

INFORMATION SECURITY POLICY

POLICY

Reference	ISP-01		
Approving Body	Information Governance Committee		
Date Approved	2025		
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	2025		
Version	9		
Summary of Changes from Previous Version	Multi-Factor Authentication		
Supersedes	8		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Committee Information Governance Working Group		
Date of Completion of Equality Impact Assessment	29 th May 2025		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Potential non-compliance with: <ul style="list-style-type: none"> • Computer Misuse Act 1990 • UK General Data Protection Regulation • The Network and Information Systems Regulations 2018 (UK) • Data Protection Act 2018 • Data (Use and Access) Act 2025 		
Target audience	All staff and the general public		
Review Date	June 2027		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Head of Data Security and Privacy		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Head of Data Security and Privacy		

Associated Documents/ Information	Date Associated Documents/ Information was reviewed
Password Management Procedure	July 2024
Template control	April 2024

CONTENTS

1.0 INTRODUCTION	4
2.0 POLICY STATEMENT	4
3.0 DEFINITIONS/ ABBREVIATIONS.....	7
4.0 ROLES AND RESPONSIBILITIES.....	9
5.0 APPROVAL	11
6.0 DOCUMENT REQUIREMENTS	11
6.1.1 Secure Control of Information Assets.....	11
6.1.2 Physical Access Controls	12
6.1.3 Password and Access Control	13
6.1.4 Multi-Factor Authentication.....	14
6.1.5 Equipment Siting and Security	14
6.1.6 System and Network Security	15
6.1.7 Information Risk Assessment.....	15
6.1.8 Information Security Incident Reporting and Management.....	16
6.1.9 Protection from Malicious Code	17
6.1.10 Monitoring System Access and Use.....	17
6.1.11 Information Sharing Protocols.....	18
6.1.12 External Parties	18
6.1.13 Remote Working Security Obligations	18
Working Offsite.....	19
6.1.14 Transportation of Records	20
6.1.15 Encryption.....	21
6.1.16 Disposal of Equipment and Media	21
6.1.17 Decommissioning of Applications, Systems, and Hardware	21
6.1.18 Business Continuity and Disaster Recovery Plans.....	22
6.1.19 Forensic Readiness	22
6.1.20 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
APPENDIX 3 – REMOTE WORKING SECURITY OBLIGATIONS CHECKLIST	31

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.

In accordance with Part 5 of the Data (Use and Access) Act 2025, Sherwood Forest Hospitals NHS Foundation Trust commits to ensuring that all personal and confidential data is:

- Processed lawfully, fairly, and transparently, with a clearly defined and documented legal basis for each processing activity.
- Used strictly for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.
- Minimised to what is necessary in relation to the purposes for which it is processed.
- Subject to robust technical and organisational safeguards to ensure confidentiality, integrity, and availability.
- Subject to oversight by the Information Commission, with full cooperation in audits, investigations, and compliance reviews.

The Trust will maintain a Data Use Register to document all instances of data access and sharing, including the purpose, legal basis, recipients, and retention periods, in line with the transparency requirements of the Act.

All staff must complete mandatory training on the principles of lawful data use and access and must report any suspected misuse or unauthorised access immediately through the Trust's incident reporting procedures.

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 NHS Foundation Trust (SFHFT).

NHIS - 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 confidential 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/mobile devices such as laptops, PC's, 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 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 can 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. Record Management responsibilities will be written into all accountable individuals' job descriptions.

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 Administrators will liaise with the Information Governance Team on the management of records in that directorate/speciality/department. The Information Governance Team will provide support and guidance to nominated departmental representatives.

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 offsite from a non-fixed location i.e. 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

Trust Board has responsibility, in compliance with the Trust's Governance manual, to ensure and gain assurance that the Trust has in place robust arrangements for the management of records and that such arrangements are complied with.

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 Chief Medical Officer 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

1

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

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 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. 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 Secure Control of Information Assets

Each information asset should have a named custodian who will be responsible for the information security of that asset. Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) have been appointed in all divisions to take ownership 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.

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.

6.1.2 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. 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.

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 ID badges are not visible, 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 be changed regularly, and ideally when members of staff leave the department or when staff have received disciplinary action for any IG related incident.

6.1.3 Password and Access Control

Access to information within or accessed from information systems will be regulated and limited to authorised users according to least privilege principles.

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 auditable.

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

² <https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/>

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.

6.1.4 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. This second layer of security is designed to prevent anyone but you from accessing your account, even if they know your password.

There are four options available that you can choose from to authenticate your account: Microsoft Authenticator App (available on all Trust devices), text message, phone call, or NHS smartcard. Guidance on how to set up MFA is available here: [Getting Started with MFA – NHSmail Support³](#).

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>

Multi-factor authentication has been mandated for all NHSmail users from 30th June 2023.

6.1.5 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:

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

- 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.
- 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 require additional consideration due to their functionality and should be kept secure at all times even when charging or left unattended.

6.1.6 System and Network Security

Trust equipment must not be connected to any unauthorised external networks. However connecting to home broadband is permitted. The Trust's systems and network will be configured by Nottinghamshire Health Informatics Service (NHIS) in accordance with NHS standards and industry best practice. When connecting from locations outside of NHS owned premises, connection via VPN (Virtual Private Network) is required to connect to networked systems, and to securely access corporate resources.

Network management and 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.

6.1.7 Information Risk Assessment

The core principle of risk assessment and management involves identification and quantifying information security risks based on the perceived consequence (value of asset, severity of impact) and the likelihood of occurrence. To optimise resource allocation it is essential to ensure that each information asset is secured to a level appropriate to its associated risk.

Technical vulnerabilities of information systems used at the Trust should be identified before the procurement and implementation of the system.

The introduction of new systems and significant changes to existing systems will adhere to a formal risk assessment process using the Trust's Data Protection Impact Assessment (DPIA). This ensures 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 formally, recorded on the Trust's risk register, and action plans should be implemented to manage those risks effectively.

The risk register and all related actions will be reviewed regularly. The management and treatment of information security risks will comply with the Trust's Risk Management and Assurance Policy.

NHIS should be involved in determining the information security requirements as part of any procurement process prior to the awarding of contracts. Failure to do so may result in a refusal of connection to the network.

All system modifications should undergo formal change control, and live data must be separated and adequately protected from test data. The Information Commission recommends avoiding the use of actual personal data for system testing. If there is no practical alternative to using live data, systems administrators should implement alternative methods for system testing.

6.1.8 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 identified information security weaknesses should be documented in the risk registers.

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

Examples of security incidents include:

- Systems left logged on and unattended
- Passwords written down or visible to others
- Using another person's password
- Divulging your password
- Using 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 Head of Data Security and Privacy and equivalent officer at NHIS will keep the Information Governance Committee and the SIRO informed of the Trust's information security status through regular reports, presented at the IG Committee.

6.1.9 Protection from Malicious Code

Under the Computer Misuse Act 1990, unauthorised access to computer systems and the introduction of computer viruses are criminal offences. The Act aims to secure computer material against unauthorised access or modification, making it an offence to access a computer, programs, or data without permission.

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

Staff should avoid actions that may increase the risk of introducing a virus or malware to the Trust Network and must not remove or amend the security controls of any Trust provided device. This includes installing non-authorised software, sharing data from non-Trust network PC's, laptops, and sharing or accessing suspicious emails or websites. Users should be vigilant when receiving emails from unknown sources and avoid opening emails with unexpected attachments.

6.1.10 Monitoring System Access and Use

Processes will be established to monitor system access and usage. This will include regular audits of user access to systems to ensure that access is appropriate to the staff members role,

and that system use complies with the conditions under which access was granted. The Account Management SOP must be completed for each system and reviewed annually. This process will be overseen by the IG Committee, with evidence presented in the annual report to SIRO.

A record of staff members with elevated or administrator access rights will be maintained, and access will be regularly reviewed and revoked as necessary. Event logs will be protected against tampering to maintain the integrity of system access monitoring.

6.1.11 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 be shared only in accordance with Data Protection Legislation and the NHS Confidentiality Code of Practice. [Confidentiality Code of Practice.](#)

All routine information sharing will be covered by formal agreements, which will document the decision to share and set requirements for protecting confidential information.

6.1.12 External Parties

Prior to granting third-party access—whether physical or system/network access—risks to the Trust's information and information processing facilities must be identified and managed. All third-party contractors are required to have formal contracts in place, sign a confidentiality agreement, and be informed on how to report an incident within the Trust.

External suppliers involved in processing and/or storing data on behalf of the Trust are expected to demonstrate compliance with national and industry-recognised standards of information security. This includes, but is not limited to, achieving a 'Standards Met' submission in the Data Security and Protection Toolkit, obtaining ISO 27001:2017 certification, or meeting the requirements of the Cyber Essentials Scheme, among others.

6.1.13 Remote Working Security Obligations

When working outside the Trust network and physical environment, the same physical and logical controls may not be present. Consequently, there is a heightened risk of information loss or unauthorised access. Therefore, remote workers must take all necessary precautions to safeguard confidential information under these circumstances. Non-compliance with Trust policies and procedures may result in disciplinary action.

Remote workers have the obligation to ensure that:

- Mobile devices and removable media, where applicable, are encrypted in accordance with national NHS requirements (e.g. 256-bit encryption).
- Only authorised mobile devices and removable media are used for Trust business.
- Mobile devices and removable media are never employed as the primary source of data. The source data should reside on the Trust's shared drives where backup and security measures can be effectively managed. If the source data is portable, such as a DVD/CD, it must be authorised and securely stored, with a record of off-site removal maintained for reference.
- Mobile devices and removable media are used solely when there is an identified business need pertinent to the staff member's role, as agreed upon with line management.
- Mobile devices and removable media are kept secure at all times. All staff are responsible for the physical protection against loss, damage, abuse, or misuse. This includes ensuring security during usage, storage, and transit.
- Mobile devices, particularly laptops, are connected to the Trust's network 'on-site' regularly (recommended once a week) to receive updates, such as antivirus and Windows security updates. In cases where the user is away for an extended period due to health reasons or holiday, or working remotely, the device must be connected upon return.
- The use of mobile devices and removable media should be minimised in public areas and at home to reduce the risk of shoulder surfing and, consequently, unauthorised access to confidential information.
- Under no circumstances should confidential information be processed on personal devices, with the sole exception of accessing NHSmail, which is permitted.

Working Offsite

Remote workers must also adhere to the following guidelines when working offsite:
Treat home workspaces like professional workspaces.

- Protect devices during transit; treat them as hand luggage. Avoid leaving devices in cars or public areas.
- Ensure screens are locked if unattended, especially around children/housemates.
- Position screens to prevent unauthorised viewing (shoulder surfing).
- Store devices safely and securely at the end of the working day.
- Do not leave devices unattended in insecure areas (e.g., unlocked house).
- Close/lock windows and doors when unattended; draw curtains/blinds at night.
- Log off or lock your computer (Ctrl+Alt+Delete or Windows+L) when unattended.
- Blur your background during video calls.
- Ensure conversations are not overheard during calls or video meetings. Conversations should be held in areas where they are less likely to be overheard.
- Report lost/stolen devices or VPN tokens immediately.
- Save files to shared drives, not on your devices.
- Do not use personal email/messaging for patient/staff data.

- Return Trust equipment at the end of the remote working arrangement.
- Assess the need to transport records in order to minimise the risk of data loss.
- Paper documents should not be taken off-site unless necessary and agreed with Information Governance.
- Paper documents must be stored and carried securely, not loosely.
- Use removable media only when required and approved.
- VPN connections must be properly terminated after use.
- Maintain a clear desk and clear screen policy. Ensure records are inaccessible to patients, the public, and non-Trust staff.
- Secure confidential/business-critical information when offices are vacated.
- Lock external doors and windows when unattended. Consider external protection for ground-level windows.
- Staff must safeguard username and passwords and not share them.
- Devices must be secure even when charging or left unattended.
- Take reasonable steps to minimise theft or damage to Trust property.
- Change passwords regularly and when prompted.

6.1.14 Transportation of Records

During physical transportation, information is susceptible to unauthorised access, misuse, or corruption, particularly when media is sent via postal services or couriers.

To safeguard confidential information during transit, appropriate measures must be implemented. A secure transportation plan should be established for transferring large volumes of data between the Trust and a supplier, or among multiple suppliers, especially when changing service providers.

Special controls should be adopted as necessary to prevent unauthorised disclosure or modification of confidential information. At a minimum, these controls should include:

- Utilising reliable transport or courier services
- Ensuring packaging is adequate to protect contents from potential physical damage during transit, in accordance with manufacturer specifications
- Employing locked containers
- Hand delivery
- Using tamper-evident packaging to indicate any attempt at access
- Opting for recorded or registered delivery methods.

Staff members are responsible for maintaining the security and confidentiality of information while it is in their possession. It is crucial to adhere to the following guidelines:

- Information must be stored and carried in a secure bag or case

- Information should not be transported loosely
- Information must not be left unattended during transit.

Staff should be familiar with Trust Safe Haven procedures when transferring any confidential information. Consideration should always be given to the necessity of transporting or moving records, as this practice increases the risk of data loss.

6.1.15 Encryption

Encryption involves converting information into a code that prevents unauthorised access, as passwords alone provide only basic security, leaving the data relatively accessible.

NHIS will:

- Ensure that appropriate encryption algorithms and tools are available and employed to secure Trust data and systems.
- Encrypt all mobile computing devices, including smartphones and tablets, issued by the Trust.

6.1.16 Disposal of Equipment and 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 effective measures to ensure data destruction has been implemented. It is advisable to seek guidance from the NHIS and the Information Governance Department prior to disposing of IT equipment or IT Media.

The destruction and disposal of equipment and media containing confidential information will consider data retention requirements. When third parties are involved in this process, the Trust will ensure that a sufficient record of collection exists to maintain an audit trail and that the third party complies with the relevant legislation regarding waste disposal. All data storage devices must be purged of sensitive data prior to disposal, which is to be managed by NHIS via a third party. If this is not feasible, the equipment or media must be destroyed by an authorised third party or returned to the NHIS for confidential disposal.

6.1.17 Decommissioning of Applications, Systems, and Hardware

In scenarios where systems, applications, and associated hardware are replaced, upgraded, or fully decommissioned, the Trust is committed to taking all necessary actions to ensure the security and availability of data in compliance with relevant data retention requirements. Particular attention must be given to the correct migration and preservation of data and to facilitating its subsequent use 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, ensuring that both system and network

access are revoked as necessary. Divisions and Corporate functions must consult with NHIS to establish a decommission plan for any systems and associated data hosted by NHIS. For detailed guidance, please refer to the Trust's Transfer of Data Policy.

6.1.18 Business Continuity and Disaster Recovery Plans

A managed process will address business interruptions from IT service failures. The Trust will create business impact assessments and continuity and disaster recovery plans for all critical information, applications, systems, and networks.

NHIS will back up systems regularly, store backups in approved locations, and test restore processes.

All departments must have Business Continuity Plans to maintain essential services during IT failures.

Information security controls should be part of continuity or disaster recovery plans. Forensic readiness planning will align with these functions.

6.1.19 Forensic Readiness

With the rise in computer-related crimes, monitoring systems and staff to secure digital evidence is crucial. The Trust has policies ensuring staff understand legal sensitivities of evidence and can interface with law enforcement.

Forensic readiness aims to provide a systematic basis for digital evidence admissibility. The Trust's approach must:

- Protect the Trust, its staff, and patients with reliable digital evidence.
- Allow rapid investigation of events with minimal disruption.
- Plan and store evidence proactively.
- Demonstrate due diligence in information asset governance.

Typical crimes analysed include IP theft, fraud, identity theft, email abuse, and inappropriate content. Evidence can be in system logs, emails, backups, media, computers, networks, and phone records.

Digital evidence is any data from an information system used in investigations, including internal hearings and legal proceedings.

New digital systems should ensure:

- Evidence gathering without business interference.
- Prioritized evidence collection for significant processes.
- Cost-effective investigation proportionate to incidents.
- Clear evidence impacting investigation outcomes.

Refer to the Trust Confidentiality Audit Policy for audit needs.

6.1.20 Digital forensic investigation

Investigations involving digital evidence require formal case files. Criminal matters must be referred to law enforcement. Digital evidence should be handled as confidential information.

If expertise beyond Trust capabilities is needed, a senior-level risk assessment should consider data loss and system failure against the cost of external forensic experts, involving relevant senior personnel.

NHIS is engaged with Intaforensics as a formal contractual arrangement for digital forensic services. There is an expectation that any identification of the need for digital forensic investigation will then drive decision making on reporting to the national cyber security centre, to the Department of Health and Social Care, and to the Information Commissioner, and NHS Fraud as appropriate.

6.1.21 Cyber Security Risk

Network and system risks cannot be completely eliminated but managed through informed decisions to reduce their likelihood and impact on Trust operations, assets, and confidential information.

NHIS will manage the Trust's cyber security risk by ensuring:

- Secure configuration of digital assets, network, and data
- Regular review of controls' relevance and adequacy
- Real-time monitoring for quick detection and response to events.

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 Committee 360 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

All employment contracts include a confidentiality clause, addressing information security during recruitment and in job descriptions.

Staff receive information security awareness training during induction, with annual updates to keep knowledge current.

As technology evolves, the Trust provides regular security training tailored to staff roles.

Annual data security awareness level 1 training is mandatory for all new starters and existing staff. This can be completed online, covering Data Protection and confidentiality topics.

The training meets statutory requirements for Information Governance in the UK Core Skills Training Framework (UK CSTF), updated in May 2018 to include GDPR.

Senior Information Risk Owner, Information Asset Owners, and Information Asset Administrators must attend regular risk awareness training 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.⁴

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
- Data (Use and Access) Act 2025

⁴ <https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/>

- UK General Data Protection Regulation
- 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: 29 th May 2025			
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 / Belief	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? <ul style="list-style-type: none"> None. 			
What data or information did you use in support of this EqlA? <ul style="list-style-type: none"> 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? <ul style="list-style-type: none"> No. 			

<p>Level of impact</p> <p>From the information provided above and following Equality Impact Assessment guidance on how to complete, the perceived level of impact is:</p> <p>Low Level of Impact</p>
<p>Name of Responsible Person undertaking this assessment:</p> <p>Gina Robinson, Data Security and Privacy Compliance Officer</p>
<p>Signature: G Robinson</p>
<p>Date: 29th May 2025</p>

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.

APPENDIX 3 – REMOTE WORKING SECURITY OBLIGATIONS CHECKLIST

- ☐ Mobile devices and removable media are encrypted in accordance with national NHS requirements (e.g., 256-bit encryption).
- ☐ Only authorised mobile devices and removable media are used for Trust business.
- ☐ Mobile devices and removable media are never employed as the primary source of data. The source data should reside on the Trust's shared drives where backup and security measures can be effectively managed.
- ☐ Portable data (e.g., DVDs/CDs) must be authorised and securely stored, with a record of off-site removal maintained for reference.
- ☐ Mobile devices and removable media are used solely when there is an identified business need pertinent to the staff member's role, as agreed upon with line management.
- ☐ Mobile devices and removable media are kept secure at all times. All staff are responsible for the physical protection against loss, damage, abuse, or misuse. This includes ensuring security during usage, storage, and transit.
- ☐ Mobile devices, particularly laptops, are connected to the Trust's network 'on-site' regularly (recommended once a week) to receive updates, such as antivirus and Windows security updates. In cases where the user is away for an extended period due to health reasons or holiday, or working remotely, the device must be connected upon return.
- ☐ The use of mobile devices and removable media should be minimised in public areas and at home to reduce the risk of shoulder surfing and, consequently, unauthorised access to confidential information.
- ☐ Under no circumstances should confidential information be processed on personal devices, with the sole exception of accessing NHSmail, which is permitted.

Working Offsite Guidelines

- ☐ Treat home workspaces like professional workspaces.
- ☐ Protect devices during transit; treat them as hand luggage. Avoid leaving devices in cars or public areas.
- ☐ Ensure screens are locked if unattended, especially around children/housemates.
- ☐ Position screens to prevent unauthorised viewing (shoulder surfing).
- ☐ Store devices safely and securely at the end of the working day.
- ☐ Do not leave devices unattended in insecure areas (e.g., unlocked house).
- ☐ Close/lock windows and doors when unattended; draw curtains/blinds at night.
- ☐ Log off or lock your computer (Ctrl+Alt+Delete or Windows+L) when unattended.
- ☐ Blur your background during video calls.
- ☐ Ensure conversations are not overheard during calls or video meetings. Conversations should be held in areas where they are less likely to be overheard.
- ☐ Report lost/stolen devices or VPN tokens immediately.
- ☐ Save files to shared drives, not on your devices.

General - No Additional Protection

- ☐ Do not use personal email/messaging for patient/staff data.
- ☐ Return Trust equipment at the end of the remote working arrangement.
- ☐ Assess the need to transport records in order to minimise the risk of data loss.
- ☐ Paper documents should not be taken off-site unless necessary and agreed with Information Governance.
- ☐ Paper documents must be stored and carried securely, not loosely.
- ☐ Use removable media only when required and approved.
- ☐ VPN connections must be properly terminated after use.
- ☐ Maintain a clear desk and clear screen policy. Ensure records are inaccessible to patients, the public, and non-Trust staff.
- ☐ Secure confidential/business-critical information when offices are vacated.
- ☐ Lock external doors and windows when unattended. Consider external protection for ground-level windows.
- ☐ Staff must safeguard username and passwords and not share them.
- ☐ Devices must be secure even when charging or left unattended.
- ☐ Take reasonable steps to minimise theft or damage to Trust property.
- ☐ Change passwords regularly and when prompted.