INFORMATION TECHNOLOGY NETWORK SECURITY POLICY

Policy Type	Non Clinical
Directorate	Corporate
Policy Owner	Director of Finance, Estates and IM&T
Policy Author	Information Security Manager
Next Author Review Date	1st January 2023
Approving Body	Policy Management Sub-Committee 24th June 2019
Version No.	2.0
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
	1.0		Executive Director of Transformation and Integration	New Policy	Ratified at Policy Management Group
17 Mar 16	1	16 Mar 16	Executive Director of Transformation and Integration	New Policy	Approved Trust Executive Committee
May 2019	1.1		Director of Finance, Estates and IM&T	Policy review	
13 Jun19	1.1		Director of Finance, Estates and IM&T	Endorsed at	Information Governance Sub-Committee
24 Jun 19	2.0	24 Jun 19	Director of Finance, Estates and IM&T	Approved at	Policy Management Sub-Committee
29 Jan 21	2.0	24 Jun 19	Director of Finance, Estates and IM&T	12 month blanket policy extension due to covid 19 applied with author review date set 6 months prior to Valid to Date.	Quality & Performance Committee
11 May 21	2.0	24 Jun 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 4
2 Introduction 4
3 Definitions 4
4 Scope 4
5 Purpose 4
6 Roles and Responsibilities 5
7 Policy detail/Course of Action 7
8 Consultation 11
9 Training 11
10 Monitoring Compliance and Effectiveness 11
11 Links to other Organisational Documents 12
12 Appendices 12

1 Executive Summary

1.1 This policy defines the controls applied to the Trust's IT network to help ensure the confidentiality, integrity and availability of information which flows over it, to ensure compliance with the Data Protection Act 2018 and the Data Security & Protection Toolkit.

2 Introduction

2.1 This document sets out the Network Security arrangements for the Isle of Wight NHS Trust. The Policy applies to all staff working directly for the Trust, and any organisation that has entered into an agreement for the provision of ICT services by the Trust.

3 Definitions

3.1 **Computer Network** – refers to physical (i.e. PC plugged into wall port) and wireless (wi-fi) networks, and all supporting infrastructure.

4 Scope

4.1 This policy applies to all Networks used for:

- The storage, sharing and transmission of clinical and non-clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images

4.2 The aim of this policy is to ensure the security of the Trust's Network and to do this, the organisation will:

- Ensure the protection of the network from unauthorised access, and protect information from unauthorised disclosure and accidental modification.
- Ensure the accuracy and completeness of the organisation's IT assets

4.3 The term 'Network' relates to the physical wired and wireless networks provided by the Trust as well as the computer domains (e.g. STMARYSLAN) to which users connect.

5 Purpose

5.1 The purpose of this Policy is to set out the process to be used to enable staff to use the network in a responsible and appropriate way, including:-

- Understanding their responsibilities when accessing the network

- Understanding the possible implications and risk/possible damage to the organisation's reputation of using the network inappropriately.

6 Roles and Responsibilities

6.1 Senior Information Risk Officer (SIRO)

6.1.1 The SIRO is responsible for managing information risk across 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 Trusts Information Governance (IG) arrangements/framework and provide written advice to the Accountable Officer regarding the information risk elements of their Annual Governance Statement.

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

6.1.3 The SIRO has ultimate responsibility for ensuring compliance with this policy across the breadth of the Trust.

6.2 Deputy Director of Information Management & Technology (IM&T)

6.2.1 The Deputy Director of IM&T has operational responsibility for overseeing the implementation of Network security processes and procedures that are applicable across the Trust, in particular within the Information Communication Technology department, and ensuring that appropriate documentation is in place to support this, including this policy.

6.3 Information Communication Technology (ICT) Network Manager

6.3.1 The ICT Network manager oversees day-to-day operation of the trust's network. They are responsible for, working in conjunction with the Information Security Manager, providing a secure network in line with the business requirements of the Trust.

6.4 Information Security Manager

6.4.1 The responsibilities of the Information Security Manager will include:

- Acting as a central point of contact on information security within the organisation and for external organisations that has entered into an agreement for the provision of ICT services by the Trust.
- Implementing an effective framework for the management of information security.
- Assisting in the formulation of Information Security Policy and related policies.
- Advise on the content and implementation of the Information Security Programme.

- Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on information security matters, including representing the organisation on cross-community committees.
- Advising users of information systems, applications and Networks of their responsibilities.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk, or where risks are identified these are managed in line with the Trusts Risk Management Strategy and Policy.
- Ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

6.5 Information Asset Owners (IAOs)

6.5.1 Information Asset Owners (IAOs) are senior members of staff (Service Leads) responsible for information risks within their service areas. They are responsible for providing assurance to the SIRO that information risks are, identified, recorded and that controls are in place to mitigate those risks. IAOs will work closely with the trust's Information Governance team, Information Communication Technology team, and Information Security Manager to ensure that:

- Security of the Network used by their staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Their staff are made aware of their security responsibilities.
- Their staff have had suitable security training.
- An action plan and action outcome is developed in the event of a breach to the trust's Networks.

6.5.2 The Information Asset Owner will seek to minimize risk by ensuring that appropriate reviews and plans are in place to mitigate risks. This will include business continuity planning.

6.6 Information Asset Administrators (IAA)

6.6.1 IAOs can chose to appoint an Information Asset Administrator (IAA) to support the delivery of information risk management responsibilities within their service areas. However, where they chose not to do this the Information Asset responsibilities rest with the Information Asset Owner. Information Asset Administrators should ensure that:

- Staff within their areas aware of the trust's policies and procedures and their responsibilities for the secure use of the trusts ICT systems.

- They recognise actual or potential security incidents and take steps to mitigate those risks.
- They consult with their IAOs on incident management and ensure that information asset registers are accurate and up to date.

6.7 All Permanent Staff

6.7.1 All staff and those working for the Trust have a duty, outlined in their terms and conditions of working, either individually or via their company for 3rd Party external contractors, to adhere to the principles outlined in this policy.

6.8 Non-permanent Staff

6.8.1 The same responsibilities as for permanent staff apply to those working on behalf of the organisation, whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of but not directly employed by the Trust, are required read and adhere to this policy

7 Policy detail/Course of Action

7.1 Risk Assessment

7.1.1 The Information Security Manager, working in conjunction with the Network Manager, will be responsible for risk assessing, and reporting upon, the Trust's network.

- Risk assessments will be conducted on the network annually, the scope of the risk assessment will change depending on which area of the network requires assessing.
- Risk assessments will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the Network.
- Formal risk assessments will be conducted using CRAMM methodologies and will conform to ISO27001 standards.
- Regular vulnerability assessments / penetration tests will be performed to ensure compliance with defined controls.

7.2 Physical and Environmental Security

- 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.
- All public network facing firewalls will be accredited to Common Criteria EAL4 / Protection Profile compliant as a minimum.
- All unused network ports will be unpatched to minimise the likelihood of unauthorised equipment being connected to the network.
- Areas which are controlled with secure key-code locks will be periodically changed, following a compromise of code or when a member of staff leaves.

- Critical or sensitive Network equipment will be protected from power supply failures.
- Critical or sensitive Network equipment will be protected by intruder alarms and/or CCTV and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive Network equipment.
- All visitors to secure Network areas must be authorised by a senior member of the IT department.
- All visitors to secure Network areas must be made aware of Network security requirements.
- All visitors to secure Network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
- The Information Security Manager will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.
- The Information Security Manager / Network manager will receive, and action, Cyber Security 'CareCERT' recommendations where applicable

7.3 Access Controls

7.3.1 Access to Secure Network Areas – Trust Staff

- Access to secure network areas is restricted to only those staff who need access to the area as part of their role.
- Access to secure areas are regularly reviewed and ensure that the list is accurate and up to date.

7.3.2 Logical Access to Network – All NHS Staff

- All access to the network must be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- Ensure a formal registration and de-registration procedure to access the network, with line manager authorisation.
- Access rights to the network must be allocated based on the user's job rather than user's status within the organisation.
- User access rights (as configured in Active Directory) will be removed or reviewed when a user leaves the organisation or changes job upon notification from the HR department.
- Security privileges must be granted to those that require the access. This access is limited to trust Staff whose role requires them to have System Administrative access.
- All users must have an individual user identification (username) and password.
- Users are responsible for ensuring that their username and password is kept safe.

- Generic/shared user identification and password will only be granted with a justifiable business requirement and must be only used for the purpose they have been created for. Approval can be sought from the IAO, Deputy Director of IM&T, or the Information Security Manager.

7.3.3 Third Party Access to the Network

- Third party access to the network will based on a formal contract that satisfies all necessary NHS, and Data Security & Protection Toolkit security conditions
- All third party access to the network will managed and logged on the Trust's Sostenuto servicedesk system.

7.3.4 Connections to External Networks

- All connections to external networks and systems conform to the Network Security policy, Code of Connection, the Electronic Communications policy and supporting guidance

7.3.5 Access via VPN (Virtual Private Network) – All NHS Staff

- The VPN token will only be issued after the completion of the user acceptance form. Completed forms are held by the IT department.
- Access will only be provided to Trust managed devices.
- All users must conform to the Acceptable Use policy (as if connected to the local network)

7.4 **Wireless network access**

7.4.1 Wireless access to the network will also be in accordance with the requirement of this policy. There will also be additional access controls via certificate and radius servers.

7.5 **Operating Procedures**

7.5.1 Data Backup and Restoration

- The Network Manager is responsible for ensuring that backup copies of Network configuration data are taken regularly.
- Documented procedures for the backup process and storage of backup tapes are produced and communicated to all relevant staff.
- Backup tapes are stored securely and copies stored off-site.
- There are documented procedures for the safe and secure disposal of IT equipment including backup media and these procedures are communicated to all relevant staff.
- The disposal of backup media follows and complies with the trust policy for decommissioning and disposal of old equipment.

7.6 **Fault Logging**

7.6.1 The Network Manager will ensure that a log of all faults on the Network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

7.7 **Business Continuity**

7.7.1 The Trust will ensure that There are existing Business Continuity and Disaster Recovery Plans for all critical systems.

7.7.2 The Business Continuity Plans and Disaster Recovery Plans are regularly reviewed and the process is tested annually.

7.7.3 The plans must be reviewed (and in the main produced) by the IAO and tested annually.

7.8 **Accreditation of Network Systems**

7.8.1 Additions to the network must be approved by the ICT Networks manager before they commence operation; ensuring that they do not pose an unacceptable security risk to the organisation and meets Information Governance Toolkit (IGT) requirements /standards.

7.9 **System Change Control**

7.9.1 The Deputy Director of IM&T will ensure that changes to the security of the Network are in line with the Trust's Business Case process.

7.9.2 Relevant Network Security Policies, design documentation, security operating procedures and Network operating procedures are updated regularly especially when changes to legislations or national guidance necessitates an early review.

7.9.3 Acceptance testing of all new Network systems is be carried out, in line Information Security requirements.

7.9.4 Any changes to network configuration must go through the Trust's Business Case process.

7.9.5 Testing facilities will be used for all new Network systems. Development and operational facilities will be separated.

7.10 **Incident – Reporting, Investigations and Resolutions**

7.10.1 All staff should ensure that they report actual/potential security incidents as soon as they become aware to the Trust's IT service desk and through the Trusts Incident Management System in line with Trust policy.

7.10.2 All incidents, investigations and resolutions will be recorded on the Service Desk system for reporting, knowledge base and future learning.

7.10.3 There may be instances where incidents are reported directly to the Security team or Information Governance due to their sensitivity. These are likely to be legal and/or forensic incidents which will be dealt with according to the Trust's Incident Management and Reporting Procedures.

7.10.4 Once reported these incidents will be reviewed by the Deputy Director of IM&T and where appropriate the Information Governance Lead Officer.

8 Consultation

8.1.1 Prior to submission for approval, this document was circulated to the IM&T team, and the Information Governance team for their comments to be included.

9 Training

9.1 This IT Network Security Policy does not have a mandatory training requirement or any other training needs.

10 Monitoring Compliance and Effectiveness

10.1 In order to provide assurances that controls in place are working effectively, the Information Security Manager will work closely with the, Trust's, IM&T team and the IG team to ensure that audits of systems and access controls to networks are conduct on a regular basis. Examples of events that will be audited will include:

- Frequency, circumstances and location etc:
- Failed attempts to access confidential information
- Repeated attempt to access confidential information
- Shared login and passwords

10.2 The Trust will ensure that:

- There is continuous improvement in confidentiality and data protection and learning outcomes;
- All incidents are audited to ensure any recommendations made have been implemented.
- An action plan and action outcome is developed in the event of a breach to the trust's Networks.
- Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring;

10.3 The Trust will embed improvements to its Network Security and Information Governance Framework/arrangements and demonstrate it is proactive in assessing and preventing information risk.

11 Links to other Organisational Documents

11.1 The following documentation relates to the management of information and together underpins the trust's Information Governance Assurance Framework. This procedure should be read in conjunction other policies:

- Information Governance Risk Policy
- Information Technology Security Policy
- Information Security Policy
- Incident Management Policy
- Business Continuity Plans
- Business Continuity Policy

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	**IT Network Security Policy**

Totals	**WTE**	**Recurring £**	**Non-Recurring £**
Manpower Costs	**N/A.**	**N/A.**	**N/A.**
Training Staff	**N/A.**	**N/A.**	**N/A.**
Equipment & Provision of resources	**N/A.**	**N/A.**	**N/A.**

Summary of Impact: No change in resources required.

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:	IT Network 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*
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.	Stuart Collier
Date Initial Screening completed	09/03/2016