Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

INFORMATION SECURITY POLICY

POLICY

Reference	ISP-01		
Approving Body	Information Governance Committee		
Date Approved	4th April 2023		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	x		
Issue Date	April 2023		
Version	8		
Summary of Changes from Previous Version	Multi-Factor Authentication		
Supersedes	7		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Committee Information Governance Working Group		
Date of Completion of Equality Impact Assessment	1st November 2022		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Potential non-compliance with: • Computer Misuse Act 1990 • UK General Data Protection Regulation • The Network and Information Systems Regulations 2018 (UK)		
Target audience	All staff and the general public		
Review Date	April 2025		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Information Governance Manager and Data Protection Officer, Jacquie Widdowson		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Information Governance Manager and Data Protection Officer		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Password Management Procedure	January 2022

Template control	June 2020

CONTENTS

1.0 INTRODUCTION 4
2.0 POLICY STATEMENT 4
3.0 DEFINITIONS/ ABBREVIATIONS 6
4.0 ROLES AND RESPONSIBILITIES 8
5.0 APPROVAL 10
6.0 DOCUMENT REQUIREMENTS 10
6.1.1 Information Security & Confidentiality Awareness/Training 11
6.1.2 Secure Control of Information Assets 11
6.1.3 Physical Access Controls 12
6.1.4 Password and Access Control 12
6.1.5 Multi-Factor Authentication 13
6.1.6 Equipment Siting and Security 14
6.1.7 System and Network Security 15
6.1.8 Information Risk Assessment 15
6.1.9 Information Security Incident Reporting and Management 16
6.1.10 Protection from Malicious Code 16
6.1.11 Monitoring System Access and Use 17
6.1.12 Information Sharing Protocols 17
6.1.13 External Parties 17
6.1.14 Introduction & Accreditation of Information Systems 18
6.1.15 Change Control 18
6.1.16 Remote working 18
6.1.17 Transportation of Records 19
6.1.18 Encryption 20
6.1.19 Disposal of Equipment & Media 20
6.1.20 Decommissioning of applications, systems, and hardware 20
6.1.21 Business Continuity and Disaster Recovery Plans 21
6.1.22 Cyber security risk 21
6.1.23 Forensic Readiness 22
6.1.24 Digital forensic investigation 23
8.0 TRAINING AND IMPLEMENTATION 25
9.0 IMPACT ASSESSMENTS 25

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED Trust DOCUMENTS.....25

11.0 KEYWORDS.....26

12.0 APPENDICES.....26

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA) 27

APPENDIX 2 – GOOD PRACTICE GUIDE FOR STAFF.....30

1.0 INTRODUCTION

Information is one of Sherwood Forest Hospitals NHS Foundation Trust (the Trust's) most important assets. The Trust stores, processes and manages a vast amount of confidential information relating to patients, clients and employees and failure to ensure adequate security of information may lead to legal action, including financial penalties. The general public's confidence in the Trust could be compromised, adversely affecting its reputation if information is not kept safe and secure.

Keeping information secure yet available to those that need it presents a challenge. With the ease that information can flow between organisations it is important that a consistent approach is adopted to safeguard information. This policy strives to achieve a sensible balance of confidentiality, integrity and availability through the use of appropriate controls.

2.0 POLICY STATEMENT

Information systems used by the Trust represent a considerable investment. Much of the information is of a confidential and sensitive nature, and it is necessary for all information systems to have appropriate protection against any events whether accidental or malicious, which may put at risk the activities of the Trust or the investment in information.

The Trust has a responsibility to maintain the confidentiality, integrity and availability of information held both manually and digitally, and addresses the following issues:

- Confidentiality - Data is available to those with specific authority who require access; Data is not disclosed to people who do not require it.
- Integrity - is about information being accurate and up-to-date. Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Data should be complete and accurate and not tampered with during or after submission. Ensuring that during the process of transmission data integrity is maintained.
- Availability – is about information being there when it is needed to support care. System design must include appropriate access controls and checks, so that the information in the system has consistency, accuracy, can be trusted as correct and can be relied on when providing healthcare. Data is available and delivered to the right person, at the time when it is needed and that there is accessibility to systems at all times. Having safeguards in place for power outages, natural disasters, hardware failures and systems upgrades.

The Trust must also minimise the risk of security breaches and must meet the requirements for secure connection to the Health and Social Care Network (HSCN) and protect the security and confidentiality of the data that it holds.

Information Security Management is essential to the organisation and this policy addresses security management for the processing and use of NHS information. This policy is based on current legal requirements, relevant standards, and professional best practice to ensure staff understand their responsibilities towards use of their organisations information assets.

The UK GDPR requires us to process personal data securely. Article 5(1)(f) concerns 'integrity and confidentiality' of personal data - in short, it is the UK GDPR's 'security principle'. It states that personal data shall be:
'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

Article 32 which apply whether we are a data controller or a data processor. These require us to put in place appropriate technical and organisational measures to ensure an appropriate level of security of both the processing and our processing environment.

These provisions cover fundamental information security concepts including:

- minimisation of personal data collected;
- managing, limiting and controlling access to personal data;
- protecting the classic 'CIA triad' (confidentiality, integrity, and availability) of personal data;
- resilience of processing systems and services, and the ability to restore availability and access to personal data; and
- regular testing of the effectiveness of measures implemented.

The measures you implement should be appropriate to the risk presented.

Do ……

- Adhere to the Information Security Management: NHS Code of Practice
- Be aware of who you are allowed to share information with and how it is shared securely
- Report any information security incident/breaches following the Trust incident reporting procedure and Nottinghamshire Health Informatics Service (NHIS) IT via the Service Desk
- Ensure that confidential information is stored and handled securely
- All staff must complete data security awareness training on induction and annually.

Don't…...

- Ignore, turn off or bypass any information security controls put in place or recommended by the Trust or NHIS
- Send personal/sensitive data unless you know it is secure/encrypted
- Share passwords

The Trust will maintain the confidentiality, integrity and availability of information, information systems (including devices), manual records, applications, and networks for which it is responsible by:

- Ensuring that staff are aware of, and comply with, the relevant legislation as described in this and related policies and guidelines.
- Describing the principles of information security and explaining how they will be implemented in the Trust.
- Creating and maintaining a level of awareness of the need for information security as an integral part of the day to day business and ensuring staff understand their own responsibilities.
- Ensuring an acceptable level of assurance is in place where information is processed on its behalf by external third parties.
- Ensure systems, applications and networks are able to withstand or recover from threats to their Confidentiality, Integrity and Availability.
- Protecting the Trust's information.

Failure by any employee of the Trust to adhere to the policy and its guidelines may be viewed as gross misconduct and may result in disciplinary action.

3.0 DEFINITIONS/ ABBREVIATIONS

The Trust - Sherwood Forest Hospitals Foundation Hospitals Trust (SFHFT). Information Communication and Technology services are provided by Nottinghamshire Health Informatics Service (NHIS), who are hosted by Sherwood Forest Hospitals NHS Foundation Trust.

Staff - All staff (including Medirest, Skanska, agency and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Confidential information - Confidential information can be anything that relates to patients, staff or any other information (such as medical and staff records, contracts, tenders, etc.) held either in paper, disc, computer file or printout, video, photograph or even heard word of mouth. It includes information stored on portable devices such as laptops, mobile telephones and external hard drives/memory sticks). Personal information that is subject to a duty of confidence has a number of characteristics, i.e. the information:

- is not in the public domain or readily available from another source
- has a certain degree of sensitivity, (more than gossip) such as medical history
- has been provided with the expectation that it will only be used or disclosed for particular purposes. This expectation may arise because a specific undertaking has been given,

because the confider places specific restrictions on the use of data which are agreed by the recipient, or because the relationship between the recipient and the data subject generally gives rise to an expectation of confidentiality, for instance as arises between a patient and a doctor.

Information Security - The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Personal data breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised or malicious disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service. An identified weakness or vulnerability of a system or process that puts the security and availability of information at risk. A breach may be caused by a technical failure or by inappropriate actions of an individual(s).

Information Asset - An information asset is a body of information, defined and managed as a single unit (e.g. SystmOne, Microsoft Outlook) so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.

Information Asset Owner (IAO) –Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the Trust. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process..

Information Asset Administrator (IAA) – Information Asset Administrators ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents, and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, they seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Register (IAR) – An Information Asset Register (IAR) is a simple way to understand and manage the Trust's information assets and the risks to them. It is important to know and fully understand what information we hold in order to protect it and be able to exploit its potential.

Local Area Network (LAN) - a collection of devices connected together in one physical location,

Remote working - is the term used when working from a non-fixed location ie home, using mobile devices such as laptops, tablets, smartphones etc.

Cyber security - Cyber security is how individuals and organisations reduce the risk of cyber-attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

Forensic readiness planning - Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence, related monitoring and collection processes and capabilities, storage requirements and costs.

UK GDPR – United Kingdom General Data Protection Regulation

4.0 ROLES AND RESPONSIBILITIES

Trust Board

The Trust Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Information Governance Committee

The Committee is responsible for ensuring that this policy is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

Chief Executive

The Chief Executive has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee.

Senior Information Risk Owner

The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated SIRO, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The SIRO also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian

The Medical Director is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required. The Caldicott Guardian will be central to the framework for handling

person identifiable information in the NHS and will be fully aware of their responsibilities specified in the Caldicott Guardian Manual (Department of Health, 2017 Manual[1]).

Data Protection Officer

We are a public authority and have appointed a Data Protection Officer. The Data Protection Officer reports to the Senior Information Risk Owner and works with the Caldicott Guardian. The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our Data Protection Officer has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Information Asset Owners (IAOs)

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)

Information Asset Administrators ensure that IG policies and procedures are followed, recognise actual or potential IG security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Directors and Services Managers

Responsible for ensuring a comprehensive risk assessment is undertaken regarding the safety and security of the health records during transport to and from, and while present at non Trust premises. Completed risk assessments should be submitted to the Information Asset Owner for evaluation and approval by the Medical Records Advisory Group, also ensure that risk assessments are accurately maintained and risks re-evaluated and updated if significant changes are made to services.

Duty Nurse Managers

Out-of-hours or on occasions when the Caldicott Guardian, Information Governance Manager/ Data Protection Officer or Information Asset Owner are unavailable, Duty Nurse Managers in the first instance will be required to assume responsibility for any decision regarding urgent

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

disclosures that cannot be delayed, they can if necessary seek assistance from staff involved in the Gold/Silver On-Call Protocol consulting with the Trust's Legal Advisors as necessary.

All Staff

All staff (including Medirest, Skanska, agency and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Contractors and agency staff and other third parties staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of IG security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors.

Any IG security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

The Trust will investigate all suspected/actual security breaches and report through their incident reporting procedures.

5.0 APPROVAL

This policy has been approved by the Information Governance Committee.

6.0 DOCUMENT REQUIREMENTS

It is essential that the Trust's information systems and data networks are adequately protected from events that may compromise the provision of its services; to this effect the Trust is committed to developing and maintaining an information systems infrastructure, which has an appropriate level of security.

Cyberattacks on digital records and other systems pose a risk to privacy because hackers could access confidential information, potentially causing harm to patient safety and care delivery. Hackers can use ransomware viruses to hold medical records or devices hostage, risking our access to vital tools and information.

To ensure a consistent approach to information security, the following controls will apply either holistically or to specific groups or individuals within the Trust.

6.1.1 Information Security & Confidentiality Awareness/Training

Information security and confidentiality requirements are addressed during recruitment and included in job descriptions and all contracts of employment contain a confidentiality clause.

Information security awareness is included in the staff induction training; for which on-going awareness through annual mandatory updates is in place to ensure that staff awareness is refreshed and updated as necessary.

Technology is ever changing and in order to keep abreast of any associated vulnerabilities, the Trust will ensure that staff receive regular and appropriate information security training as relevant for their job function.

6.1.2 Secure Control of Information Assets

Each information asset should have a named custodian who will be responsible for their information security of that asset; Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) have been appointed in all Divisions and Corporate functions to take responsibility for information assets. The Trust has an information asset register that is maintained by the Information Governance team to record information assets and these are populated on a department level. Corporate Records are recorded by corporate departments as part of the Trust Records Inventory.

Divisions and Corporate functions must ensure they update and maintain details of all information assets held in the register, ensuring risk assessments are completed in line with the agreed schedule. Devices purchased outside of the NHS will not be authorised to access the Trust network without senior sign off.

Staff must maintain a clear desk and clear screen policy to reduce the risk of unauthorised access to information assets such as papers, media, and information processing facilities.

The following guidelines must be considered:

- Confidential or business critical information, e.g. on paper or on digital storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when offices are vacated;.

- Documents containing confidential information should be removed from printers immediately
- Computers must be logged off or locked (windows+L)
- All files containing confidential or business critical information must be saved onto the shared drives and not on individual devices e.g. desktops. This ensures that information is backed up and accessible on a daily basis.

All IAOs should undertake risk management training to ensure they understand the responsibilities associated with the assets that they own.

6.1.3 Physical Access Controls

Only authorised staff with a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

Facilities that serve multiple users should be capable of restricting access only to those authorised.

All staff must wear identification badges at all times.

Door codes and passwords must not be written onto the back of ID badges., on the wall or any other area that could be utilised by another.

Staff entering non-public areas should be challenged, if lacking visible ID badges, and asked to produce some form of identity or asked to sign into the building if on a specific business activity.

As good practice, keypad locks on doors should also be changed regularly, potentially when members of staff leave the department and when staff members have received disciplinary action for any IG related incident.

6.1.4 Password and Access Control

Access to information contained within or accessed from information systems will be controlled and restricted to authorised users.

IAOs will ensure that:

- Where necessary unique IDs exist for all user accounts. If generic accounts are used, they will be audited and associated with a named user.
- Redundant or disabled accounts are identified for periodic review and removed
- User access rights are segregated where applicable (role -based access)
- Regular password changes are enforced
- A Standard Operating Procedure is in place that sets out the security controls of the system or asset.

Staff are responsible for keeping their login credentials secure (this includes Smartcards), and must ensure it is neither disclosed to, nor used by anyone else, under any circumstances.

Staff must only access systems using their own login and password. Further information on the set up and management of passwords is available in our Password Management Procedure available here[2]. The Password Management procedure includes:

a) How to avoid choosing obvious passwords (such as those based on easily discoverable information).
(b) Not to choose common passwords (use of technical means, such as using a password blacklist, is recommended).
(c) Do not use common passwords.
(d) Can I write my password down?
(e) Super users/system administrators.
(f) Managing shared access.
(g) Have different passwords for work and personal use.

All staff are accountable for any activity carried out under their login and password, and this is audited.

Staff must ensure any unattended devices are logged out of or locked securely.

It is the responsibility of all Line Managers to ensure that all new staff and staff that are changing their role, are properly inducted, are given appropriate access to all necessary information and communications technology (ICT) systems, in line with relevant local procedures, to adequately perform their duties.

No member of staff will be allowed to access confidential information until line management are satisfied that they have undertaken the appropriate level of training.

It is the responsibility of Line Managers to inform relevant IAOs or the NHIS Service Desk of any staff terminating or changing their employment immediately or notice being given to enable arrangements for removal of access and closure of accounts.

6.1.5 Multi-Factor Authentication

Multi-factor authentication (MFA) is an additional way of checking that it is really you when you log in to your account.

[2] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8640

There are five options available that you can choose from to authenticate your account: Microsoft Authenticator App (available on all Trust devices), text message, phone call, FIDO2 token or NHS smartcard. Guidance on how to set up MFA is available here: Getting Started with MFA – NHSmail Support[3].

How to set up multi-factor authentication

1. Self-enrol - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Getting+Started+with+MFA_Steps+for+Self-Enrolment.pdf
2. Microsoft Authenticator App - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Setting+Up+MFA_Steps+for+Mobile+App.pdf
3. Text message - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Setting+Up+MFA_Steps+for+Text+Message.pdf
4. Call - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Setting+Up+MFA_Steps+for+Phone+Call.pdf
5. Smartcard – no guidance available from Microsoft at the time of writing.

Multi-factor authentication will be mandated for all NHSmail users from 30th June 2023.

6.1.6 Equipment Siting and Security

IT equipment supporting critical or sensitive business activities will be housed in secure areas with appropriate access and entry controls. Information assets should be protected from physical security threats and environmental hazards.

The following controls will be considered as a minimum:

- Access to information and information systems will be monitored to ensure relevant access to confidential information
- External doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level
- Suitable alarm systems will be installed and cover all external doors and accessible windows.
- Equipment will be sited in appropriate environments with power supply protection and air conditioning where necessary.
- The location of equipment and information assets will be assessed for the suitability of the environment before installation e.g. risk of flooding, potential security flaws in the design or layout of the area.
- Devices used to access confidential information should be sited in a way the information displayed will not be easily accessible to people who should not have access e.g. in public areas screens should be facing away from visitors. The use of Privacy screens can also be considered

[3] https://support.nhs.net/knowledge-base/getting-started-with-mfa/#mobile-app-method-enrolment

- Power and telecommunications cabling carrying data or supporting information services will be protected from interception, interference, and damage.
- Equipment will be correctly maintained to ensure its continued availability and integrity.

Mobile Devices will need additional consideration due to their functionality and should be kept secure at all times even when charging or left unattended.

6.1.7 System and Network Security

Trust equipment must not be connected to any unauthorised external networks. The Trust's systems and network will be configured by Nottinghamshire Health Informatics Service (NHIS) in accordance with NHS standards and industry best practice.

Network management & security is the responsibility of NHIS; all devices connected to the Trust's network must meet required standards which are determined by the Trust and NHIS and unauthorised devices will not be allowed to connect to the network.

Penetration tests or vulnerability assessments on the Trust network will be conducted by authorised specialist personnel under the supervision of NHIS and tests should be planned, documented and repeatable.

6.1.8 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of the perceived consequence (value of asset, severity of impact) and the likelihood of occurrence. In order to make the best use of resources, it is important to ensure that each information asset is secured to a level appropriate to the measure of risk associated with it.

Information about technical vulnerabilities of information system used at the Trust should be obtained prior to the procurement and implementation of the system.

The introduction of new systems and major changes to existing systems will follow a formal process of risk assessment using the Trust's Data Protection Impact Assessment (DPIA) for each of the Trust's information systems to ensure each system is secured to an appropriate level and that any identified risks to the confidentiality, integrity, availability and security of the asset are identified and mitigated to an acceptable level Identified information security risks should be managed on a formal basis. They should be recorded on the Trust risk register and action plans put in place to effectively manage those risks.

The risk register and all associated actions will be reviewed at regular intervals. The management and treatment of information security risks will be in accordance with the Trust's Risk Management and Assurance Policy.

6.1.9 Information Security Incident Reporting and Management

All information security incidents and near misses will be reported and investigated in accordance with the Trust's formal procedure for reporting security incidents, to ensure quick, effective, and orderly response. Any information security weaknesses should be documented in the risk registers.

All incidents should be logged with the Trust Incident reporting tool (Datix), accessible via the Trust Intranet. If immediate remedial action is required to any IT system or equipment NHIS should be contacted via the customer portal https://customerportal.notts-his.nhs.uk/https://customerportal.notts-his.nhs.uk/ or on Extension 4040.

Examples of security incidents:

- Systems left logged on and unattended
- Passwords written down or visible to others
- Using another person's password
- Divulging your password
- Making use of information for personal gain
- Accessing information for personal knowledge
- Unauthorised release of information
- Attempting to gain access under false pretences
- Infection of the network with malicious software (suspected viruses or malware)
- Knowingly entering inaccurate data
- Deleting data prior to the legal retention period expiring
- Loss or misuse of personal information
- Malicious damage to equipment or data
- Theft or loss of a Trust Device

This list is not exhaustive.

The Information Governance Manager/DPO and equivalent officer at NHIS keep the Information Governance Committee and the SIRO informed of the information security status of the Trust by means of regular reports, presented at the IG Committee.

6.1.10 Protection from Malicious Code

Under the Computer Misuse Act 1990 'hacking' and the introduction of computer viruses are criminal offences. The purpose of the Act is to make provision for securing computer material against unauthorised access or modification. It makes unauthorised access to a computer, programs, or data an offence.

Controls will be implemented to detect and prevent infection from contaminated media and communications and NHIS will ensure that all Trust owned and managed devices have approved anti-virus software installed.

Staff should not act in a way that may increase the risk of the introduction of a virus or malware on the Trust Network and must not remove or amend the security controls of any Trust provided device. This includes the installation of non-authorised software, sharing data from PCs not on the Trust network and sharing or accessing suspicious emails or websites. Users must be vigilant when receiving emails from unknown sources and not open emails with unexpected attachments.

6.1.11 Monitoring System Access and Use

Processes will be implemented to monitor system access and use. This will include regular audits of user access to systems to ensure that access is pertinent to the member of staffs' role and use of the system and related information is in line with the conditions under which access was granted. The Account Management SOP must be completed for each system and reviewed annually this will be monitored through the IG Committee and evidence presented as part of the annual report to SIRO.

A record of staff having elevated or administrator access rights will be maintained, and the access regularly reviewed and revoked where applicable. Event logs will be protected against tampering in the event that system access will be required to be monitored.

6.1.12 Information Sharing Protocols

The Trust will ensure there is justification and a legal basis before sharing personal or confidential information with any third party. Patient identifiable information will only be shared in accordance with Data Protection Legislation and the NHS Confidentiality Code of Practice. Confidentiality Code of Practice.

All routine information flows will be covered by formal agreements and the decision to share information with a third party will be documented and the agreements will identify requirements for the protection of confidential information.

6.1.13 External Parties

Risks to the Trust's information and information processing facilities will be identified and managed prior to granting third-party access (including physical and system/network access). All third-party contractors must have formal contracts in place, sign a confidentiality agreement and be aware of how to report an incident in the Trust.

Any external suppliers involved in processing and/or storing data on behalf of the Trust will be expected to demonstrate adherence to national and industry recognised standards of information

security, e.g. 'Satisfactory' Data Security and Protection Toolkit submission, ISO 27001:2017 certification, Cyber Essentials Scheme amongst others.

6.1.14 Introduction & Accreditation of Information Systems

Any new (or significantly changed) system or process where personal data is processed must be subjected to a Data Protection Impact Assessment (DPIA) at an early stage in the project. It will be the responsibility of the Project Manager or system implementer to ensure this is completed and acted on.

The aim is to identify and adequately mitigate any unacceptable risks to an individual's privacy and asses the security arrangements for the protection of such data. The DPIA will identify:

- What data is processed
- Who has access to the data
- Where data is stored

The Trust will also ensure that all new and existing information systems, applications, and networks capable of storing or granting access to Trust and/or confidential information have an agreed System Level Security and Access procedure in place.

NHIS should be involved in establishing and defining the information security requirements as part of any procurement process before award of contract.

6.1.15 Change Control

Changes to information systems, applications or networks must be reviewed and approved by NHIS and Information Governance following approved change control procedures.

All changes to the system should be processed under formal change control and live data should be separated and adequately protected from test data. The Information Commissioners Office (ICO) advises that the use of actual personal data for system testing should be avoided. Where there is no practical alternative to using live data for this purpose, systems administrators should develop alternative methods of system testing.

6.1.16 Remote working

The physical and logical controls that are available within the Trust network and physical environment may not be available by design when working outside of that environment. As a result, there is an increased risk of information loss or unauthorised access. Remote workers must take necessary precautions to protect confidential information in these circumstances.

Remote workers have a responsibility to ensure that:

- Mobile devices and removable media where applicable, are encrypted in line with national NHS requirements e.g. 256bit
- Only authorised mobile devices and removable media are used for Trust business
- Mobile devices and removable media should never be used as the primary source of data. The source data should reside on the Trust's shared drives where the backup and security of this can be controlled. Where the source data is portable like a DVD/CD, this must be authorised and stored securely with a record of off-site removal kept for reference.
- Mobile devices and removable media must only be used where there is an identified business need relevant to the member of staff's role as agreed with line management.
- Mobile devices and removable media must be kept secure at all times. All staff are responsible for the physical protection against loss, damage, abuse, or misuse. This includes when it is used, where it is stored, and how it is protected in transit.
- Mobile devices, in particular laptops must regularly (recommended once a week) be connected to the Trust's network 'on-site' to allow updates to be picked up e.g. Antivirus and Windows security updates. (In the event that the user is away for a prolonged period of time either on health grounds or holiday, the device must be connected on return).
- Mobile devices and removable media use should be kept to a minimum when used in public areas to reduce the risk of shoulder surfing and in turn unauthorised access to confidential information.
- Under no circumstances must confidential information be processed on personal devices, the only exception to this is accessing NHSmail which is permitted.

6.1.17 Transportation of Records

Information can be vulnerable to unauthorised access, misuse, or corruption during physical transport, for instance when sending media via the postal service or via courier.

Media containing confidential information must be protected against unauthorised access, misuse, or corruption in transit. A secure transportation plan should be in place for the transfer of large volumes of data either between the Trust and a supplier or between two or more suppliers as part of a change of service provider.

Special controls should be adopted, where necessary, to protect confidential information from unauthorised disclosure or modification and as a minimum should include;- -

- The use of reliable transport or couriers
- Packaging being sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturer's specifications
- Use of locked containers
- Delivery by hand
- Tamper-evident packaging (which reveals any attempt to gain access).

- Recorded or registered delivery options

Staff are responsible for ensuring that the security and confidentiality of information is maintained whilst in their care and it is important to note that records must;-

- be stored and carried in a secure bag/case
- not be carried 'loosely'
- not be left unattended in transit

Staff should be aware of Trust Safe Haven procedures when transferring any confidential information and consideration should always be given to the business need for transporting or moving records as this increases the risk of data loss.

6.1.18 Encryption

Involves converting information using a code that prevents it being understood by anyone who isn't authorised to read it; passwords only provide basic security, so the data is still quite easy to access.

NHIS will therefore:

- ensure that suitable encryption algorithms and tools are available and utilised to secure Trust data and systems
- encrypt all mobile computing devices (, including smartphones and tablets) etc. (where issued by the Trust).

6.1.19 Disposal of Equipment & Media

All confidential data as defined under UK GDPR/Data Protection Act, stored on digital media or on paper should be disposed of only after reliable precautions to destroy the data have taken place. Advice should be sought from the NHIS and the Information Governance Department before any disposal of IT equipment or IT Media.

Destruction and disposal of equipment and media containing confidential information will take into consideration data retention requirements. Where third parties are involved in this process, the Trust will ensure that adequate record of collection exist to maintain an audit trail and that the third party complies with the relevant legislation regarding disposal of waste. All data storage devices must be purged of sensitive data prior to disposal, which is to be actioned by NHIS via a third party. Where this is not possible, the equipment or media must be destroyed by a delegated third party or returned to the NHIS for confidential disposal.

6.1.20 Decommissioning of applications, systems, and hardware

Where systems, applications and associated hardware are replaced, upgraded, or decommissioned altogether, the Trust will take necessary steps to ensure the security and availability of data in line with the relevant data retention requirements. Particular emphasis should be given to proper data migration and preservation and to facilitating subsequent use of data by the receiving systems.

The Trust should review the appropriateness of access to Trust data held in decommissioned systems including access by third party suppliers; the Trust should ensure where necessary that both system and network access is appropriately revoked. Divisions and Corporate functions should consult with NHIS to agree a decommission plan for any systems and associated data hosted by NHIS. Please refer to the Trust's Transfer of Data Policy[4].

6.1.21 Business Continuity and Disaster Recovery Plans

A managed process will be developed to counteract the business interruptions caused by major IT service failure. The Trust shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems, and networks.

NHIS will ensure that all systems will be backed-up at regular intervals. Backups stored in approved locations and restores of back-ups are tested regularly.

All departments must have Business Continuity Plans in place to maintain essential services in their departments in the event of an IT system failure.

Adequate information security controls should exist within business continuity or disaster recovery processes. The Trust will also ensure that forensic readiness planning is aligned with business continuity and disaster recovery functions.

6.1.22 Cyber security risk

As it pertains to network and system operations risks cannot be completely eliminated, but instead must be managed through informed decision making processes with the goal being to reduce the likelihood and impact of a cyber-event to the Trust's operations, assets and confidential information (i.e. both staff and patients).

NHIS will ensure the effective management of the Trust's cyber security risk ensuring;-; -

- The secure configuration of digital assets, network, and data within its control
- Regular review of the relevance and adequacy of controls,
- Real time monitoring to allow for quick detection and response to events

[4] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=9855

6.1.23 Forensic Readiness

There continues to be a significant increase in the number of crimes involving computers and as a result, the need to use digital evidence requires enhanced system and staff monitoring. In addition to this, the technical, physical, and procedural means to secure data to evidential standards of admissibility is equally important.

Policies, processes, and procedures are in place at the Trust to ensure that staff recognise the importance and legal sensitivities of evidence, and have appropriate advice including when interfacing with law enforcement agencies.

The aim of forensic readiness is to provide a systematic, standardised, and legal basis for the admissibility of digital evidence. The Trust's forensic readiness approach must: -

- Protect the Trust, its staff, and its patients through the availability of reliable digital evidence gathered from its systems and processes.
- Allow consistent, rapid investigation of major events or incidents with minimum disruption to Trust business.
- Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required.
- Demonstrate due diligence and good governance of the Trust's information assets.

Typical computer crimes that involve forensic analysis include IP theft, fraud, identity theft, email abuse and inappropriate content. In this context, forensic evidence may include evidence in the form of system log files, emails, back-up data, removable media, portable computers, network, and telephone records amongst others that may be collected in advance or subsequent to an event or dispute occurring.

Digital evidence is any information that can be secured from an information system and used during the course of an investigation; this extends to internal disciplinary hearings, employment tribunals, arbitration panels and courts of law.

As part of the deployment of new digital systems at the Trust, due consideration should be given to forensic planning to ensure that the system is able to:

- gather digital evidence (user and data log files) without interfering with business processes;.
- Prioritise digital evidence gathering for those processes that may significantly impact the Trust, its staff, and its patients;.
- Allow investigation to proceed at a cost in proportion to the incident or event;.
- Provide easily interpretable digital evidence where it impacts on the outcome of any investigation, dispute, or legal action.

Where an audit is required the Trust Confidentiality Audit Policy should be referred to.

6.1.24 Digital forensic investigation

Is any live investigation involving Digital Evidence and each investigation should have a formal case file.

Certain investigations particularly those involving criminal matters, must be referred to the appropriate law enforcement authority or regulator. Digital evidence handled during investigations should be treated as sensitive confidential information without exception.

Where an investigation requires expertise beyond the Trusts "in-house" capability, a risk assessment should be carried out balancing data or information loss, and or system damage and failure with the cost of employing external forensic expertise. This assessment should be made at a senior level and involve the Senior Information Risk Owner (SIRO), the Information Asset Owner (IAO) concerned, the IG Manager/DPO, and, depending on the sensitivity and confidentiality of the information compromised, the Caldicott Guardian (CG).

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored **(WHAT – element of compliance or effectiveness within the document will be monitored)**	**Responsible Individual** **(WHO – is going to monitor this element)**	**Process for Monitoring e.g. Audit** **(HOW – will this element be monitored (method used))**	**Frequency of Monitoring** **(WHEN – will this element be monitored (frequency/ how often))**	**Responsible Individual or Committee/ Group for Review of Results** **(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g verbal, formal report etc) and by who)**
DSPT Validation	360 Assurance	Audit	Annually	IG Group/IG Manager/Risk Committee
Adherence to Information Security policy and guidelines in nominated Division/Corporate Function	IG Commitee360 Assurance	Audit	Annually	IG Group
IAO report to the SIRO for each division; including reference to security incidents and risks (Copy available from IG office)	IAO	Self-Assessment Return	Annually	IG Manager/ DPO/ SIRO
Network Security Monitoring and reporting by NHIS	NHIS	Report shared, Hygiene report	TBC	IG Committee
Account Management SOP	IAO	Completion of SOP. Audit to be presented as part of the report to SIRO	Quarterly	IG Committee

8.0 TRAINING AND IMPLEMENTATION

8.1 Training

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[5] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

8.2 Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[6]

9.0 IMPACT ASSESSMENTS

This document has been subject to an **Equality Impact Assessment**

An Equality Impact Assessment has been undertaken on this Policy and has not indicated that any additional considerations are necessary. See, see completed form at Appendix 1

This document is not subject to an **Environmental Impact Assessment**.

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED Trust DOCUMENTS

Evidence Base:

- Data Protection Act 2018.
- UK General Data Protection Regulation

[5] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[6] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

- Network and Information Systems Regulations
- Copyright, Designs and Patents Act 1988.
- Computer Misuse Act 1990.
- Human Rights Act 1998.

Related SFHFT Documents:

- Confidentiality Audit Policy
- Data Protection Impact Assessment Procedure
- Data Protection, Confidentiality & Disclosure Policy
- Email and Internet & Email Policy
- Information Governance Policy
- Information Sharing Policy
- Password Management Procedure
- Remote Working Policy
- Risk Management and Assurance Policy
- Safe Haven Procedure

National Guidance:

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- NHS Confidentiality Code of Practice 2016
- Information Security Management: NHS Code of Practice 2007
- National Data Guardian - 10 Data Security Standards

11.0 KEYWORDS

Data security, integrity, availability, password, cyber

12.0 APPENDICES

Please refer to the contents table

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Information Security Policy			
New or existing service/policy/procedure: Existing Policy			
Date of Assessment: 1st November 2022			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy	None

		read or large print, and may be available in alternative languages, upon request	
Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None
Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None.

What data or information did you use in support of this EqIA?

- Trust guidance for completion of equality impact assessments.

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

- No.

Level of impact From the information provided above and following Equality Impact Assessment guidance on how to complete, the perceived level of impact is: Low Level of Impact
Name of Responsible Person undertaking this assessment: Gina Robinson, Information Security Officer
Signature: G.H.Robinson
Date: 1st November 2022

APPENDIX 2 – GOOD PRACTICE GUIDE FOR STAFF

This section is intended to be an aide to employees by listing some of the common aspects of the security policy. It is not intended to be a comprehensive summary and does not reduce or alter the standards or principles laid out in the Information Security Policy.

- Contact your Line Manager if you are aware that you are not meeting the standards and principles of the security policy.
- All staff must attend mandatory training sessions that are made available to them and identify areas of training need regarding information and security issues.
- Be aware of potential risks that surround the data and systems that you use – remember it is your responsibility to keep personal data confidential.
- Where possible, store all data to the shared network file servers (i.e. S, G or H Drives, as these drives are backed up on a daily basis and not on local computer 'C' drives. If you do not have access to a network file server, please contact the NHIS Service Desk
- Safeguard portable IT equipment, memory sticks and external storage devices. Do not leave them visible in unprotected areas. These devices must be encrypted.
- Dispose of confidential information on printouts, external storage devices in a secure manner and in line with the Waste Management Policy.
- Always log off or press Ctrl+Alt+Delete then Enter or Windows + L if you leave your computer unattended.
- Wear your identification badge at all times and challenge strangers without one.
- Observe building security procedures. Close and lock windows and doors when unattended and ensure curtains and blinds are drawn, if applicable at night.
- Staff must not hold confidential information on any mobile devices without the recommended encryption in place. Ensure mobile devices are docked on a regular basis to ensure virus software is up to date.
- If you suspect you have a computer virus or are unsure about any of the above, contact the NHIS Service Desk on extension 4040 or direct dial 01623 410310.