INFORMATION TECHNOLOGY SECURITY POLICY

Policy Type	Non Clinical
Directorate	Corporate
Policy Owner	Director of Finance, Estates and IM&T
Policy Author	Deputy Director of IM&T/Interim Head of ICT
Next Author Review Date	1st January 2023
Approving Body	Policy Management Sub-Committee 24th June 2019
Version No.	4.0
Policy Valid from date	1st June 2019
Policy Valid to date:	30th June 2023

'During the COVID19 crisis, please read the policies in conjunction with any updates provided by National Guidance, which we are actively seeking to incorporate into policies through the Clinical Ethics Advisory Group and where necessary other relevant Oversight Groups'

DOCUMENT HISTORY

(Procedural document version numbering convention will follow the following format. Whole numbers for approved versions, e.g. 1.0, 2.0, 3.0 etc. With decimals being used to represent the current working draft version, e.g. 1.1, 1.2, 1.3, 1.4 etc. For example, when writing a procedural document for the first time – the initial draft will be version 0.1)

Date of Issue	Version No.	Date Approved	Director Responsible for Change	Nature of Change	Ratification / Approval
26 Mar 12	1.0	26 Mar 12	Executive Director of Transformation and Integration		Approved at Provider Executive Board
14 Jan 15	1.1		Executive Director of Transformation and Integration		Ratified at Information Governance Steering Group
06 Feb 15	1.1		Executive Director of Transformation and Integration	Minor Amendments	
23 Feb 15	1.2		Executive Director of Transformation and Integration	Via Voting Buttons	Ratified at Risk Management Committee
17 Mar 15	2	17 Mar 15	Executive Director of Transformation and Integration		Approved at Policy Management Group
19 Feb 16	2.1		Executive Director of Transformation and Integration	Minor amendments to document structure	
22 Feb 16	2.1		Executive Director of Transformation and Integration	Minor amends by Information Security Manager to comply with IG Toolkit requirements	Ratified at Policy Management Group
25 Feb 16	3.0	25 Feb 16	Executive Director of Transformation and Integration	Minor amends by Information Security Manager to comply with IG Toolkit requirements	Approved at Trust Executive Committee
May 2019	3.1		Director of Finance, Estates and IM&T	Policy review	
13 Jun 19	3.1		Director of Finance, Estates and IM&T	Endorsed at	Information Governance Sub-Committee
24 Jun 19	4.0	24 June 19	Director of Finance, Estates and IM&T	Approved at	Policy Management Sub-Committee
29 Jan 21	4.0	24 June 19	Director of Finance, Estates and IM&T	12 month blanket policy extension due to covid 19 applied with author review date set 180 days prior to Valid to Date.	Quality & Performance Committee
11 May 21	4.0	24 June 19	Director of Finance, Estates and IM&T	Extended policy uploaded and linked back with new cover sheet	Corporate Governance

NB This policy relates to the Isle of Wight NHS Trust hereafter referred to as the Trust

Contents

1 Executive Summary

1.1 This document sets out the Trust policy for the protection of the confidentiality, integrity and availability of the computer network and its resources. It establishes the security responsibilities for IT security. It provides reference to documentation relevant to this policy.

2 Introduction

2.1 The aim of this policy is to ensure the security of the Trust's network. To do this the Trust will:

- Preserve integrity of the computer network
- Protect the computer network and its resources from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets.
- Preserve confidentiality
- Protect assets against unauthorised disclosure.

3 Key Definitions

3.1 **Configuration Management** - focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life.

3.2 **Computer Network** – refers to all the IT resources of the Trust (the Data centre, the wired and wireless networks, desktop pcs, servers etc.)

4 Scope

This policy applies to all information, information systems, networks, applications, locations and staff of the Isle of Wight NHS Trust or supplied under contract to it

5 Roles and Responsibilities

5.1 Chief Executive

The Chief Executive has delegated the overall responsibility for security, policy and implementation to the Senior Information Risk Officer (SIRO).

5.2 Senior Information Risk Officer (SIRO)

5.2.1 The SIRO is responsible for managing information risk in the Trust and will implement and lead the NHS IG risk assessment and management of information risk via the Information Risk Management Structure. They will also advise the Trust Board and other relevant committees on the effectiveness of the Information Governance Framework and provide written advice to the Accountable Officer regarding the information risk elements of their Annual Governance Statement.

The SIRO will advise the Trust on matters relating to IG Risk and Information Security.

5.3 Deputy Director of IM&T

5.3.1 The Deputy Director of IM&T has overall responsibility for the ICT services provided to the Trust and to ensure that polices are procedures are in place and adhered to within the department.

5.3.2 The Deputy Director of IM&T has delegated the responsibility for Information / IT Security implementation and monitoring to the Information Security Manager.

5.4 Information Security Manager

5.4.1 The Information Security Manager will;

5.4.1.1 Recommend effective security countermeasures.

5.4.1.2 Act as a central point of contact on information security within the Trust, for both staff and external organisations.

5.4.1.3 Implement an effective framework for the management of security based upon the requirements of ISO27001.

5.4.1.4 Produce Trust standards, procedures and guidance on Information Security matters for approval by the Information User Group.

5.4.1.5 Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.

5.4.1.6 Liaise with external organisations on information security matters, including representing the Trust on cross-community committees.

5.4.1.7 Create, maintain, provide guidance on and oversee the implementation of IT Security.

5.4.1.8 Represent the Trust on internal and external committees that relate to IT security.

5.4.1.9 Ensure that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.

5.4.1.10 Ensure that access to the Trust's computer network is limited to those who have the necessary authority and clearance.

5.4.1.11 Provide advice and guidance to development teams to ensure that the policy is complied with.

5.4.1.12 Approve system security policies for the infrastructure and common services.

5.4.1.13 Approve tested systems and agree rollout plans.

5.4.1.14 Provide a central point of contact on IT security issues.

5.4.1.15 Provide advice and guidance on:

- Policy Compliance
- Incident Investigation
- IT Security Awareness
- IT Security Training

- IT Systems Accreditation
- Security of External Service Provision
- Contingency Planning for IT systems

5.4.1.16 Review proposals that have been made to connect the Trust's systems, applications or networks to systems, applications or networks that are operated by external organisations.

5.4.1.17 Disseminate advice of external sources / authorities on IT security matters.

5.4.1.18 Review, and arrange implementation where required, of HSCIC 'CareCert' CyberSecurity recommendations and security alerts.

5.5 Information Governance Lead Responsibilities

5.5.1 To ensure that appropriate Data Protection Act 2018 notifications are maintained for information stored on the network.

5.5.2 Dealing with enquires, from any source, in relation to the Data Protection Act 2018 and facilitating Subject Access Requests.

5.5.3 Advising users of information systems, applications and networks of their responsibilities under the Data Protection Act 2018, which may include Subject Access Requests.

5.5.4 Advising the Deputy Director of IM&T on breaches of the Data Protection Act 2018 and recommended actions.

5.5.5 Encouraging, monitoring and checking compliance with the Data Protection Act 2018.

5.5.6 Liaising with external organisations regarding Data Protection Act 2018 matters.

5.5.7 Promoting awareness and providing guidance and advice related to the Data Protection Act 2018 as it applies within the Trust.

5.6 Information Asset Owners (IAO) Responsibilities

5.6.1 Ensuring the security of the network, that is information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.

5.6.2 Ensuring that their staff are made aware of their security responsibilities.

5.6.3 Ensuring that their staff have had appropriate security training.

5.7 User Responsibilities

5.7.1 All personnel or agents acting for the Trust have a duty to:

- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the Trust's IT systems.
- Report on any suspected or actual breaches in security.

5.7.2 All users accessing the computer network will have their own unique user identification and password.

5.7.3 Users are responsible for ensuring their password is kept secret.

5.7.4 User access rights will be immediately revoked or reviewed for those users who have left the Trust or changed roles.

5.7.5 Users are responsible for ensuring that they save their own data to the designated network storage area.

5.7.6 Users must ensure that they protect the computer network from unauthorised access. They must log off the computer network when finished working.

6 Policy detail/Course of Action

6.1 The overall Information Technology Security Policy for the Trust is described below:

6.2 The Trust's computer network will be available when needed, can be accessed only by authorised users and will contain complete and accurate information. The computer network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, the Trust will undertake to the following:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its computer network assets.
- Implement the Information Technology Security Policy in a consistent, timely and cost effective manner.

6.3 Where relevant, the Trust will comply with:

- Copyright, Designs & Patents Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Data Protection Act 2018
- The Human Rights Act 2018
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

6.3.1 The Trust will comply with other laws and legislation as appropriate.

6.3.2 The policy must be approved by the Deputy Director of IM&T, prior to the formal ratification and approval route.

6.4 Physical & Environmental Security

6.4.1 Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

6.4.2 Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

6.4.3 The Deputy Director of IM&T is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if he/she suspects the code has been compromised.

6.4.4 Critical or sensitive network equipment will be protected from power supply failures.

6.4.5 Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.

6.4.6 Smoking, eating and drinking is not permitted in areas housing critical or sensitive network equipment.

6.4.7 All visitors to secure network areas must be authorised by the Deputy Director of IM&T, following a risk assessment.

6.4.8 All visitors to secure network areas must be made aware of network security requirements.

6.4.9 All visitors to secure network areas must be signed in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

6.4.10 The Deputy Director of IM&T will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

6.4.11 For further details see Network operating procedure.

6.5 Access Control to Secure Network Areas

6.6 Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose role requires it. The Deputy Director of IM&T will maintain and periodically review a list of those with unsupervised access.

See service delivery procedure.

6.7 Access Control to the Network

6.7.1 Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.

6.7.2 There must be a formal, documented user registration and de-registration procedure for access to the network.

6.7.3 Departmental managers must approve user access.

6.7.4 Access rights to the network will be allocated on the requirements of the user's role.

6.7.5 Security privileges (i.e. 'superuser' or network administrator rights) to the network will be allocated on the requirements of the user's role.

6.8 Third Party Access Control to the Network

6.8.1 Third party access to the network will be based on a formal contract that satisfies all necessary NHS security conditions.

6.8.2 All third party access to the network must be auditable.

See network operating procedure.

6.9 External Network Connections

6.9.1 The Deputy Director of IM&T is responsible for ensuring that all connections to external networks and systems conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance.

6.9.2 The Deputy Director of IM&T must approve all connections to external networks and systems before they commence operation.

6.10 Maintenance Contracts

6.10.1 The Deputy Director of IM&T will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the IT Department's Asset register.

6.11 Data and Software Exchange

6.11.1 Formal agreements for the exchange of data and software between organisations must be established and approved by the Information Asset Owners.

6.12 Fault Logging

6.12.1 The Deputy Director of IM&T is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A report of any faults and review of countermeasures will be taken to the IT User Group.

6.13 Security Operating Procedures (SyOps)

6.13.1 The Deputy Director of IM&T is responsible for producing Security Operating Procedures (SyOps) and security contingency plans that reflect this Information Security Policy. Where appropriate will co-ordinate with the Local Security Management Specialist (LSMS) so that a robust and integrated security systems SyOps can be developed, which will take into account National Security Intelligence which the LSMS is privy to.

6.13.2 Changes to operating procedures must be authorised by the Deputy Director of IM&T.

6.14 Network Operating Procedures

6.14.1 The Deputy Director of IM&T is responsible for documented operating procedures for the operation of the computer network and its resources, to ensure its correct, secure operation.

6.14.2 Changes to operating procedures must be authorised by the Deputy Director of IM&T.

6.15 Data Backup and Restoration

6.15.1 The Deputy Director of IM&T is responsible for ensuring that backup copies of network configuration, network storage and server data are taken regularly.

6.15.2 All backup tapes will be stored securely in the fire proof safes.

6.16 Business Continuity & Disaster Recovery Plans

6.16.1 The Deputy Director of IM&T is responsible for ensuring that business continuity plans and disaster recovery plans are produced for the network.

6.17 Unattended Equipment and Clear Screen

6.17.1 The Trust operates a clear screen policy that means users must ensure that workstations are locked or logged off if a workstation is left unattended. Users failing to comply may be subject to disciplinary action.

7 Consultation

7.1.1 During February and March of 2015, this policy was reviewed by the IT Seniors Team meeting for discussion and consultation, Information Governance Steering Group and Risk management Group. The recommendation from the latter was that a review should take place in six months' time to reflect additional policies currently in production (Agile Worker for example). This iteration of the Policy, was considered at the Policy Management Group, prior to submission to the Trust Executive Committee for final approval

8 Training

8.1.1 This Information Technology Security Policy does not have a mandatory training requirement.

8.1.2 The Trust will ensure that all users of the computer network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

8.1.3 All users of the computer network must be made aware of the contents and implications of the Information Technology Security Policy.

8.1.4 Key responsibilities contained in the Information Technology Security policy will be covered by the Information Governance training provided to all staff.

8.1.5 Irresponsible or improper actions by users may result in disciplinary action(s). See HR Policy 'Disciplinary and Dismissal Policy and procedure' for further details.

9 Monitoring Compliance and Effectiveness

9.1 Security Audits

9.1.1 The Deputy Director IM&T / Information Security Manager will perform auditable checks on the implementation of published security policies.

9.1.2 Any serious risks identified will be reported to the Information Governance Steering Group for awareness.

9.2 Malicious Software

9.2.1 ICT team will provide reports on the measures in place to detect and protect the computer network from viruses and other malicious software

9.3 Secure Disposal or Re-use of Equipment

9.3.1 Where equipment is being disposed of, IT Department staff must ensure that all data on the equipment (e.g. on hard disks or tapes) is securely overwritten. Where this is not possible IT Department staff should physically destroy the disk or tape.

9.3.2 Ensure that where disks are to be removed from the premises for repair, where possible, the data is securely overwritten by the IT Department.

9.3.3 See ICT equipment disposal procedures for more information.

9.4 System Change Control

9.4.1 Ensure that the Deputy Director of IM&T reviews changes to the security of the computer network. All such changes must be reviewed and approved by the Deputy Director of IM&T. The IT Team leaders are responsible for updating all relevant design documentation, security operating procedures and computer network operating procedures appertaining to their specialty.

9.4.2 The Deputy Director of IM&T may require checks on, or an assessment of the actual implementation based on the proposed changes.

9.4.3 The Deputy Director of IM&T is responsible for ensuring that selected hardware or software meets agreed security standards.

9.4.4 As part of acceptance testing of all new computer network systems, the IT department with the permission of the IT Manager will attempt to cause a security failure and log other criteria against which tests will be undertaken prior to formal acceptance.

9.4.5 Testing facilities will be used for all new computer network systems. Development and operational facilities will be separated.

9.5 Security Monitoring

9.5.1 Ensure that the computer network is monitored for potential security breaches. All monitoring will comply with current legislation.

9.6 Reporting Security Incidents & Weaknesses

9.6.1 All potential security breaches must be investigated and reported to the Deputy Director of IM&T. Security incidents and weaknesses must be reported in accordance with the requirements of the Trust's incident reporting procedure.

9.7 System Configuration Management

9.7.1 Ensure that there is an effective configuration management system for the computer network.

10 Links to other policies and documents

- Network Operating Procedure
- Service Delivery Procedure
- HR Policy 'Disciplinary and Dismissal Policy and procedure'
- Incident reporting procedure
- ICT equipment disposal

11 References

- Copyright, Designs & Patents Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Data Protection Act 2018
- The Human Rights Act 2018
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

12 Appendices

- Appendix A - Financial and Resourcing Impact Assessment on Policy Implementation
- Appendix B - Equality Impact Assessment (EIA) Screening Tool

Appendix A

Financial and Resourcing Impact Assessment on Policy Implementation

NB this form must be completed where the introduction of this policy will have either a positive or negative impact on resources. Therefore this form should not be completed where the resources are already deployed and the introduction of this policy will have no further resourcing impact.

Document title	**Information Technology Security Policy**

Please note this policy will result in no change in resources and as such this section has not been completed.

Totals	**WTE**	**Recurring £**	**Non Recurring £**
Manpower Costs			
Training Staff			
Equipment & Provision of resources			

Summary of Impact:

Risk Management Issues:

Benefits / Savings to the organisation: Equality Impact Assessment

- Has this been appropriately carried out? YES/NO
- Are there any reported equality issues? YES/NO

If "YES" please specify:

Use additional sheets if necessary

Please include all associated costs where an impact on implementing this policy has been considered. A checklist is included for guidance but is not comprehensive so please ensure you have thought through the impact on staffing, training and equipment carefully and that ALL aspects are covered.

Manpower	**WTE**	**Recurring £**	**Non-Recurring £**
Operational running costs			
Totals:			

Staff Training Impact	**Recurring £**	**Non-Recurring £**
Totals:		

Equipment and Provision of Resources	Recurring £ *	Non-Recurring £ *
Accommodation / facilities needed		
Building alterations (extensions/new)		
IT Hardware / software / licences		
Medical equipment		
Stationery / publicity		
Travel costs		
Utilities e.g. telephones		
Process change		
Rolling replacement of equipment		
Equipment maintenance		
Marketing – booklets/posters/handouts, etc		
Totals:		

- Capital implications £5,000 with life expectancy of more than one year.

Funding /costs checked & agreed by finance:	
Signature & date of financial accountant:	
Funding / costs have been agreed and are in place:	
Signature of appropriate Executive or Associate Director:	

Appendix B

Equality Impact Assessment (EIA) Screening Tool

Document Title:	Information Technology Security Policy
Purpose of document	*This document sets out the Trust policy for the protection of the confidentiality, integrity and availability of the computer network and its resources.*
Target Audience	*All staff*
Person or Committee undertaken the Equality Impact Assessment	*Information Security Manager*

1. To be completed and attached to all procedural/policy documents created within individual services.

2. Does the document have, or have the potential to deliver differential outcomes or affect in an adverse way any of the groups listed below?

If no confirm underneath in relevant section the data and/or research which provides evidence e.g. JSNA, Workforce Profile, Quality Improvement Framework, Commissioning Intentions, etc.

If yes please detail underneath in relevant section and provide priority rating an determine if full EIA is required.

		Positive Impact	**Negative Impact**	**Reasons**
Gender	Men	*Not applicable*	*Not applicable*	
	Women	*Not applicable*	*Not applicable*	
Race	Asian or Asian British People	*Not applicable*	*Not applicable*	
	Black or Black British People	*Not applicable*	*Not applicable*	
	Chinese people	*Not applicable*	*Not applicable*	
	People of Mixed Race	*Not applicable*	*Not applicable*	
	White people (including Irish people)	*Not applicable*	*Not applicable*	

	People with Physical Disabilities, Learning Disabilities or Mental Health Issues	*Not applicable*	*Not applicable*	
Sexual Orientation	Transgender	*Not applicable*	*Not applicable*	
	Lesbian, Gay men and bisexual	*Not applicable*	*Not applicable*	
Age	Children	*Not applicable*	*Not applicable*	
	Older People (60+)	*Not applicable*	*Not applicable*	
	Younger People (17 to 25 yrs)	*Not applicable*	*Not applicable*	
Faith Group		*Not applicable*	*Not applicable*	
Pregnancy & Maternity		*Not applicable*	*Not applicable*	
Equal Opportunities and/or improved relations		*Not applicable*	*Not applicable*	

Notes:

Faith groups cover a wide range of groupings, the most common of which are Buddhist, Christian, Hindus, Jews, Muslims and Sikhs. Consider faith categories individually and collectively when considering positive and negative impacts.

The categories used in the race section refer to those used in the 2001 Census. Consideration should be given to the specific communities within the broad categories such as Bangladeshi people and the needs of other communities that do not appear as separate categories in the Census, for example, Polish.

3. Level of Impact

If you have indicated that there is a negative impact, is that impact:			
		YES	**NO**
Legal (it is not discriminatory under anti-discriminatory law)			
Intended			

If the negative impact is possibly discriminatory and not intended and/or of high impact then please complete a thorough assessment after completing the rest of this form.

3.1 Could you minimise or remove any negative impact that is of low significance? Explain how below:
3.2 Could you improve the strategy, function or policy positive impact? Explain how below:

3.3 If there is no evidence that this strategy, function or policy promotes equality of opportunity or improves relations – could it be adapted so it does? How? If not why not?	
Scheduled for Full Impact Assessment	Date:
Name of persons/group completing the full assessment.	
Date Initial Screening completed	