Public – To be published on the Trust external website

Information Security and Risk Policy

Ref: IT-0010-v7

Status: Ratified

Document type: Policy

Contents

1 Introduction

Staff, patients and their carers and families (data subjects) entrust their most sensitive and private of information to the care of the Trust at a time when they are most unwell and vulnerable.

Information is of greatest benefit and value when it is accurate, up-to-date and accessible where and when it is needed.

It is paramount that staff are aware of the risks associated with handling and using information assets (i.e. both sensitive information and the equipment and systems used to access, store and process that information), and have confidence to work in ways which keep information assets secure.

This policy supports all three strategic goals by pulling together various aspects of legislation and best practice to advise staff of how we work in the Trust to reduce the vulnerabilities that can arise when working with information, systems and equipment.

This policy supports the 8 Caldicott principles, Digital Technology Assessment Criteria (DTAC), the UK data protection legislation (Data Protection Act 2018 and UK GDPR) and the requirements of the NHSE Data Security and Protection Toolkit (DSPT).

The Digital Technology Assessment Criteria for health and social care (DTAC) is the national baseline criteria for digital health technologies entering and already used in the NHS and social care. It brings together legislation and good practice in the areas of:

- Clinical safety
- Data protection
- Technical security
- Interoperability
- Usability and accessibility

The knowledge that DTAC is embedded within the Trust gives assurance to staff, patients, citizens and partner agencies that the digital health tools in use within the Trust meet best practice and statutory standards.

Information Security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the Trust is providing a secure and trusted environment for the management of information used in delivering it business.

- Clarity over the personal responsibilities around information security expected of staff when working on Trust business.
- A strengthened position in the event of any legal action that may be taken against the Trust (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security (including addressing requirements of the Data Security and Protection Toolkit (DSPT) and forms part of the Trust Information Security Management System (ISMS) that conforms to ISO/IEC 27001).
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

2 Why we need this policy

2.1 Purpose

This policy aims to preserve the principles of:

- Confidentiality – That access to data shall be confined to those with appropriate authority and protected from breaches, unauthorised disclosures of or unauthorised viewing.
- Integrity – That information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification and not allow unauthorised modification of data.
- Availability – That information shall be available, delivered to the right person, at the right time when it is needed and protected from disruption, loss and denial-of-service attack.

This policy fits within the Trust’s overall organisational risk framework and is needed to:

- Ensure the Trust complies with data protection and information governance law:
  - This is a legal responsibility for the Trust and for all individuals who work within it.
  - We need to ensure that we have the correct and up to date information; it is available to those who have a genuine need to access, use and

share data; and personal information is kept secure and confidential from those who do not have a genuine need to access, use and share it.

- Help staff keep information about individuals safe, secure, confidential and accurate:
    - We have a duty of confidentiality to our patients and our colleagues.
    - We all, as individuals and as part of the Trust, have a duty of care in keeping person identifiable information (PII) safe, secure and accurate and available to only those who have a genuine need to share, access and use it.
- Advise all Trust users of Trust IT resources and information (see 3.1) on the process of identifying risks when dealing with confidential, restricted or sensitive information whether at rest, in use or in transit.

2.2 Objectives

This policy aims to support staff in identifying an acceptable level of risk when dealing with information. The policy also aims to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and risk management and explaining how they will be handled in the Trust.
- Introducing a consistent approach to information security and risk management, ensuring that all members of staff and, in particular, Information Asset Owners and Information Asset Administrators, fully understand their own responsibilities.
- Creating and maintaining within the Trust a level of awareness of the need for information security and risk management as an integral part of the day-to- day business.
- Protecting information assets under the control of the Trust.
- Protecting the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant.
- Providing a consistent approach to risk management, where information risks are identified, analysed and dealt with in a timely and effective way.
- Identifying an acceptable level of information risk, beyond which escalation of risk management decisions is necessary.

- Safeguarding the Trust’s information assets.
- Safeguarding the reputation of the Trust through the safe and secure use of personal information.

3 Scope

3.1 Who this policy applies to

- All users of the Trust’s Digital and Data systems, services and information including, but not limited to: substantive employees, agency and sub-contract staff, locums, partner organisations, suppliers and volunteers.

3.2 What this policy applies to

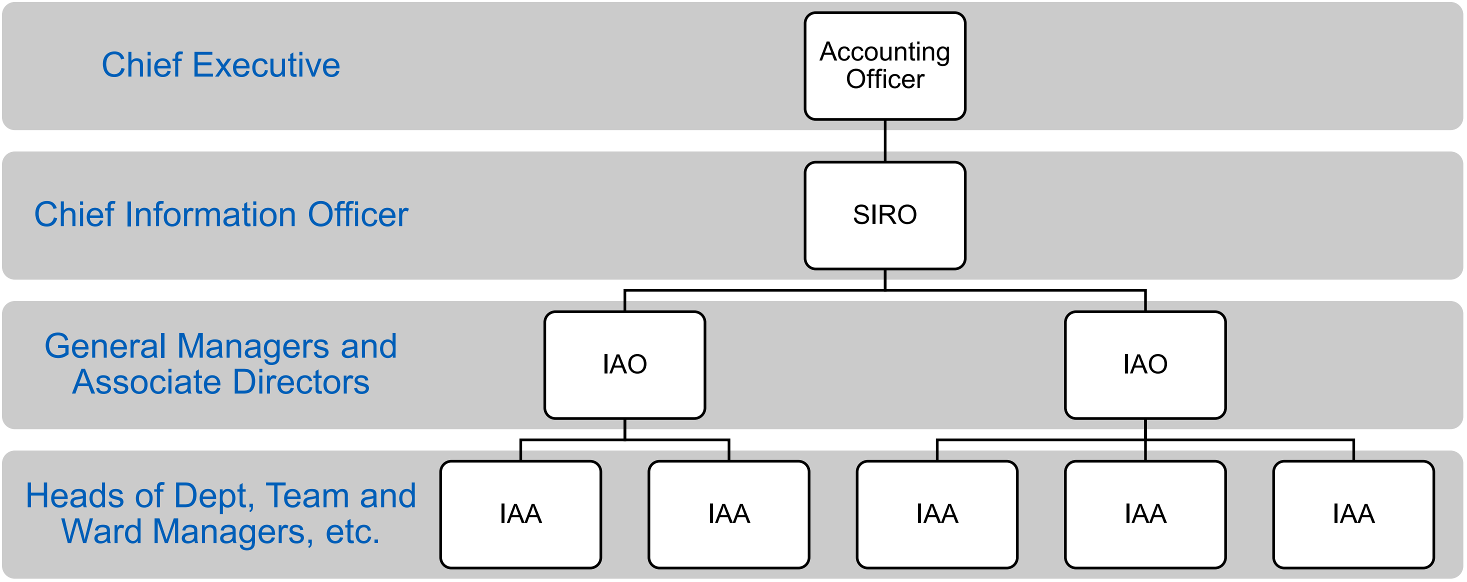
The policy applies to all Trust information assets including but not limited to information systems, networks, applications, locations and equipment under the control of the Trust. It also applies to any future information held by the Trust and any future equipment used to store or process the information.

Only equipment and storage devices that have been provided and/or approved by the Trust may be used to store or process business information, particularly person identifiable information (PII).

This policy includes all IT resources under the ownership of the Trust and applies to:

- All information (digital, hard copy, photographic or audio) collected, processed, stored, produced, and communicated through the use of IT resources by or on behalf of the Trust.
- IT information systems owned by or under the control of the Trust.
- The Trust’s networks, infrastructure, and websites.
- Any device or equipment that connects to the Trust’s network which can access, reproduce, store, process or transmit information.

3.3 Information risk management structure


Chief Executive
Accounting Officer
Chief Information Officer
SIRO
General Managers and Associate Directors
IAO
IAO
Heads of Dept, Team and Ward Managers, etc.
IAA
IAA
IAA
IAA
IAA

Key:

Senior Information Risk Owner (SIRO)

Information Asset Owner (IAO)

Information Asset Administrator (IAA)

3.4 Roles and responsibilities

Role	Responsibility
Chief Executive	Ultimate responsibility for information security and risk management within the Trust.
Senior Information Risk Owner (SIRO)	• Coordinating the development and maintenance of information risk management policies, procedures and standards for the Trust. • The ongoing development and day-to-day management of the Trust's Risk Management Programme for information privacy and security. • The SIRO is supported by Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). • The SIRO advises the Chief Executive and the Trust Board on information risk management strategies and provides periodic reports and briefings on Program progress.
Caldicott Guardian	• Ensuring implementation of the Caldicott Principles, National Data Guardian Standards, and confidentiality and appropriate sharing of service user information throughout the Trust.
Information Asset Owner (IAO)	• Supporting the SIRO in ensuring that information risk assessments are performed on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency. • Submitting risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks. • Ensuring that Digital Technology Assessment Criteria are completed for any new or proposed change to use

	of Trust technology and data (See Digital Technology Assessment Criteria Procedure).
Information Asset Administrator (IAA)	To support the IAO in ensuring that information risk assessments are performed on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency.
Data Protection Officer (DPO)	Ensuring that Data Security and Protection standards are implemented effectively across the Trust, including: • The co-ordination, action planning and reporting of information security work and activity. • Maintaining the Trust's Record of Processing Activities (ROPA) and data flow mapping registers and their regular review. • Ensuring that investigation into all information incidents is completed.
System Owners	Ensuring that the security requirements identified within the relevant system specific policy are embedded in technical and organisational measures.
Line Managers	Ensuring that their permanent and temporary staff and contractors are aware of:- • The information security policies applicable in their work areas. • Their personal responsibilities for information security. • How to access advice on information security matters. • How to identify risks to data confidentiality and how to reduce such risks. • Their individual responsibility for the security of their physical environments where information is processed or stored.
All staff (including those with honorary contract)	• Responsible for operational security of individual information systems and equipment they use, in line with this and other related Trust policies. • To be aware of risks in dealing with confidential or restricted information and to seek advice and guidance

	on how to deal with such risks, in line with Trust policies. • To be alert to any risk of accidentally revealing confidential or restricted information. Each user also needs to be on guard against unauthorized attempts to access information confidential or restricted information. • Complying with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so will result in disciplinary action. • Ensuring that no breaches of IT security result from their actions. • Understand their responsibilities to prevent theft, protect and maintain the confidentiality and integrity of the Trust’s information assets and data and security of the Trust’s networks. • Ensure operational security of information and IT equipment and systems is used. • Participate in training and/or guidance in the use of any IT equipment or systems provided by the Trust in relation to their own duties and responsibilities. • Comply with communications concerning any collective or individual action that must be undertaken in response to potential or actual information security threats. • Understand their responsibilities to accurately enter data into IT systems and take appropriate action to identify and report missing, lost and incorrect data. • Ensure that any incident that could potentially affect the security of information is reported on the Trust incident reporting system in a timely manner.
Incident Investigations Officer	Investigate information incidents and report to the Information Security Officer.
Other Authorised Users of Trust IT Resources	Are personally responsible for ensuring that no breaches of IT security result from their actions and shall: • Comply with this policy, its related processes, guidance and safe working practices.

	- Confirm such agreement in writing, via contract, system access agreement, memorandum of understanding or other mutually agreed mechanism.
System Administrators	All administrators of systems that hold and/or process person identifiable information are required to sign an agreement which acknowledges their enhanced privileges and holds them accountable to the highest standards of use.

4 Policy

4.1 Security and risk

4.1.1 Management of security and risk

Information risk management is part of the Trust's overall risk management framework, as information risk should not be managed separately from other business risks, and will be considered as an element of the overall corporate governance framework.

4.1.2 Information risk assessments

In assessing the risks related to individual information assets priority must always be given to those that comprise or contain personal information about service users, their families, carers and staff.

Information risk is not the sole responsibility of IT or Information Governance staff. All staff have a responsibility to protect the security of confidential information particularly when it is person identifiable. All staff therefore should actively participate in identifying potential information risks in their areas and contribute to the implementation of appropriate action. This requires a structured approach with the clear identification of specific roles and responsibilities to ensure that risks can be managed across all levels in the organisation. The Trust bases this approach on the clear identification of information assets. All information systems and equipment where data is held will be recorded on the Trust's asset register (database). Ownership for each asset is allocated to a senior accountable manager. Information asset administrator roles are allocated to operational staff with day to day responsibility for managing risks within their designated information asset. Administrators are supported where appropriate by the Health Informatics Service (see Home: Health Informatics Service) with responsibility for providing technical assistance on information risk management.

Information risk assessments will be done in line with the Organisational Risk Management Policy and following the national Digital Technical Assurance Criteria (DTAC). Information security risks will be managed by the Information Asset Owner via the Trust's risk management approach.

The Trust employs the DTAC for all new systems and changes to existing systems. This cover 5 key areas, Clinical safety, Data protection, technical assurance, Interoperability, Usability and accessibility.

As required by the Data Protection Act 2018 (GDPR), the Trust has embedded the process for undertaking a Data Protection Impact Assessment (DPIA) for all new systems and changes to existing systems. The DPIA process includes risk assessment and is documented in the DPIA Procedure.

Risk assessment will consider potential impacts on the confidentiality, integrity and availability of systems and data, and the likelihood of those impacts occurring.

In assessing the appropriate level of security, account is taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

All new Trust equipment that is used to store or transfer person-identifiable or business-sensitive data undergoes a standardised risk assessment.

4.1.3 Information security incidents and weaknesses

All information security events, near misses and suspected weaknesses are to be reported to the Information Security Officer. All information security events will be reported on the Trusts risk management system as soon as practicable to enable them to be investigated.

Decisions regarding the management of weaknesses and risks identified through the information risk assessment process are the responsibility of Digital Performance and Assurance Board. The implementation of technical and organisational measures to mitigate risk is monitored by the Cyber Security Group (see 4.2).

4.1.4 Business continuity and disaster recovery plans

Business continuity and disaster recovery plans will be maintained by the system owner. System specific policies must also include this requirement. Plans are developed with information security standards included and are tested annually as a requirement of the Data Security and Protection Toolkit.

4.2 Cyber Security and technical measures

Cyber Security is increasing in importance, particularly because of new technology and ways of working. As a result of these advances, NHS Digital have produced the Digital Security and Protection Toolkit which focusses on Cyber Security and advances in technology.

The Trust has created a Cyber Security Group which meets on a monthly basis and assesses any issues and risks which have been noted, any updates or patches needed to Trust systems and any incidents which have occurred due to technical concerns.

Cyber Security Group monitors the implementation of CareCert (Care Computer Emergency Response) notifications which are received on a weekly basis. These are issued by NHS Digital to support health and social care organisations in responding effectively and safely to cyber security threats. The Cyber Security Group discusses these alerts and the ways in which to disseminate them throughout our network if they are applicable to any of the Trust systems. The group provides assurance of the governance of all technical measures taken by the Trust to adhere to the toolkit and maintain a high level of Cyber Security.

Digital Performance and Assurance Board will undertake a review of cyber security risk and include on the Board Assurance Framework the top 3 cyber risks.

Unless approved by the SIRO, all systems procured for use by the Trust will comply with the minimum requirements set out within the DTAC framework and be assessed to identify potential security threats, vulnerabilities and risks that might be introduced by their implementation.

4.3 Staff training and contracts

4.3.1 Information security and risk awareness training

⚠ All users **must** receive Data Security and Awareness training including information security and risk awareness as described in the Learning and Development Policy appendix 1.

Training is part of induction and is also refreshed annually or when there are changes to systems or legislation. The Trust has processes in place where individuals fail to apply the organisation’s policies and practices, for example further training and guidance and disciplinary measures if appropriate.

4.3.2 Contracts of employments

❗ All staff **must** remember that information security and management of risk is part of our terms and conditions of employment. This means we each have a responsibility to keep personal and restricted information confidential.

Confidentiality and security clauses are written into each staff member’s contract of employment. Volunteers, work placements and other individuals who undertake work on behalf of the Trust but who do not have a contract of employment will sign an undertaking which includes responsibility for security and confidentiality. Those who are paid by another organisation but who undertake work on behalf of the Trust may also be provided with an honorary contract which includes confidentiality and security clauses.

4.3.3 Working abroad

Any staff member who is planning to work from abroad temporarily must have their line manager's authorisation and must sign an undertaking to confirm understanding of their responsibilities for security of their Trust device(s). See the Access to Systems Policy for more information and a copy of the undertaking.

4.4 Security of assets

4.4.1 Control of assets

All IT resources of the Trust (hardware, software, networks, systems or data) are the property of the Trust; they shall be recorded in appropriate asset registers and have a named information asset owner or system manager who is responsible for the control, management and security of that asset.

All information assets will be managed by an Information Asset Administrator (IAA) (see 3.3 and 3.4) who is responsible for maintaining a register of all IT equipment within their area.

The IAA must agree in advance the transfer of mobile devices such as smartphones to other staff and update the asset register accordingly. The device must be returned to the Centralised Asset Management Team prior to being reallocated. This is imperative so the mobile device can be wiped of information and to ensure insecure devices are removed from circulation. If the device is lost, the person named as owner on the asset register will be deemed liable.

Staff moving team within the Trust (who will require the use of a smartphone or other mobile device) must take their existing devices with them to their new Trust role.

4.4.2 Equipment security

All equipment will be physically protected from damage, loss or other hazards at all times including information transfer. Staff are responsible for protecting the assets under their control whilst the Trust retains responsibility for static assets.

4.4.3 Computer and network procedures

Digital and Data Services are responsible for maintaining IT systems and networks, adhering to authorised procedures and best practice. In the event that operation and maintenance of Trust systems and networks outside of authorised procedures is needed, e.g. in response to an incident, disaster recovery and business continuity processes will be followed. Any change to IT systems and networks that does not follow authorised procedures will be considered to be an information incident and managed as such.

4.4.4 Portable media

Staff must only use Trust purchased equipment and encrypted laptops, smart phones and data keys for business purposes.

You must not introduce any portable media - other than those provided and explicitly approved by the Trust – to the Trust's network. Trust approved equipment will always be security marked to show that it is owned by the Trust.

USB ports are locked down to only those portable media devices where a legitimate business need has been identified and agreed, and which are recorded on the Trust's central asset register.

4.4.5 Laptops

Trust issued laptops and tablets must be transported within the locked boot of the car so that the device is out of sight. When travelling on public transport, extra care should be taken to ensure they are not left behind. When transporting to the staff member's home overnight, laptops should be stored within the home out of plain sight, preferably within a cupboard or wardrobe.

4.5 Access controls

4.5.1 User access control

Only those with a justified and authorised need will be given access to restricted areas, e.g. server rooms. Access to restricted areas by non-authorised staff will be considered to be an information incident and managed as such.

4.5.2 Confidentiality

Access to confidential information or restricted information will be given on a need to know basis.

Person identifiable information (PII) including staff and patient records must only be accessed by those with a legitimate need (see Records Management Policy). Accessing PII without a legitimate need and without explicit authority may result in disciplinary action.

Storing Information on a Trust PC - no information should be stored on the hard drive (base unit or C drive) of a desk top computer. This is because the information on that hard drive is not encrypted, so can be viewed by anyone logged onto the computer who can access the C Drive, no matter who they are. This could cause a breach of information in two ways: firstly, the person who could then view the information may not have the legal requirement to be able to access the information, therefore do not have a need to know. Secondly, should the computer be stolen, or accessed inappropriately, they would be able to get the information and use it in whatever ways they like. This would cause a breach which would at the very least, bring the Trust into disrepute and may, depending on the amount, type and number of pieces of information, be subject to scrutiny by the Information Commissioners Office. Finally, information held on a C drive is not backed up. Should your data be corrupted, e.g. a Word document you are working on, this will be lost and might not be retrievable.

Storing information on a laptop – All Trust laptops are encrypted to the NHS standard of AES 256. This means that even if the laptop is stolen, the thief could not gain access to data held on the device. A stolen laptop must be reported on Trusts incident management system and logged with the information service desk as soon as possible. It would then be disabled via Microsoft Defender for Endpoint; should the laptop be found and recovered, it can then be networker-enabled. Information is allowed to be stored on the hard drive of a Trust laptop as it is encrypted; however, information should only be kept there for a short time as no one piece of equipment should be the sole source of information in case of corruption or loss. Once connected to the Trusts network, the information should be transferred to the required network drive, either the home drive if in draft, or the shared drive should others need access.

Other IT equipment – this includes memory sticks, cameras, Dictaphones etc. All of these items must be encrypted where possible. The Trust does not permit general use of memory sticks and such devices are blocked from use. However, there are limited permitted uses, for example retrieval of CCTV footage and disclosure of records for Subject Access Requests, which are permitted on a case-by-case basis. Again, memory sticks and Dictaphones are encrypted to NHS standards but cameras can hold Secure Digital (SD) cards. The cameras themselves cannot be encrypted and only in some cases, will the SD card be encrypted. Local procedures in place where these cameras are used must state in the instructions for use that the SD card is removed from the camera, and the information stored on a nominated place on the network, immediately the camera has finished being used. Likewise, with all other portable information storage equipment, information should be stored on them for the least amount of time possible and should be transferred to the network at the soonest possible stage so that the information can be backed up by the Trust systems.

4.5.3 Computer access control

Except for penetration and vulnerability testing that has been authorised by the SIRO, attempting to gain unauthorised access to Trust data or systems, or seeking and exploiting weaknesses in IT systems or networks for unauthorised purposes, is a serious contravention of Trust policy and a criminal offence. It is strictly forbidden and is not tolerated under any circumstances by the Trust.

> You **must** have a legitimate reason to use the Trust's computing facilities. This means you can only access confidential information if you have a genuine reason such as patient care or to progress the business of the Trust.
>
> If you do not have a genuine reason, you will be subject to the Trust disciplinary procedure.

4.5.4 Application access control

There must be a business need for access to business systems, and authorisation will depend on the availability of licenses for the software being used.

4.5.5 Monitoring system access and use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis. Any monitoring will be undertaken in accordance with the Regulations of Investigatory Powers Act, the Human Rights Act and UK Data Protection Legislation (Data Protection Act 2018 and UKGDPR).

4.6 Moving sensitive information

Where service users' paper records need to be transported, refer to the Trust's Moving Records and Other Sensitive Information Procedure.

4.6.1 Classification of sensitive information

Information will be classified as follows:

NHS Confidential: will be used for patients' clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies (paper/soft copy and electronic).

NHS Restricted: will be used to mark all other sensitive information such as financial and contractual records. This includes information stored on computers, printed out or written, sent by fax or stored on disk etc.

NHS Restricted documents must be stored in lockable cabinets.

4.6.2 Encryption

It is a legal requirement that PII is not sent from the Trust to any external recipient unless the information is encrypted to the NHS Standard of AES256

A matrix of all approved encrypted email addresses is available in the Email Policy. The procedure also describes how to send PII to a non-secure email address using the [secure] process (this is also described in the Communicating with Service Users Procedure). The Trust also allows the use of Egress for any large file transfers outside of NHSmail.

- In any other circumstance, you must seek advice before sending the confidential information from the Digital and Data Services Compliance Team by emailing:
    - tewv.informationsecurity@tewv.nhs to identify a secure process;
    - tewv.isa@nhs.net if this is a new data flow and an information sharing agreement needs to be put in place.

4.6.3 Data transfer and sharing

Only authorised staff may be involved in the process of transferring batched or bulk person identifiable information (PII) by means of portable electronic media.

Contact the Digital and Data Services or Trust Information Security Officer for further guidance on permitted media.

Bulk PII is defined by the NHS Digital as either one piece of data that contains more than 50 pieces of PII or more than 50 separate pieces of data containing PII. If large quantities of paper or electronic data need to be transferred for any reason, you must contact your senior manager to gain permission.

4.6.4 Transfers of personal information outside of the UK

A transfer of personal data to another country or international organisation that is covered by the GDPR (i.e. within the EEA) does not require any specific authorisation providing that the transfer process follows Trust data security requirements.

A transfer of personal data to any other country must be discussed with the Trust's Data Protection Officer to agree how the data will be safeguarded. Email **tewv.dpo@nhs.net**

4.6.5 NHSmail

> Only a Trust-issued NHSmail account must be used for Trust business. Web based emails (such as Hotmail) must never be used for Trust business or sending emails which contain PII.

4.7 Software and systems

4.7.1 Protection from malicious software

Users are prevented from installing software on Trust equipment. All requests for software installation are managed via the procurement process to ensure that proposed software is safe for use within the Trust before it has been purchased. To start the procurement process, log a call via the service desk portal on the staff intranet.

4.7.2 Accreditation of information systems

All new information systems must be vetted via the DTAC process. A system specific policy (SSP) must be produced referencing security management specific responsibilities and, in particular, supplier support arrangements and business continuity and disaster recovery processes. The SSP must be approved by Heads of Information prior to implementation of the system.

4.7.3 System change control

Changes to systems, policy or networks, including reviews and updates, must be reviewed with the involvement of the Digital and Data Services and approved by Change Assurance Group. All new information systems, applications and networks must include a security plan approved by the Digital and Data Services before starting live operation. The DTAC Procedure, Maintenance of IT Systems Policy and Introduction or upgrade of Information Systems Procedure cover in detail the process to be followed for introducing new information systems or amendments to existing systems.

4.7.4 Software copyright

> All information products must be licensed and approved. Users must not attempt to install software on Trust equipment without permission from Digital and Data Services. Users breaching this requirement will be subject to disciplinary action. Only software which is supported by the supplier is permitted on Trust systems. This is to ensure that the products we use remain safe and secure via regular patching and upgrades.

4.8 Information Incident Management

Information incident reporting is in line with the Trust's overall incident management reporting processes. Information incidents will be reported as soon as possible and recorded in accordance with the Incident Reporting Policy, on the Trust's Incident Reporting System. Information incidents involving personal data are to be reported and managed in line with the Trust's Information Incidents Procedure (Confidentiality and Privacy Breaches).

This procedure describes the process to be followed following an information incident to support a fair and open culture. The process puts the person or people affected and the impact upon them at the centre.

5 Reporting

Information incidents are a standard agenda item at the Trust's Information Governance Group. Learning from these incidents is disseminated when needed via Care Board representatives.

The Digital and Data Services and the Information Security Officer will report monthly to the Information Governance Group, Cyber Security Group and Digital Performance and Assurance Group on information and technical security and any related incidents.

6 Definitions

Term	Definition
AES 256 encryption algorithm	• A process for encrypting information.
Availability	• Information must be available and delivered to the right person at the time it is needed.
Confidentiality	• Access to data will be confined to those with delegate authority
Consequence	• The outcome of an event or situation, e.g. loss, injury, disadvantage or gain. There may be a

	range of possible outcomes associated with an event.
DSPT	• Data Security and Protection Toolkit (mandated for NHS organisations by NHS England)
DTAC	• Digital Technology Assessment Criteria
IAA	• Information Asset Administrator
IAO	• Information Asset Owner
Integrity	• Information must be complete and accurate. All systems, assets and networks must operate correctly and to specification.
ISO27001	• The International Standards Organisation guidelines for ensuring personally identifiable information is stored, processed and disclosed lawfully and correctly.
Likelihood	• The probability of the risk event happening.
Person Identifiable Information (PII)	• PII is information that could enable a person's identity to be established by one means or another. This might be fairly explicit, such as an unusual surname or isolated postcode, or bits of different information which if taken together, could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.
Restricted Information	• Information about the Trust that is confidential. This includes financial information or sensitive information about business plans.
Risk	• The chance that damage, loss or injury will occur, which will impact on objectives. It is

	measured in terms of consequence and likelihood.
Risk Assessment	• The overall process of risk analysis and risk evaluation.
Risk Management	• The culture, processes and structures that enable the effective management of potential opportunities and adverse effects.
Risk Management Process	• The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Risk Treatment	• Selecting and implementing options for dealing with risk. Treatment options will involve one or a combination of the following: ○ Avoid the risk. ○ Reduce the likelihood of occurrence. ○ Reduce the consequences of occurrence. ○ Transfer the risk. ○ Retain/accept the risk.
SIRO	• Senior Information Risk Owner. The Trust's SIRO is the Chief Information Officer (CIO).

7 Related documents

Information Governance Policy

Confidentiality and Sharing Information Procedure

Information Incidents Procedure (Confidentiality and Privacy)

Information Asset Procedure

Maintenance of IT Systems Policy and related procedures

Access to Information Systems Policy and related procedures

Records Management Policy and related procedures

8 How this policy will be implemented

- This policy will be published on the staff intranet and on the Trust's external website.
- All staff are notified of the changes to this policy via all staff policy bulletin.
- There are no risks to being able to live the Trust values as a result of implementing this policy.

8.1 Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
N/A				

8.2 Training needs analysis

Role-specific training for key data security and protection roles is identified within a Training Needs Analysis and monitored via the Trust's Data Security and Protection Toolkit submission and related processes.

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	Mandatory Data Security Awareness	2 hours	Annually
New starters	Mandatory induction	1 hour	Once on 1st day of employment

9 How the implementation of this policy will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).

1	Thematic analysis of incident data	Frequency = Monthly
		Method = Analysis of incident data
		Responsible = Information Security and Compliance Team
			Information Governance Group (IG incidents)
			Cyber Security Group (technical security incidents)
			Digital Performance and Assurance Group

10 References

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Computer Misuse Act 1990
- Sexual Offences Act 2003
- Privacy and Electronic Communications Regulations Act 2003
- Confidentiality: NHS code of Practice 2003
- HSCIC Code of Practice on Confidential Information 2014
- Regulatory and Investigative Powers Act 2000
  - NHSE Data Security and Protection Toolkit (DSPT)
  - Digital Technology Assessment Criteria (DTAC)

11 Document control (external)

To be recorded on the policy register by Policy Coordinator

Required information type	Information
Date of approval	21 January 2025
Next review date	21 January 2028
This document replaces	IT-0010-v6 Information Security and Risk Policy
This document was approved by	DPAG
This document was approved	13 December 2024
This document was ratified by	Management Group
This document was ratified	21 January 2024
An equality analysis was completed on this policy on	02 September 2024
Document type	Public
FOI Clause (Private documents only)	N/A

Change record

Version	Date	Amendment details	Status
4	Jan 2015	Added detail around bulk data and portable media/encryption following disestablishment of Portable Media and Encryption Policy	Withdrawn
4	Jan 2017	Review date extended 12 months	
5	Dec 2017	Reviewed and amended in line with GDPR:	Withdrawn

		3.1.2 – two additional paragraphs added 3.1.3 – one additional paragraph added 3.2 – new section re cyber security and technical measures 3.6.3 – new section re transfers of data outside the EEA	
5.1	May 2018	New section 3.4.5 re security of laptops	Withdrawn
6	Aug 2020	Full revision with minor amendments throughout.	Withdrawn
6	May 2023	Review date extended to 31 December 2023	Withdrawn
6	June 2024	Review date extended to 31 August 2024 (agreed Mar 2024)	Withdrawn
7	21 Jan 2025	SIRO structure refreshed in line with current organisational structure Asset Management updated to reference centralised management processes Extensive rewrite reflecting implementation of Digital Technology Assessment Criteria processes for identifying risk Para 4.3 added re working abroad Access Control section 4.5 has been refreshed in line with current best practice Paragraph added at 4.8 to discuss information incident management	Ratified

Appendix 1 - Equality Impact Assessment Screening Form

Please note: The Equality Impact Assessment Policy and Equality Impact Assessment Guidance can be found on the policy pages of the intranet

Section 1	**Scope**
Name of service area/directorate/ department	Digital and Data Services
Title	Information Security and Risk Policy
Type	Policy
Geographical area covered	Trust-wide
Aims and objectives	This policy aims to preserve the principles of confidentiality, integrity and availability and fits within the Trust's overall organisational risk framework. The policy is needed to: • Ensure the Trust complies with data protection and information governance law. • Help staff keep information about individuals safe, secure, and accurate. • Advise all Trust users of Trust IT resources and information on the process of identifying risks when dealing with confidential, restricted or sensitive information whether at rest, in use or in transit.
Start date of Equality Analysis Screening	01 March 2024
End date of Equality Analysis Screening	02 September 2024

Section 2	**Impacts**
Who does the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	The policy benefits all individuals and organisations whose sensitive and personal information the Trust holds, transfers or processes.
Will the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups? Are there any Human Rights implications?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men and women) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women / people who are breastfeeding, women / people accessing perinatal services, women / people on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO** • **Human Rights Implications NO** (Human Rights - easy read)

Describe any negative impacts / Human Rights Implications	None
Describe any positive impacts / Human Rights Implications	Adhering to the policy will ensure the security of information relating to individuals at a time when they are at their most unwell and vulnerable, including sensitive information the Trust may hold relating to a person's protected characteristic(s).

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	NHSE's Data Security and Protection Toolkit National Data Guardian Standards Digital Technology Assessment Criteria UK Data Protection Legislation Incident investigation findings Best practice guidance
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	This policy has undergone full staff consultation. Trust staff comprise all protected characteristics. Digital and Data Services are also engaged in cocreation activities which will be extended to the procedures which staff must follow to ensure the implementation of this policy.
If you answered No above, describe future plans that you may have to	N/A

engage and involve people from different groups	

Section 4	**Training needs**
As part of this equality impact assessment have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	N/A
Describe any training needs for patients	N/A
Describe any training needs for contractors or other outside agencies	N/A

Check the information you have provided and ensure additional evidence can be provided if asked.

Appendix 2 – Approval checklist

Title of document being reviewed:	Yes / No / Not applicable	Comments
1. Title		
Is the title clear and unambiguous?	Yes	
Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2. Rationale		
Are reasons for development of the document stated?	Yes	
3. Development Process		
Are people involved in the development identified?	Yes	
Has relevant expertise has been sought/used?	Yes	
Is there evidence of consultation with stakeholders and users?	Yes	
Have any related documents or documents that are impacted by this change been identified and updated?	N/A	
4. Content		
Is the objective of the document clear?	Yes	
Is the target population clear and unambiguous?	Yes	
Are the intended outcomes described?	Yes	
Are the statements clear and unambiguous?	Yes	

5. Evidence Base		
Is the type of evidence to support the document identified explicitly?	Yes	
Are key references cited?	Yes	
Are supporting documents referenced?	Yes	
6. Training		
Have training needs been considered?	Yes	
Are training needs included in the document?	Yes	
7. Implementation and monitoring		
Does the document identify how it will be implemented and monitored?	Yes	
8. Equality analysis		
Has an equality analysis been completed for the document?	Yes	
Have Equality and Diversity reviewed and approved the equality analysis?	Yes	04/09/2024
9. Approval		
Does the document identify which committee/group will approve it?	Yes	
10. Publication		
Has the policy been reviewed for harm?	Yes	
Does the document identify whether it is private or public?	Yes	
If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	N/A	

11. Accessibility (See intranet accessibility page for more information)		
Have you run the Microsoft Word Accessibility Checker? (Under the review tab, ‘check accessibility’. You must remove all errors)	Yes	
Do all pictures and tables have meaningful alternative text?	Yes	
Do all hyperlinks have a meaningful description? (do not use something generic like ‘click here’)	Yes	