d. maintain a proper, current, asset register (ISO A.18.1.2)
- e. maintain proof and evidence of ownership of licenses, disks and manuals (ISO A.18.1.2)
- f. implement controls to ensure that the maximum number of permitted users is not exceeded (ISO A.18.1.2)
- g. carry out regular checks to ensure that only authorised software and licensed products are installed (ISO A.18.1.2)
- h. provide a policy for maintaining appropriate license conditions (ISO A.18.1.2)
- i. provide a policy for disposing or transferring software to others (ISO A.18.1.2)
- j. use appropriate audit tools, as/if necessary (ISO A.18.1.2)

- k. comply with terms and condition for software and information obtained from public networks (ISO A.18.1.2)

#### **28.4 Safeguarding of organisational records (ISO A.18.1.3)**

All organisational records are securely stored to prevent loss or destruction to important and sensitive information. They are classified according to the same guidelines as all other informational assets (Appendix A). All such documents are retained in paper format.

All legal, statutory or regulatory requirements for maintaining records are complied with. Retention of such documentation is specified in Appendix E of this document.

To help maintain compliance with regulatory and statutory requirements, NCEPOD.

- a. Has guidelines for the retention of data (Appendix E) and for the storage, handling and disposal of all necessary records and information (this document as a whole, which is issued to all appropriate staff) (ISO A.18.1.3)
- b. Has a retention schedule (Appendix E) identifying essential record types and the period of time for which they should be retained (ISO A.18.1.3)
- c. Has an inventory of key information retained (as part of the Information Asset Register) (ISO A.18.1.3)
- d. Has implemented appropriate security controls to protect such records and information from loss, destruction and falsification (ISO A.18.1.3). These controls are described throughout this information document.

#### **28.5 Data protection and privacy of personal information (ISO A.18.1.4)**

NCEPOD is registered as a Data Controller. The Chief Executive, on behalf of the Trustees, has responsibility for compliance with the General Data Protection Regulation (GDPR). See Section 18 for a statement of NCEPOD's responsibilities under the Act.

#### **28.6 Prevention of misuse of information processing facilities (ISO A.18.1.5)**

The information processing facilities provided by NCEPOD are for business use. NCEPOD reserves the right to monitor use of the facilities to detect and prevent improper usage.

Where appropriate, a message is prominently displayed at the log on stage indicating that the system being entered is private and that unauthorised access is not permitted.

Where any such monitoring takes place, the staff member(s) involved is informed prior to the monitoring occurring.

#### **28.7 Collection of evidence (ISO A.16.1.7)**

##### **28.7.1 Rules of evidence (ISO A.16.1.7)**

Where any action to be taken involves the law, either civil or criminal, NCEPOD will conform to the rules of evidence as laid down in the relevant law, or in the rules for the specific course in which the case is heard. NCEPOD will take relevant advice on each individual matter, covering the admissibility, quality and completeness and consistency of the evidence (ISO A.16.1.7).

### **28.7.2 Admissibility of evidence (ISO A.16.1.7)**

As above, NCEPOD will take relevant advice to achieve admissibility of evidence under the particular law, or code of practice, involved.

### **28.7.3 Quality and completeness of evidence (ISO A.16.1.7)**

NCEPOD will take relevant advice as to the quality and completeness of evidence. In each case, to aid this, NCEPOD will attempt to provide the means for a strong trail of evidence to be established by ensuring that.

- a. during a search for paper-based evidence: any originals found are kept securely, who found it is recorded, along with where it was found, when it was found and who witnessed the discovery (all searches should be witnessed, if possible by an independent third party). The log should be kept securely with the evidence. Any internal investigation should ensure that the originals are not tampered with (ISO A.16.1.7)
- b. for electronic based evidence: any removable media relevant are stored securely, copies of information on hard disks or in memory are taken (where the original cannot be removed intact). A log of all actions during the copying process is kept, and the process should be witnessed (again, if possible, by an independent third party). Arrangements will be made to store one copy of the media and the log securely at the bank, so that all attempts to access the media are logged (ISO A.16.1.7)

## **29 Personnel security (ISO 6)**

### **29.1 Objective (ISO A.8)**

To reduce the risks of human error, theft, fraud or misuse of facilities by addressing security considerations at the recruitment stage, and within staff contracts.

### **29.2 Security considerations for personnel management (ISO A.6 & A7)**

Staff members are bound by the terms of the NCEPOD Information Security, Confidentiality and Data Protection Policy by their Terms and Conditions of Employment (ISO A.7.1.2)

Casual staff and third-party users not bound to Policy by the Terms and Conditions of their employment are required to sign a confidentiality agreement prior to being given access to information processing facilities (ISO 8.1). These agreements are reviewed when there are changes to the terms of employment of contract, or to the nature of the information that they are handling.

Verification checks are made at the time of job application for permanent staff positions, including:

- a. availability of satisfactory business and personal references (ISO A.7.1.1)
- b. confirmation of claimed academic and professional qualifications (ISO A.7.1.1)
- c. independent identity check, if appropriate (passport or similar document) (ISO A.7.1.1)

A similar screening process should be carried out for contractors and temporary staff, whenever they will be handling sensitive information. Where those staff are provided through an agency, the contract with the agency should clearly specify the agency's responsibility for screening, and the notification procedure they need to follow if screening has not been completed or if the results give cause for doubt or concern. (ISO A.7.1.1)

The Chief Executive will ensure that appropriate supervision is undertaken with regard to new and inexperienced staff with authorisation for access to sensitive systems (ISO A.7.2.1)

Staff are bound to confidentiality by their Terms and Conditions of Employment (ISO A.7.2.1). The Terms and Conditions, in conjunction with the Staff Handbook, spell out the employee's rights and responsibilities (ISO A.7.2.1).

## **Appendix A - Information classification guidelines**

All assets held by NCEPOD are classified in terms of Criticality and Sensitivity. This classification arises from the risk assessment procedures outlined earlier within this document. Assets include any item owned or used by NCEPOD, be it physical (e.g. hardware) or informational (electronic or paper-based).

Assets are assessed as falling into one of three levels within each category. The handling of, and security for, each asset will then be implemented according to the overall risk category for the asset (a combination of criticality and sensitivity) – summarised under Appendix B Asset labelling and handling.

### **Criticality:**

#### **High**

NCEPOD would be unable to fulfil any of its primary business objectives if the asset was compromised or lost.

#### *Examples:*

*The NCEPOD virtualization Hosts that manage all virtual servers.*

The NCEPOD file server, which hosts all of NCEPOD's informational assets.

The NCEPOD database, which contains the bulk of the information to run a study, and to enable analysis of the information returned in order to publish NCEPOD's reports (primary business objective).

#### **Medium**

Assets the absence of which would cause significant short-term disruption to NCEPOD, hindering NCEPOD in carrying out its business objectives. Replacement of the asset would be subject to a delay that significantly interferes with the fulfilment of NCEPOD's business objectives.

#### **Low**

Loss or failure of such assets would not interfere with the day to day running of NCEPOD, and where the assets can be replicated or replaced quickly and easily. NCEPOD could continue to operate efficiently with little or no disruption in the short term.

**Sensitivity:**

**High**

Compromise of these assets would mean a serious breach of confidentiality and would cause substantial damage to the reputation of NCEPOD, such that NCEPOD may no longer continue to function effectively (or at all). Assets the compromise of which is likely to lead to significant legal actions against NCEPOD by any third party.

Compromise includes unauthorised access to hardware, software and information, including physical or electronic removal (or copying) from the NCEPOD environment.

**Medium**

Compromise of these assets would damage the reputation of NCEPOD, but not to the extent that NCEPOD would be unable to function or would be exposed to major legal action by third parties. Would cause short-term disruption and loss of reputation/efficiency but would be recoverable.

**Low**

Compromise of such assets would have little or no effect on the reputation of NCEPOD and would not breach confidentiality issues.

## **Appendix B - Asset labelling and handling**

### **Assets within the office environment:**

#### **HH, MH, LH**

All assets classified as being highly sensitive are subject to the full weight of controls as enumerated within the entire policy and procedures. This includes all procedures governing asset handling (ISO A.8.1), access restrictions (ISO A.9.2), authorisation (ISO A.6.1.1), data validations, environmental storage (ISO A.11.2), distribution (ISO A.8.3), marking (ISO A.11.1) & review (ISO A.8.1) – all as laid out in the relevant sections of the procedures.

Electronic assets must be protected fully from unauthorised access by implementing all access controls as described within the policy and procedures.

#### **HM, MM, LM**

All assets classified as being of medium sensitivity are subject to the full weight of controls as enumerated within the entire policy and procedures. This includes all procedures governing asset handling (ISO A.8.1), access restrictions (ISO A.9.2), authorisation (ISO A.6.1.1), data validations, environmental storage (ISO A.11.2), distribution (ISO A.8.3), marking (ISO A.11.1) & review (ISO A.8.1) – all as laid out in the relevant sections of the Procedures.

Electronic assets must be protected fully from unauthorised access by implementing all controls as described within the policy and procedures.

#### **HL, ML**

Assets which are high or medium criticality, but of low sensitivity. While there are limited implications where breaches of security are concerned, due to the high to medium criticality of the asset to NCEPOD, full concern should be paid to the proper maintenance and care of the asset so that the availability is not compromised. Business continuity plans for replacing faulty assets should be in place.

#### **LL**

No special controls are required for this category.

### **Assets taken offsite:**

#### **HH/MH/LH**

No asset that is classified as having a high sensitivity is to be taken away from the NCEPOD offices, without the express (documented) permission of the Chief Executive. The decision on whether the asset needs to be held in a securely encrypted format is to be made on a case-by-case basis. Where encryption is required, it is specified in the Authorisation form provided to the user. An original copy of the material taken outside must be retained until the copy is returned. There are very few circumstances where removal of such highly sensitive information is authorised.

All such removal should be logged (both outgoing and on its return). Specific attention should be paid to requirements under asset handling (ISO A.8.1), access restrictions (ISO A.9.2), authorisation (ISO A.6.1.1), environmental storage (ISO A.11.2), distribution (ISO A.8.3), and marking (ISO A.11.1) – all as laid out in the relevant sections of the Procedures.

*Material that should never be taken off-site:*

Completed study questionnaires, medical case notes that have not been anonymised.

#### **HM/MM/LM**

No asset that is classified as having a medium sensitivity is to be taken away from the NCEPOD offices, without the express (documented) permission of the Chief Executive. Such information may need to be held in a securely encrypted format, if specified by the Chief Executive (specification will be formally documented). An original copy of the material taken outside must be retained until the copy is returned.

All such removal should be logged (both outgoing and on its return). Specific attention should be paid to requirements under asset handling (ISO A.8.1), access restrictions (ISO A.9.2), authorisation (ISO A.6.1.1), environmental storage (ISO A.11.2), distribution (ISO A.8.3), and marking (ISO A.11.1) – all as laid out in the relevant sections of the Procedures.

#### **HL**

If the asset is a physical asset, or is information held in a physical form that cannot be replicated, it may only be taken away from the office with the authorisation of the named owner. If a copy of the asset can be maintained on site, the temporary removal of the information does not need to be authorised, but it must still be logged.

If the information is held in electronic form, it does not need to be logged, as a copy will remain on site.

#### **ML**

If the asset is a physical asset, or is information held in a physical form that cannot be replicated, it may only be taken away from the office with the authorisation of the asset's owner. Otherwise, the temporary removal of the information does not need to be authorised, but it must still be logged. If the information is held in electronic form, it does not need to be logged, as a copy will remain on site.

#### **LL**

Information classified as LL may be taken away from the NCEPOD offices without authorisation, but an original copy must be retained on site until the safe return of the asset (if possible).

### **Appendix C - Access control policy**

Appendix C specifies *types* of information (financial, personnel, project-based etc.) that each staff member either should or should not have access to. It is NOT about controls for handling the information according to its *security classification*, which are laid out in Appendix B (and throughout the rest of this document).

Appendix C therefore states whether a staff member is allowed access to the type of information AT ALL. If he/she is, then Appendix B (in conjunction with the Asset Register and the rest of the Procedures) provides the manner for handling that information in a secure manner (in line with its security classification).

Appendix C also specifies what applications each staff member is authorised to use. A policy of prohibited unless actively permitted (ISO A.9.1.1) is used here. Use of any application not listed here is prohibited and may result in disciplinary proceedings.

**Access to information:**

Information type	Chief Executive	Office Administrator	Clinical Researchers & Research Staff	IT Manager	Admin. Officers	Co-ordinators	Case Reviewers
Project based – planning	Yes	Yes	Yes	Yes	Yes	Yes	No
Project based – unanonymised information	Yes	Yes	Yes	Yes	Yes	Yes	No
Project based – anonymised information	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Project based – clinician and local reporter correspondence	Yes	Yes	Yes	Yes	Yes	No	No
Project based – report drafts	Yes	Yes	Yes	No	No	Yes	Yes
Project based – analysis data	Yes	Yes	Yes	Yes	No	Yes	Yes
Business based – Report launch correspondence	Yes	Yes	No	Yes	Yes	No	No
Business based – Report orders / invoice & payments	Yes	Yes	No	No	Yes	No	No
Business based – Financial records	Yes	Yes	No	No	No	No	No
Business based – Personnel records	Yes	No	No	No	No	No	No
Business based – Company records	Yes	Yes	No	No	No	No	No
Business based – Contracts	Yes	Yes	No	Yes	No	No	No
Business based – Confidentiality / Data Exchange Agreements	Yes	Yes	No	Yes	Yes	No	No
Business based – Steering Group Correspondence	Yes	Yes	No	No	No	Yes	No
Business based – Advisor correspondence	Yes	Yes	No	No	No	Yes	Yes
IT based – logs	Yes	No	No	Yes	No	No	No
IT based – configuration logs	Yes	No	No	Yes	No	No	No
Security based - incident logs	Yes	No	No	Yes	No	No	No

**Access to applications**

Application	Chief Executive	Office Administrator	Clinical Researcher & Research Staff	IT Manager & support staff	Admin. Officers	Co-ordinators	Case Reviewers
MS Word	Yes	Yes	Yes	Yes	Yes	Yes	No
MS Excel	Yes	Yes	Yes	Yes	Yes	Yes	No
MS Access	Yes	Yes	Yes	Yes	Yes	Yes	No
MS PowerPoint	Yes	Yes	Yes	Yes	Yes	Yes	No
MS Outlook	Yes	Yes	Yes	Yes	Yes	Yes	No
Adobe Acrobat Viewer	Yes	Yes	Yes	Yes	Yes	Yes	No
MS Internet Explorer	Yes	Yes	Yes	Yes	Yes	Yes	No
MS Visio	Yes	Yes	Yes	Yes	Yes	No	No
<del>ABBYY Share NA – FormDesigner/FormReader NA</del>	<del>NA</del>	<del>NA</del>	<del>NA</del>	<del>NA</del>	<del>NA</del>	<del>NA</del>	<del>NA</del>
MS Visual Studio	Yes	No	No	Yes	No	No	No
Photoshop Elements	Yes	Yes	Yes	Yes	Yes	No	No
Dreamweaver	Yes	No	Yes	Yes	No	No	No
Sage 50 Accounting	Yes	No	No	No	No	No	No
Adobe Acrobat Professional	Yes	Yes	Yes	Yes	No	No	No
PGP Personal Privacy	Yes	Yes	Yes	Yes	No	Yes	No
<del>PCAnywhereNA</del>	<del>No</del>	<del>No</del>	<del>No</del>	<del>Yes</del>	<del>No</del>	<del>No</del>	<del>No</del>
Altaro Virtualisation Backup	No	No	No	Yes	No	No	No
APC PowerChute	No	No	No	Yes	No	No	No
MS Exchange Server	No	No	No	Yes	No	No	No
Kasaya Software	No	No	No	Yes	No	No	No
Adobe Create Cloud	Yes	NO	NO	Yes	No	No	No

**Appendix D - Business Continuity Plan**

**Business Continuity Plan**

As stated in Section 16 of the NCEPOD Information Security Procedures, the NCEPOD Business Continuity Plan is formed from the totality of the plans outlined here. Each individual plan within the Business Continuity Plan attempts to address the procedures needed to overcome specific events detrimental to the successful functioning of NCEPOD. These events will occur on a scale from minor incident to major disaster, but each will have a plan, which is detailed in a structured, standard manner to enable quick action to recover from/deal with the situation. Section 16 of the Information Security Procedure provides specific details of the planning and review process. All sections that it is feasible to test are tested on a scheduled basis as outlined and logged in the IT Housekeeping log on the NCEPOD Intranet (Intranet\Security Procedures and resources\Security Resources\Log Files\IT Housekeeping).

Appendix D is split into two sections.

Part One is the Impact Analysis Table, which summarises the events considered a threat to NCEPOD, the likelihood and consequence of the event, and the plan to be used to address the event. This Table is reviewed (and amended, if necessary) as part of the annual review of the Plan.

Part Two lists the individual plans.

Both parts form NCEPOD’s Disaster Recovery Plan.

**Ownership**

Each step of each plan has an owner, who is the person responsible for the actions to be undertaken within that stage. This owner is assigned as the most appropriate person to deal with the issues/take the actions outlined in the step. Ownership is assigned and reviewed by the Information Security Forum.

Each plan also has an overall owner (who may or may not be involved with the majority of the steps in the plan). The overall owner is responsible for ensuring that any changes in situation/processing/personnel etc. are addressed and (if necessary) the plan altered to account for them.

These owners are specified according to job role. Also specified is a deputy-owner – the person who is to assume responsibility in the nominated owner’s absence.

Note: Where Staff is specified, it relates to the owner (staff member) of an individual asset.

<b>Code</b>	<b>Owner</b>	<b>Deputy</b>
CE	Chief Executive	IT Manager
OA	Office Administrator	Chief Executive
IA	IT Manager	IT support staff member
Staff	Owner of an individual asset	IT Manager

**Impact Analysis Table**

<b>Scenario</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Addressed by:</b>
General power cut	Low	Complete inability to process information or use any electrical equipment	Plan 1: Electrical power failure to office
Loss of internet connection	Low-Medium	Main issue would be loss of email, which would have consequences if problem remained unresolved medium to long term	Plan 2: Failure of NCEPOD’s Internet connection
Denial of service	Low	Variable (depending on systems affected)	Plan 3: Denial of Service
Failure of online questionnaire system	Low	Minor if short-term resolution achieved, worsening as time progresses without resolution. All projects include online questionnaires	Plan 4: Failure of online questionnaires
Inability to access files and folders on the server	Low	Major - complete inability to access files and folders on server, possibly including email	Plan 5: Server hard drive failure
Complete inability to log on to server	Low	Major - complete inability to access files and folders on server, including email	Plan 5: Server hard drive failure

Scenario	Likelihood	Impact	Addressed by:
Loss of access to NCEPOD offices (with no actual damage to processing equipment or data)	Low	Major. Although information assets are recoverable (when access granted) NCEPOD will not be able to function as normal in the intervening period.	Plan 6: Fire in part of building not immediately effecting NCEPOD – COVID-19 pandemic
Complete destruction of physical assets (all network hardware, all paperwork)	Low	Major. Potential loss of electronic and paper-based assets.	Plan 7: Fire in NCEPOD offices

## Individual plans

Each plan is in tabular form, for clarity. Each plan conforms to the following scheme:

<b>Element of the plan</b>	<b>Explanation</b>	<b>1BOwner</b>
<b>Prior precautions</b>	Details of precautions that must be in place <i>prior to the potential event</i> , in order to minimise the impact of the event, should it occur. To enable speedier resolution of problems associated with the event, and to minimise the chances of damage/disruption to other systems that are dependent upon the asset affected.	Staff member(s) responsible for the actions detailed in this step.
<b>Activation</b>	Conditions for activating the plan. Normally self-explanatory.	As above
<b>Immediate precautions</b>	Actions to be taken <i>immediately</i> - before <i>any</i> attempt to resolve the problem itself. While not always necessary, the plan will specify if action <i>must</i> be taken <i>immediately</i> to prevent/minimise further damage to the system affected, or to information contained on the system.	As above
<b>Action to resolve the issue</b>	Steps to be taken, after any immediate actions, to resolve the problem and get NCEPOD functioning properly as quickly as possible. Includes any steps that can be taken by NCEPOD staff members, a timescale for bringing in outside help (if appropriate/necessary), and a timescale for escalating to the fall-back procedures (below).	As above
<b>Fall back procedures</b>	Procedures to be taken to allow NCEPOD to continue functioning whilst the problem is being resolved.	As above
<b>Resumption procedures</b>	Procedures to be followed after resolution of the problem, but before normal business functioning can be resumed.	As above
<b>Maintenance and testing</b>	Timescale for testing the plan. Testing to involve all the owners and be carried out (as near as possible) to simulate a real event. Testing process to be performed as outlined in section 16.3.2 of the Information Security Procedures.	As above
<b>Education</b>	A list of all staff members who need to be aware of the plan, along with a timescale for any necessary education of those staff members.	As above

**Plan 1. Electrical power failure to office**

2BElement	Actions	3BOwner
<b>Prior precautions</b>	<p>Server should be connected to electricity supply through UPS.</p> <p>Daily backups to ensure that information corrupted by power failure can be restored with minimum loss of work.</p> <p>Ensure that Maintenance Contracts cover highly critical processing equipment (as specified in Asset Register) against damage caused by electrical failure.</p> <p>All highly critical processing equipment (as specified in Asset Register) to undergo cost-benefit analysis with regard to insuring against damage caused by power failure.</p>	<p>IA</p> <p>IA</p> <p>IA</p> <p>CE</p>
<b>Activation</b>	Failure of electrical power	
<b>Immediate precautions</b>	<p>Shut down server and turn of UPS.</p> <p>Switch off all workstations that were on at time of power cut and isolate at socket.</p>	<p>IA</p> <p>Staff</p>
<b>Action to resolve the issue</b>	<p>Report problem to the landlord.</p> <p>If landlord not available, contact energy supplier directly.</p> <p>Ensure staff are able to continue working on other tasks.</p>	<p>OA</p> <p>OA</p> <p>PM</p>
<b>Fall back procedures</b>	<p>None.</p> <p>NCEPOD is dependent upon electrical power for processing information. In the absence of power for any long-term period, NCEPOD would not be in a position to provide an alternative source of electricity, nor an alternative location ready furnished for data processing.</p>	
<b>Resumption procedures</b>	<p>Switch on electrical equipment.</p> <p>Boot the server, and check all services start as normal.</p> <p>Inform staff they can turn on machines and log on, but not to database yet.</p> <p>Check database for possibility of corruption. Restore if necessary.</p> <p>Inform staff can log on to database, and (if necessary) that they may need to replicate some work lost (if a restore from backup was necessary).</p>	<p>Staff /</p> <p>IA</p> <p>IA</p> <p>IA</p> <p>IA</p> <p>IA</p>
<b>Maintenance and testing</b>	<p>Full testing of the plan by switching off electricity supply to whole office is impractical and may in itself cause damage to sensitive equipment.</p> <p>However, the UPS is checked on a monthly basis, to ensure battery is displaying enough charge to allow safe shutdown of the server (5-6mins, minimum). As part of this check, the UPS is tested by switching mains power to UPS off, and speed of the drain is monitored – for monthly test, power is re-connected before battery drains.</p> <p>Full test, including server shutdown procedure, is performed quarterly (at a convenient date/time, so as not to disrupt work)</p>	<p>IA</p> <p>IA</p> <p>IA</p>
<b>Education</b>	<p>Minimal requirements. Staff members should be instructed to turn off their own machine, and to turn off electricity supply at the wall, in the event of a power cut.</p>	<p>IA</p>

**Plan 2. Failure of NCEPOD's Internet connection**

4BElement	Actions	5BOwner
<b>Prior precautions</b>	Internet connection is checked every weekday morning as part of a routine check to ensure email delivery is functioning properly. ISP (Internet Service Provider) (Virgin Media) provides a backup email server to allow safe collection of email while our mail server is off line. Ensure the correct support phone number (Virgin Media Technical Support) is maintained in the NCEPOD Contacts folder and changed immediately if notified.	IA IA IA
<b>Activation</b>	As a result of the daily check (see precautions) or following report by any staff member during the course of the day.	Staff/ IA
<b>Immediate precautions</b>	None	
<b>Actions to resolve the issue</b>	Attempt to isolate nature of the failure by inspection of router (attempt diagnostic connections, in sequence). If router is blocking traffic, reset. Restart the router. If communication with ISA Server and internal address of router are okay, but cannot access past the router, immediately contact Virgin Media Technical support centre (08000520500) Account number: 85451202.  Call to Virgin Media technical support to take place no longer than 20 minutes after the fault was noticed.	IA IA IA
<b>Fall back procedures</b>	Fibre optic line failure – none. Problems caused by failure of the Fibre optic line (as opposed to failure of our equipment) need to be investigated and resolved by Easynet (in conjunction with Virgin Media, if necessary). Leasing/rental of a second ADSL line as a precaution against failure would not be cost effective.	Virgin Media/
<b>Resumption procedures</b>	Ensure that emails queued to go out during the line failure have successfully been sent, and that we are receiving incoming emails again.	IA
<b>Maintenance and testing</b>	Not practical to involve Virgin Media in a simulation of a full line failure. Router failure simulation as part of education (see below)	IA
<b>Education</b>	IT support staff to run through the process of testing & resetting router on a quarterly basis, to ensure efficient response to actual failures.	IA

**Plan 3: Denial of Service**

6BElement	Actions	7BOwner
<b>Prior precautions</b>	Internet connection is checked every weekday morning as part of a routine check to ensure it is up and running. ISP provider (Virgin Media) provides a backup email server to allow safe collection of email while our mail server is off line due to any denial of service on NCEPOD mail server. Firewall logs are checked on a weekly basis to pinpoint suspected attempts at denial of service, and to take appropriate steps to eliminate/minimise threats.	IA IA IA IA
<b>Activation</b>	As a result of the daily Internet check (see precautions) or following report by any staff member during the course of the day.	Staff/ IA
<b>Immediate precautions</b>	Disconnect the NCEPOD network from the Internet by switching off the Virgin Media router (Hitron)	
<b>Actions to resolve the issue</b>	Attempt to isolate nature of the cyber-attack and ports involved by inspection of server event logs. If log reveals the point of cyber-attack, and action can be taken to remove the weak-point by altering the firewall ruleset and/or blocking the originating network, it is done.  If internal investigation does not indicate any action, contact The Gallery Partnership (IT support company) for advice on how to handle and resolve the problem (02070962800). Call to The Gallery Partnership to take place no longer than 30 minutes after the denial of service was noticed.  Once issue resolved/advice taken, disconnect router from network, and reconnect to standalone machine. Turn on router, and monitor the connection from the standalone machine, to ensure source of Denial of Service is properly blocked or has stopped.  Reconnect router to network.	IA IA  IA / Gallery  IA  IA
<b>Fall back procedures</b>	Contact The Gallery Partnership (above) for advice on how to handle and resolve the problem.	

8BElement	Actions	9BOwner
<b>Resumption procedures</b>	<p>Ensure that emails queued to go out during the line failure have successfully been sent, and that we are receiving incoming emails again.</p> <p>Check NT Event Logs on server to ensure no unauthorised access has occurred (i.e. DoS was not cover for any intrusion into the network).</p> <p>Collect evidence of source of Denial of Service, for possible resolution with network/ISP used to launch cyber-attack.</p> <p>Collect evidence of any intrusion (dates, times, nature of intrusion, evidence of source of intrusion etc.) for possible legal remedy.</p> <p>Report all evidence to Chief Executive.</p> <p>Document and review entire episode as a Security Incident under Section 12.</p>	<p>IA</p> <p>IA</p> <p>IA</p> <p>IA</p> <p>IA</p> <p>IA</p>
<b>Maintenance and testing</b>	<p>Regular monitoring of firewall logs (as part of weekly IT housekeeping).</p> <p>Though it is not feasible to attempt creation of an actual denial of service for testing the plan, a quarterly run through is undertaken of all steps from Immediate precautions to Resumption procedures (apart from those involving The Gallery Partnership, and reporting requirements).</p>	<p>IA</p>
<b>Education</b>	<p>IT support staff to run through the process of dealing with a denial-of-service cyber-attack on a quarterly basis (as above).</p>	<p>IA</p>

**Plan 4: Failure of online questionnaires**

10BElement	Actions	11BOwner
<b>Prior precautions</b>	Copy of the software held off-site by the developers Sunstone Technologies.	IA IA IA IA
<b>Activation NA</b>	Any reported incident that software has failed.	Staff
<b>Immediate precautions NA</b>	Instruct staff to immediately close any open sessions they have. Elicit the exact nature of the failure from staff member who reported it. Attempt to correct problem - check internet connection	IA IA IA IA
<b>Action to resolve the issue</b>	Attempt to isolate nature of the failure by inspection of router (attempt diagnostic connections, in sequence). If router is blocking traffic, reset. Restart the router. If communication with ISA Server and internal address of router are okay, but cannot access past the router, immediately contact Virgin Media Technical support centre (08000520500) Account number: 85451202.	IA IA IA IA
<b>Fall back procedures</b>	Switch staff to other work.	PM
<b>Resumption procedures</b>	Once back up and running check last action undertaken	IA IA IA
12BElement	Actions	13BOwner
<b>Maintenance and testing</b>	Regular updates received and communication with Sunstone Technology	IA IA
<b>Education</b>	Neil Smith is responsible for the development of this system and ensuring all staff who are using it are up to date with any changes made.	IA

**Plan 5: Server hard drive failure**

14BElement	Actions	15BOwner
<b>Prior precautions</b>	Daily backup schedule of information held on server, to allow restore of information with maximum of one day's work lost. Inclusion of server on maintenance contract with IT support company, with components/whole server covered on a swap out basis.	IA IA
<b>Activation</b>	Inability of anyone to access information on the system through server hard drive failure	
<b>Immediate precautions</b>	Any helpful physical evidence – paper copies of changed files, forms input etc. – should be identified and retained, as it will be helpful in any attempt to recreate as much of the lost information as possible.	Staff
<b>Action to resolve the issue</b>	Immediately contact The Gallery Partnership and inform them of hard drive failure. Request dispatch of engineer to attend NCEPOD offices with suitable replacement hard drives or replacement server (preloaded with Windows 2012R2 Server). Once disks replaced/new server installed, assist engineer with reconfiguring specific system settings & installing additional software. Restore information from latest backup tapes.	IA IA IA
<b>Fall back procedures</b>	Maintenance contract specifying repair or replace of server and components (drives) to allow NCEPOD to be up and running as quickly as possible in event of complete hard drive failure	IA /CE
<b>Resumption procedures</b>	As much of the lost information as possible should be recreated / re-entered onto the system (i.e. data entered between date/time of backup used and when the error occurred). Notes & paperwork from Immediate precautions section may be involved in this (e.g. database – questionnaire dates returned, LRFs input, spreadsheets input etc.). This to be done before authorisation given for any new information added (i.e. formal resumption of processing)	Staff IA
16BElement	Actions	17BOwner
<b>Maintenance and testing</b>	Monthly test of full restore, to ensure that information on backup tapes is available. Weekly monitoring of Event Logs (as part of routine procedures) to identify early any disk problems/errors that may lead to disk failure (to identify and take prior action, rather than waiting and losing data).	IA IA
<b>Education</b>	No special requirements	

**Plan 6: Loss of access to NCEPOD offices (with no actual damage to processing equipment or data)  
– updated in light of COVID**

18BElement	Actions	19BOwner
<b>Prior precautions</b>	<p>Having a working from home policy that covers:</p> <ol style="list-style-type: none"> <li>1. Home security</li> <li>2. Device security – including home router setup and keeping NCEPOD laptops at home up to date</li> <li>3. Access to the info that is needed from home – rules as to who can access what with regard to levels of identifiable data</li> <li>4. No information kept on the C drive – all NCEPOD data accessed via a VPN and remote desktop service</li> </ol> <p>Make sure that the office is secure at all times so that if access cannot be gained then staff are confident that the contents are safe.</p>	
<b>Activation</b>	<p>Loss of access to NCEPOD offices caused, for example, by fire or flood closing part of the building, rendering access impossible to an otherwise undamaged NCEPOD office. More recently this has been experienced due to COVID</p>	CE
<b>Immediate precautions</b>	<p>Ensure that all relevant office documents and software are on the server and can be accessed remotely</p> <p>Ensure there is security cover that can be activated if needed</p> <p>Ensure there are enough laptops to provide to staff to be able to work from home</p>	CE
<b>Action to resolve the issue</b>	<p>If relevant, contact landlord for likely timescale for re-entry to the building.</p> <p>In relation to a pandemic then a return to the office would be phased and led by Government guidelines</p>	CE
<b>Fall back procedures</b>	<p>If disruption is to last for any significant length of time, arrange for temporary accommodation in another part of building (if possible, and if accessible) or institute move to other premises.</p> <p>Initiate working from home for all staff.</p> <p>Ensure office is accessed by a staff member at least once a week if it is unoccupied for more than 30 days to ensure the insurance is covered. Before shutting the office check all unnecessary plugs are off and disconnected, including the fridge. Check all doors, taps and windows and set the alarm.</p>	CE
<b>Resumption procedures</b>	<p>No fixed procedure, this would depend on the cause.</p>	
<b>Maintenance and testing</b>	<p>Ensuring the server is maintained</p> <p>Ensuring that everyone has suitable equipment at home and that personal internet connections are kept as up to date as possible</p>	

<b>Education</b>	<p>Fire safety training (in house) every two years for all staff                      New staff members receive fire safely training as part of induction.                      Regular team meetings are/can be used discuss the issues as they occur. The Information Security Forum meetings can be used to discuss IT related matters</p>	<p>CE                      CE</p>
------------------	---	---------------------------------------

**Plan 7: Complete destruction of all physical assets (all hardware and paperwork) including office space**

20BElement	Actions	21BOwner
<b>Prior precautions</b>	<p>All physical assets should be appropriately insured, to allow complete replacement in as short a time scale as possible.</p> <p>A monthly backup is run, the tape from which is stored off-site (at a local bank). This will allow full restoration of electronically held information with maximum loss of work limited to four weeks.</p> <p>Informational assets held in physical form (i.e. on paper) that are essential to the functioning of NCEPOD are scanned so that an image of their content can be stored on the same back up as above.</p>	<p>CE</p> <p>IA</p> <p>IA /CE</p>
<b>Activation</b>	Complete loss of NCEPOD office, hardware & paperwork, for instance by flood or fire	
<b>Immediate precautions</b>	None	
<b>Action to resolve the issue</b>	<p>Contact insurance company to lodge claim.</p> <p>Contact commercial estate agent to locate suitable accommodation for re-start.</p> <p>Once suitable accommodation is arranged, and insurance claim settled, tender for purchase and installation of replacement computer system etc.</p> <p>Restore all information from backup tape held at bank.</p> <p>Any necessary (and possible) steps to recover lost paper-based project data to be initiated.</p> <p>No specific timetable – will depend upon swiftness of insurance claim, location of another suitable location to re-establish business etc.</p>	<p>CE</p> <p>CE</p> <p>CE</p> <p>IA</p> <p>PM</p>
<b>Fall back procedures</b>	None	
<b>Resumption procedures</b>	From data restored, assess whether an attempt should be undertaken to replace paper-based information that was lost on a project-by-project basis.	CE/PM
<b>Maintenance and testing</b>	None practical	
<b>Education</b>	<p>Fire safety training (in house) every two years for all staff</p> <p>New staff members receive fire safely training as part of induction.</p>	CE

## Appendix E - Guidelines for Archiving

- 1 Paperwork to be archived once a year, therefore a day should be allocated for doing this, and is the responsibility of individuals and their line manager.
- 2 Computer files to be archived every 3 months.
- 3 Local Reporter correspondence to be kept for 3 years (covering the studies being collected, reviewed and recently published), destroy the rest.
- 4 Current study data to be kept until three months following publication. Original paperwork of data once scanned and analysed can be destroyed, providing an image is retained.
- 5 Steering Group correspondence to be kept for 3 years current members, get rid of anything prior especially if simply information on meetings to be held. Keep on file information regarding Steering Group members who have retired. Keep list of all members and term served where possible.
- 6 Case Reviewer correspondence to be kept for current data being collected and reviewed. Previous correspondence to be destroyed. Keep record of all case reviewers and term served. Signed confidentiality statements should be kept.
- 7 Report Launch correspondence to be kept for last published report only. Press releases, formal responses and attendance lists to be kept for all published reports for two years and previous years archived. All press cuttings to be kept on site.
- 8 Finance records to be kept for six years from the end of the last financial year they relate to. Prior accounts to be archived, but all must be retained.
- 9 Personnel records for job applicants and interviewed candidates should be kept for one year on site then destroyed. Previous employee records should be archived up to 6 years.
- 10 Company records to be kept for 3 years and the rest archived. Steering Group and Trustee Minutes to be kept on site.
- 11 Confidentiality agreements with current suppliers must be retained. Archive previous supplier agreements.
- 12 IT Error logs should be kept for one year and previous years up to 3 years should be archived.
- 13 Configuration logs should be kept for one year and previous years up to 3 years archived.

## Appendix F – Day to day access to NHS.net/email/public folders/folders on intranet

### F.1 Email - nhs.net

1. **Logging in:** all who have access to nhs.net should login to the account daily. It takes a long time to load and update if left for a longer period.

**NHS mailbox appearing below personal mailbox in Outlook:** a password-protected mailbox will be set up below each person's mailbox. This is to avoid having to toggle between the two accounts when Outlook is opened up. The nhs.net mailbox must still require a password each time it is accessed (a password must not be saved to allow automatic entry).

2. **Access:**

Administrative Officers, Research Assistants, Researchers, Clinical Researchers, and IT Manager.

3. **Password expiry:**

Expiry emails are sent to nhs.net and appear in the inbox. Whomever goes into the mailbox and sees the notification first, should notify the IT Manager who will change the password and notify the team of the new password. The Deputy Chief Executive is the back up for when the IT Manager is away.

4. **Inbox** - study emails should be monitored in nhs.net. At least one person per study should be allocated to do this, with a plan for when they are away from the office.

Process for dealing with an email: opened, answered/forwarded to another mailbox, replied to acknowledge receipt, and marked with a tick. Then delete at that time or at least within 1 week of arrival.

5. **Attachments:** save attachments to the I:/ drive and check that they open (only when in the office).
6. **Forwarding emails:** if the email needs to be forwarded, remove the attachment before forwarding. This is for anything that includes sensitive information such as data collection spreadsheets, and case notes. Even if the case notes have been anonymised prior to sending, save the attachment on the I:/ drive as it will be too large to forward via email.
7. **Forwarding emails** to study mailbox in public folders - check that the email has arrived in public folders (sometimes full email address has been removed when forwarding or email has not arrived, so must check before deleting from nhs.net).
8. **Sent items:** once checked, delete email from Sent items in nhs.net after every session. In addition, the IT Manager has set up an Outlook rule to delete items every 2 weeks from the "Deleted" folder. Sent emails can be moved to the study folder in Outlook's public folders if response useful for study team to view. Any attachments should be removed.
9. **Deleted folder** – the IT Manager has set up an Outlook rule to delete items every 2 weeks from the "Deleted" folder.

## 10. Confidential information:

All emails that contain confidential information or have attachments that contain confidential information must be sent from nhs.net.

Do not send any confidential emails from personal mailboxes (even password protected PDFs). Sent items with confidential information in nhs.net must be deleted. If there is other content which needs to be kept, discuss with Information Security lead.

**Holiday cover:** Clinical Researcher to check the inbox or arrange for someone else to monitor it.

### F.2 Email – study folders on Outlook’s public folders and personal mailbox

#### 1. Attachments:

**Inbox-** all attachments to be saved to I:/ drive as soon as practicable and no longer than within 2 weeks of arriving. Attachments to be deleted from email once saved to I:/drive. Email retained in public folders (attachment deleted).

2. **Sent items in personal mailbox** – move to the relevant study emails in Public Folders if in reply to an email from Public Folders and/or contains a response that would be useful to share with the study team.

3. **Data breach** – delete email if there is a data breach, record on data breach spreadsheet, and email local reporter (see data breach section below).

4. **Archiving:** all emails and folders in Public Folders deleted rather than archived on CDs at the end of study.

### F.3 Case notes

1. **On CDs:** check that the files open and save to the I:/ drive within 2 weeks. If patient ID is written on the disc, use a permanent marker to black it out.

2. **Anonymising:** details of the patient and family/friends in case notes (both hard copies and electronic copies in Adobe) should be anonymised within 2 months of receipt (all clinician details can remain). If possible, anonymise electronically before printing notes and then delete. This can be done by adding a black colour or box over the information.

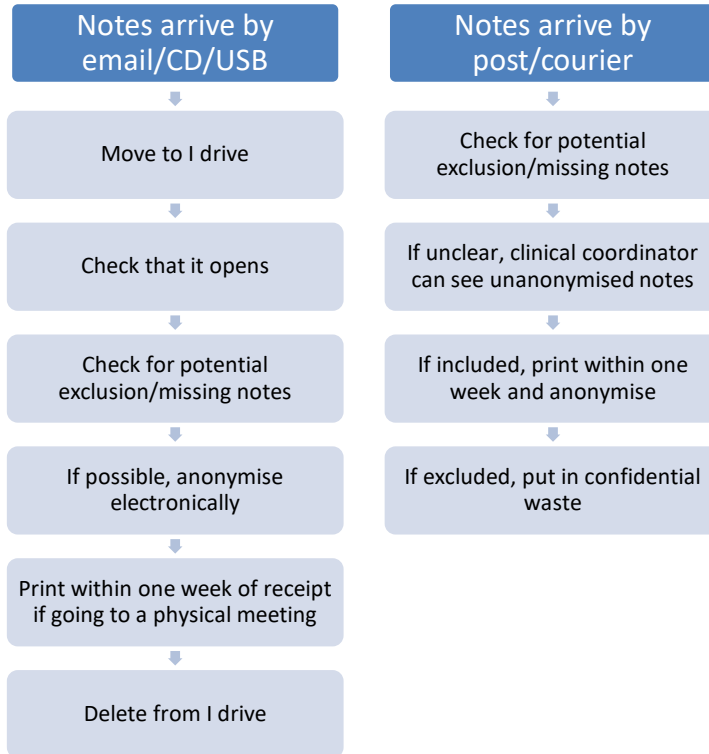
3. **Notes outside study period:** delete or put into confidential waste immediately (if a large amount, Anisa can book extra bags by Tuesday).

4. **Missing notes:** can still be anonymised but discuss as a team first to decide how urgent it is. Contact the Trust/Board with a deadline for the remaining notes. Advise that if remaining notes aren’t received, they will be marked as Not Returned.

5. **Destroying electronic copies:** once printed, electronic copies of case notes should be deleted on I:/ drive and CDs cut up. Strong scissors have been purchased in the office for this purpose.

6. **Recycling CDs:** snap or cut the CD in half and add to the A4 box in filing cabinet 2. Let Anisa know when box is almost full or more than 20 will be added to the box. Anisa will arrange for box to be collected for recycling.

**Destroying hard copies:** when the report is in the final draft stage – when type set by our report designer. This should be as soon as possible or maximum 3 months.



#### F. 4 Excluded cases

**Deleting/destroying:** when a case is being excluded, both electronic and hard copies should be destroyed at the same time.

#### F. 5 Data breaches and confidentiality

**Add the details to the data breach spreadsheet if:**

- no password has been added to patient-identifiable information such as case notes or data collection spreadsheet
- clinician details visible on spreadsheet

The person who encounters the security breach should email the Local Reporter using a standardised email. The Data Protection Officer will monitor this spreadsheet (on the first Monday of the month).

**Organisational questionnaires** – a copy can be kept by Local Reporters as no data breach.

#### F.6 Importing spreadsheets

Delete spreadsheet on I:/ drive once imported and selection has been made on database.

## **F.7 Reviewer CVs**

**Delete CVs** - once reviewers have been recruited, successful reviewers' CVs should be kept until the end of the study and unsuccessful candidates' CVs should be deleted immediately.

**Dropbox** – should not be used to share CVs – use RDS or Teams

**PowerPoint presentation at reviewer training day:** successful candidates - CVs being kept until the end of the study.

CVs of unsuccessful candidates destroyed.

## **F. 8 Back ups**

### **Daily backups occur at 9pm**

Weekly back up tape and key are taken by one of the team to the security deposit box once a week.

When walking to and from Balthorne Security - back up disk, key for box, and ID card to be kept securely in bag. On return to the office, put key in key safe and put card away securely in desk pedestal.

**Peyman** – set up rule on Outlook to delete Sent items and Deleted items every 2 weeks on nhs.net.

**Appendix G - Cross reference of ISO 27001 controls to NCEPOD procedures**

Table of cross-references is in order of ISO 27001, cross-referencing each section or control with the relevant passages in the Procedures document. Includes, where necessary, reasons that a particular area/control proposed by ISO 27001 is not implemented / is not appropriate to NCEPOD as an organisation.

ISO Clause	ISO Control Ref.	ISO Section	NCEPOD Section(s)	Reason section/control is not considered appropriate for NCEPOD
	1	Scope	1.1.1	
	3	Terms and definitions	1.1.1	
	4	Context of the organisation	1.1.1	
	4.1	Understanding the organization and its context	1, 2	
	4.2	Understanding the needs and expectations of interested parties	1.1, 2.3	
	4.3	Determining the scope of the information security management system	1, 1.1.1, 1.1.2	
	4.4	Information security management system	1.1, 1.1.1	
	5	Leadership		
	5.1	Leadership and commitment	1.1.4	
	5.2	Policy	1, 1.1, 1.1.4, 2.2	
	5.3	Organisational roles, responsibilities and authorities	1.14, 2.2	
	6	Planning		
	6.1	Actions to address risks and opportunities		
	6.1.1	General	1, 2	
	6.1.2	Information security risk assessment	1	
	6.1.3	Information security risk treatment	1	
	6.2	Information security objectives and planning to achieve them	1.1.1, 1.1.2, 1.1.4	
	7	Support		
	7.1	Resources	1.1.1	
	7.2	Competence	1.1	
	7.3	Awareness	1.1	
	7.4	Communication	1.1.2, 1.1.4	
	7.5	Documented information		
	7.5.1	General	1.1.1	
	7.5.2	Creating and updating	1.1.1, 2.2	

	7.5.3	Control of documented information	2.2	
	8	Operation		
	8.1	Operational planning and control	1, 2, 23	
	8.2	Information security risk assessment	1.1.1, 1.1.2	
	8.3	Information security risk treatment	1.1.1, 2.2	
	9	Performance evaluation		
	9.1	Monitoring, measurement, analysis and evaluation	1.1.1, 1.1.2	
	9.2	Internal audit	1.1.1, 2.2, 2.3.3	
	9.3	Management review	1.1, 2.3	
	10	Improvement		
	10.1	Nonconformity and corrective action	1, 2	
	10.2	Continual improvement	1.1	
		<b>Annex A</b>		
Information Security Policy	A.5.1	Management direction for information Security	1	
	A.5.1.1	Policies for information security	1	
	A.5.1.2	Review of the policies for information security	1.1.2 2.3	
Organisation of Information security	A.6.1	Internal organisation	2 2.2	
	A.6.1.1	Information security roles and responsibilities	1.2, 2, 3, 3.2, Asset register	
	A.6.1.2	Segregation of Duties	3.2	
	A.6.1.3	Contact with authorities		N/A
	A.6.1.4	Contact with special interest groups		N/A
	A.6.1.4	Authorisation process for information processing facilities	24.3	
	A.6.1.5	Information security in project management		
	A.6.2	Mobile Devices and Teleworking	10,10.1	

	A.6.2.1	Mobile device policy	10.3,10.4	
	A.6.2.2	Teleworking	10.3	
Human Resource Security	A.7.1	Prior to employment	Staff Handbook	
	A.7.1.1	Screening	Staff Handbook	
	A.7.1.2	Terms and conditions of employment	28.2 Staff Handbook	
	A.7.2	During employment		
	A.7.2.1	Management responsibilities	11.3	
	A.7.2.2	Information security awareness, education and training	11.5	
	A.7.2.3	Disciplinary process	1.2, 11.4.3, 12.2, 12.3, 12.4.2, 12.6.10, 15.2, 15.3.1, 17.2.1-4, 17.3.2-6, 28.3.1, 28.3.2, 20.4.4, Appendix C	
	A.7.3	Termination and change of employment		
	A.7.3.1	Termination or change of employment responsibilities	Staff handbook	
Asset Management	A.8.1	Responsibility for assets	8	
	A.8.1.1	Inventory of assets	8	
	A.8.1.2	Ownership of assets	8.2, 8.3	
	A.8.1.3	Acceptable use of assets	8, 8.2.1, 8.2.2, 8.2.3, 8.2.4	
	A.8.1.4	Return of assets	6.8.1, 9.3, Appendix B	
	A.8.2	Information classification	8.4	
	A.8.2.1	Classification of information	8.2.1, 8.2.2 8.2.3,8.4,4.2	
	A.8.2.2	Labelling of information	Appendix A Appendix B Appendix C	
	A.8.2.3	Handling of assets	13.5 Appendix B	

	A.8.3	Media handling	13.4	
	A.8.3.1	Management of removable media	13.4, 6.8	
	A.8.3.2	Disposal of media	13.4	
	A.8.3.3	Physical media in transit	19.3	
Access control	A.9.1	Business Requirement of Access Control	11, 11.1	
	A.9.1.1	Access control Policy	11.2	
	A.9.1.2	Access to networks and network services	20.3.1	
	A.9.2	User Access Management	11.3	
	A.9.2.1	User registration and de-registration	11.3.1	
	A.9.2.2	User access provisioning	11.3.2, 20.4.4.2	
	A.9.2.3	Management of privileged access rights	11.3.2, 20.4.4.2	
	A.9.2.4	Management of secret authentication information of users	20.4.5.1	
	A.9.2.5	Review of user access rights	5.2, 11.3.3, 20.4.4.3	
	A.9.2.6	Removal or adjustment of access rights	10.3, 10.8, 11.3.1, 20.4.4.3	
	A.9.3	User Responsibilities	1.1.4, 1.2, 11.4	
	A.9.3.1	Use of secret authentication information	11.4.3, 20.4.5.1	
	A.9.4	System and Application Access control	20.3,20.3.1	
	A.9.4.1	Information access restriction	20.5.2	
	A.9.4.2	Secure log-on procedures	11.4, 20.4.5.2	
	A.9.4.3	Password management system	11.4.2,11.4.3	
	A.9.4.4	Use of privileged utility programs	20.4.6	
	A.9.4.5	Access control to program source code	23.4	
	A.10	Cryptography		
	A.10.1	Cryptographic controls		NCEPOD does not use a system of public/private key encryption, so controls for handling keys are not appropriate

	A.10.1.1	Policy on the use of cryptographic controls		As above
	A.10.1.2	Key management		As above
Physical and Environmental Security	A.11.1	Secure areas	5.1	
	A.11.1.1	Physical security Perimeter	5.2	Physical security perimeters are controlled by the landlord. Further definition of security perimeters is not necessary, given other security controls defined in the procedures.
	A.11.1.2	Physical entry controls	5.2	
	A.11.1.3	Securing offices, rooms and facilities	5.2	Physical security maintained under 5.2
	A.11.1.4	Protecting against external and environmental threats	5	
	A.11.1.5	Working in secure areas	5.2	
	A.11.1.6	Delivery and loading areas	N/A	Controlled by the landlord
	A.11.2	Equipment	6, 6.1	
	A.11.2.1	Equipment siting and protection	6.2	
	A.11.2.2	Support utilities	6.3	
	A.11.2.3	Cabling security	6.4	NCEPOD has limited control over this, but is compliant within all reasonable measures
	A.11.2.4	Equipment maintenance	6.6	
	A.11.2.5	Removal of assets	6.9	
	A.11.2.6	Security of equipment and assets off-premises	6.9	
	A.11.2.7	Secure disposal or reuse of equipment	6.7, 6.8, 6.10	
	A.11.2.8	Unattended user equipment	6.11	
	A.11.2.9	Clear desk and clear screen policy	6.8, 7.2	
Operations Security	A.12.1	Operational procedures and responsibilities	23.1	
	A.12.1.1	Documented operating procedures	23.2	
	A.12.1.2	Change management	23	
	A.12.1.3	Capacity management	25.2	
	A.12.1.4	Separation of development, testing and operational environments	23.4	

	A.12.2	Protection from Malware		
	A.12.2.1	Controls against malware	15.2,15.3,15.4	
	A.12.3	Backup		
	A.12.3.1	Information backup	13.2	
Communications and Operations Management	A.12.4	Logging and monitoring		
	A.12.4.1	Event logging		Not necessary given the size of NCEPOD
	A.12.4.2	Protection of log information		Not necessary given the size of NCEPOD
	A.12.4.3	Administrator and operator logs		Not necessary given the size of NCEPOD
	A.12.4.4	Clock synchronisation	21.5	
	A.12.5	Control of operational software		
	A.12.5.1	Installation of software on operational systems	22.2	
	A.12.6	Technical vulnerability management	12	
	A.12.6.1	Management of technical vulnerabilities	12	
	A.12.6.2	Restrictions on software installation	15.3.2	
	A.12.7	Information system audit considerations	2.3.2	
	A.12.7.1	Information system audit controls	2.3.2	
Communications security	A.13.1	Network Security Management	20,20.1	
	A.13.1.1	Network controls	20.2,20.3,20.4,20.5	
	A.13.1.2	Security of network services	20	
	A.13.1.3	Segregation in networks		Inappropriate control given the size of NCEPOD, and the absence of an extranet
	A.13.2	Information transfer	18,18.1	
	A.13.2.1	Information transfer policies and procedures	18.2	
	A.13.2.2	Agreements on information transfer	19, 19.2	
	A.13.2.3	Electronic messaging	18.4,17.3	
	A.13.2.4	Confidentiality or non-disclosure agreements	28.2	

System acquisition, development and maintenance	A.14.1	Security requirements of information systems		
	A.14.1.1	Information security requirements analysis and specification	14.2	
	A.14.1.2	Securing application services on public networks		Not applicable given the nature of NCEPOD
	A.14.1.3	Input data validation	14.2	Not applicable given the nature of NCEPOD
	A.14.2	Security in development and support processes	23, 23.1	
	A.14.2.1	Secure development policy	15.2, 15.3	
	A.14.2.2	System change control procedures	23.2	
	A.14.2.3	Technical review of applications after operating system changes	23.3	
	A.14.2.4	Restrictions on changes to software packages	23.4	
	A.14.2.5	Secure system engineering principles	Can't find anything on this	
	A.14.2.6	Secure development environment	22.4	
	A.14.2.7	Outsourced development	23.6	NCEPOD does not outsource the development of its core applications software, so escrow agreements are unnecessary
	A.14.2.8	System security testing	Can't find anything on this	
	A.14.2.9	System acceptance testing	25.4	
	A.14.3	Test data		
	A.14.3.1	Protection of test data	22.3	
Supplier Relationships	A.15.1	Information security in supplier relationships		
	A.15.1.1	Information security policy for supplier relationships	9.3	
	A.15.1.2	Addressing security within supplier agreements	9.3	

	A.15.1.3	Information and communication technology supply chain	9.2	
	A.15.2	Supplier Service Delivery Management	9.2	
	A.15.2.1	Monitoring and review of supplier services	9.2, 9.3	
	A.15.2.2	Manage changes to supplier services		Not applicable. Due to few third-party agreements. This control is not necessary
Information Security Incident Management	A.16.1	Management of Information Security Incidents and Improvements	12	
	A.16.1.1	Responsibilities and procedures	12.3, 12.6	
	A.16.1.2	Reporting information security events	12.4.1	
	A.16.1.3	Reporting information security weaknesses	12.4.2	
	A.16.1.4	Assessment of and decision on information security events	12.6	
	A.16.1.5	Response to information security events	12	
	A.16.1.6	Learning from information security incidents	12	
	A.16.1.7	Collection of evidence		Not applicable
Information security aspects of business continuity management	A.17.1	Information security continuity	16, 16.1	
	A.17.1.1	Planning information security continuity	16.3.1	
	A.17.1.2	Implementing information security in continuity	16.3.1, 16.3.2, Appendix D	
	A.17.1.3	Verify, review and evaluate information security continuity	16.4, Appendix D	
	A.17.2	Redundancies		
	A.17.2.1	Availability of information processing facilities		
Compliance	A.18.1	Compliance with legal and contractual requirements	28, 28.1	

	A.18.1.1	Identification of applicable legislation and contractual requirements	28.2	
	A.18.1.2	Intellectual Property Rights (IPR)	28.3	
	A.18.1.3	Protection of records	28.4	
	A.18.1.4	Privacy and protection of personally identifiable information	28.5	
	A.18.1.5	Regulation of cryptographic controls		NCEPOD does not use a system of public/private key encryption, so regulations for the use of cryptographic controls are not applicable.
	A.18.2	Information Security Reviews	2.3.2	
	A.18.2.1	Independent review of information security	2.3.2 12.3	
	A.18.2.2	Compliance with security policies and standards	2.3.2	
	A.18.2.3	Technical compliance review	2.3.3	