Ref No: CP242

Sheffield Children's NHS Foundation Trust

Corporate Policy

Information Security Policy

Author and Contact Person	Date Approved by Policy Council	Implementation Date	Version number	Issue Date	Review Date
Kevin Connolly, Chief Information Officer	November 2023	November 2023	9	November 2023	November 2028

REQUIREMENT	ACTION
Who should be aware of this policy and where to access it	All colleagues
Who should understand the policy	All colleagues
Who should have a good working knowledge of this policy	All IM&T colleagues, all Managers.
Whether the policy should be included in the General Trust Induction Programme and/or departmental specific induction programme.	Policy content is incorporated into mandatory information governance training. Acceptance of policy requirements is pre-requisite for access to Trust IT network and systems.
Where is the policy available	Trust Intranet
Copy to be sent to HR with a request for inclusion in induction documents	No
Copy to:	Clinical Governance for publishing on Trust Intranet and updating Policy Database
Process for monitoring the effectiveness of this document	Section 6
Patient version.	No
Groups/persons consulted	Information Governance Committee
Training	Key content is covered through mandatory training (Data Security Awareness, e-learning module).
This Policy is subject to the Freedom of Information Act	

CONTENTS

1. INTRODUCTION

This corporate information security policy is a key component of the Sheffield Children's NHS Foundation Trust information governance assurance framework.

This Policy must be followed by all the Trust's employees to ensure adequate safeguards are in place to maintain confidentiality, integrity and availability of Trust information systems. This includes medical devices connected to the Trust's IT network.

We all, as individuals and as part of the Trust, have a duty of care in keeping confidential information safe, secure, accurate and available to only those who have a genuine need to share, access and use it.

This Policy gives guidance to all Trust colleagues on the processes for identifying and managing risks when dealing with confidential, restricted or sensitive information - whether at rest, in use or in transit.

2. SCOPE

This Policy applies to:

- All information, information systems, IT network infrastructure and end user devices used for the processing of Sheffield Children's NHS Trust information.
- All colleagues employed by the Trust, as well as temporary colleagues and contractors granted access to the Trust's information, systems and networks.

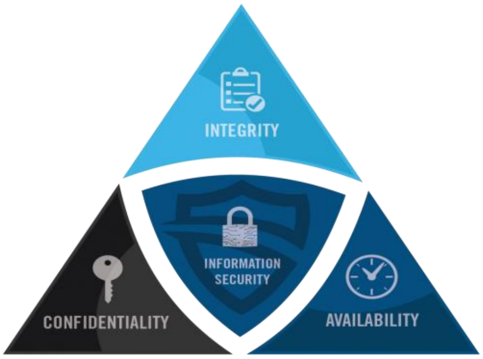
Policy content is aligned to the 10 national data security standards and the assurance requirements set out in the NHS Data Security and Protection Toolkit. The Trust is required to submit an annual assessment which evidences attainment of all standards, with sign-off by Trust Board and supported by formal Internal Audit opinion. This NHS data security assessment framework also incorporates the requirements of all relevant national and international legislation, including:

- The Data Protection Act 2018 (GDPR)
- Copyright Designs, and Patents Act 1988 (as amended by the Copyright Computer programs regulations 1992)
- Computer Misuse Act (1990) (amended in 2005)
- The Common Law of Duty of Confidentiality
- The Freedom of Information Act 2000
- Access to Health Records Act 1990 amended under GDPR
- Crime and Disorder Act 2000
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 and subsequent changes
- The Security of Network and Information Systems Regulations 2018

3. PURPOSE

3.1 Objectives

Threats to the Trust's data will be appropriately identified and based upon a robust risk assessment and management arrangements and will be managed and regularly reviewed to ensure that the objectives of the Trust's Information Security Policy are to preserve:



3.1.1 Confidentiality - Access to Data will be confined to those with appropriate authority to ensure protection against unauthorised access or disclosure.

3.1.2 Integrity – Information will be complete and accurate to maintain integrity and evidential value. All systems, assets and networks will operate correctly, according to specification.

3.1.3 Availability - Information will be available and delivered to properly authorised personnel, at the time when it is needed.

3.2 Policy Aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Trust and where external services impact the Trust services by:

3.2.1 Ensuring that all colleagues are aware of and fully comply with the relevant legislation as described in this and other policies.

3.2.2 Describing the principles of security and explaining how they will be implemented in the organisation.

3.2.3 Introducing a consistent approach to security, ensuring that all colleagues fully understand their own and others' responsibilities.

3.2.4 Creating and maintaining within the Trust a level of awareness of the need for Information Security as an integral part of the day-to-day business and long-term strategy.

3.2.5 Protecting information assets and processes under the control of the Trust.

4. ROLES AND RESPONSIBILITIES

4.1 Reporting to Trust Board

The Trust Board has ultimate responsibility for Information Security within the Trust; however it has devolved responsibility for this Policy and the wider Information Governance Strategy to the Information Governance Committee, which is accountable to the Performance Committee. The Trust's Chief Information Officer is responsible for the effective management of the Information Governance Committee, including appropriate reporting up through the Performance Committee.

4.2 Senior Information Risk Owner (Chief Information Officer)

The Senior Information Risk Owner (SIRO) owns the Trust's information risk and incident management framework, information governance policies and risk assessment processes, ensuring they are implemented consistently.

4.3 Caldicott Guardian (Medical Director)

The Caldicott Guardian's role is to ensure that the Trust satisfies the highest practical standards for handling patient information. The Caldicott Guardian acts as the 'conscience' of the Trust and will actively support work to facilitate and enable information sharing and advise on options for lawful and ethical processing of information as required. The Caldicott Guardian is part of a broader Information Security function.

4.4 Data Protection Officer

The Data Protection Officer (DPO) has a statutory responsibility and is a legal role required by the GDPR. The Data Protection Officer is responsible for overseeing implementation of data protection and security measures to ensure compliance with the GDPR requirements (and in accordance with this Policy).

The DPO will advise the Trust on matters relating to Data Protection regulation and will act as a contact and advice resource for Trust colleagues and the public.

GDPR is very clear that the Data Protection Officer must be able to act independently. Any overruling of DPO recommendations will be documented as an Incident.

4.5 Information Governance Committee

The Information Governance Committee is responsible for ensuring the development and operation of an effective information assurance framework that covers across the scope of the NHS Data Security & Protection Toolkit (and any successor regulatory requirements). The Information Governance Committee is the main forum within the Trust for considering and addressing the impact of changes to national NHS standards and any legal regulations in respect of information governance issues. Hence this primarily includes cyber security, data protection, data quality and records management.

The Information Security Policy will be maintained, reviewed and updated by the Information Governance Committee.

4.6 Information Security Officer

The Trust's designated 'Information Security Officer' leads the implementation and monitoring of the Information Security Policy within the Trust, which includes the following responsibilities:

- To coordinate and direct all Information Security issues and feedback to the Information Governance Committee, Data Protection Officer and SIRO
- To review policies, guidance and action plans developed to meet central and local Information Governance requirements.
- To performance manage action plans and assure the SIRO and Trust Board of Directors (at least annually) that there are effective processes in place for Information Governance compliance, and to report that compliance - annually - through the Data Security and Protection Toolkit.
- To act in an advisory capacity to all colleagues.
- To ensure effective management of the Trust's Cyber Security Group and oversee day-to-day IT security monitoring and incident management activities.

4.7 Cyber Security Group

The Trust's Cyber Security Group meets on a fortnightly basis and assesses performance against IT security indicators and progress on associated action plans. The Cyber Security Group also monitors the implementation of CareCert (Care Computer Emergency Response) notifications received from NHS Digital. Cyber Security Group reviews these alerts, considers their applicability to Trust systems, agrees implementation plans and oversees their completion.

Cyber Security Group also supports the designated Information Security Officer and Data Protection Officer with:

- Co-ordinating communication updates and simulation test exercises to promote user awareness and security compliance all levels of the Trust.
- Continually developing local cyber security processes and procedures.
- Regular reporting and appropriate management of cyber security key performance indicators and risk mitigation measures.

Cyber Security Group reports up to the Information Governance Committee.

4.8 Information Asset Owners (IAOs)

IAOs are senior managers within the Trust, as designated for specific information assets within the Trust (e.g. databases, clinical and business information systems).

IAOs are accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. They are responsible for identifying and documenting information flows in relation to their asset. They ensure that colleagues are aware of and comply with information governance and record management standards for the effective use of information assets.

4.9 Information Asset Administrators (IAAs)

IAAs, often referred to as 'System Managers' are operational colleagues who understand and are familiar with information risks in their area or department. They implement controls and risk assessment processes for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary.

4.10 Managers

Line managers are required to ensure that:

- All permanent and temporary colleagues and contractors are aware of this Information Security Policy and their responsibilities.
- No unauthorised colleagues are allowed to access any of the Trust's information systems, including paper records.
- Colleagues are given access to Trust information systems based on the requirements of their job role.
- All colleagues leaving the Trust complete the colleague leaver's procedures and return all Trust equipment, along with transfer of Trust data from any personal One Drive folders to an appropriate secure location within the Trust's network file storage.

4.11 All Colleagues

All colleagues will comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action. Each colleague will be responsible for the operational security of the information systems they use and how their delegated authorisation is used.

Each system user will comply with the security requirements that are currently in force, and will also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard and they have undertaken the Trust required training. They will learn from common errors as identified through the Trust incident management process.

The Trust will use mandatory training and regular email communication bulletins to improve compliance with Trust requirements and reinforcement of understanding.

5. RELEVANT PROCEDURAL DETAILS

5.1 Information Risk Assessments

5.1.1 Data Privacy Impact Assessments

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 from both a data privacy and data security perspective. Sign-off process involves the Trust's Data Protection Officer.

5.1.2 Information Asset Risk Assessments

Information risk assessments are required for all assets, to 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.

Information asset risk assessments are subject to regular review, so that they take account of vulnerability assessments, frequency of security software updates, levels of vendor support and any previous information security incident reports.

Additionally, procurement processes for any new information technology solutions must include completion of the national Digital Technology Assessment Criteria (DTAC). Advice and signposting for this will be provided by the IT Procurement team, prior to placing any new purchase order. How to use the DTAC - Digital Technology Assessment Criteria (DTAC) - NHS Transformation Directorate (england.nhs.uk)

5.1.3 Incident Reporting

All information security events, near misses and suspected weaknesses are to be reviewed and assessed through the Cyber Security Group. All information security events will be reported on Datix as soon as practicable to enable them to be investigated.

5.1.4 Business Continuity Planning

Information Asset Owners are required to ensure that Business Continuity Plans are maintained and are tested annually as a minimum. This is also a specific requirement of the Data Security and Protection Toolkit.

These asset-level Business Continuity Plans inform the target ‘Recovery Point Objectives’ and ‘Recovery Time Objectives’, to be reflected in IT Disaster Recovery Plans.

5.1.5 IT Disaster Recovery

The Trust’s Information Security Officer must ensure that IT Disaster Recovery Plans are fully documented, made appropriately available to key colleagues and are tested annually as a minimum. In this context a ‘disaster’ is defined as: “An event that results in the loss of vital computer systems for a period of time that significantly and adversely affects the Trust operations”.

In the event of any unplanned downtime for critical assets, upon incident closure a debrief shall be undertaken by the Cyber Security Group and IT Disaster Recovery Plans shall be updated if necessary, to reflect any lessons learned.

5.2 Data Security Monitoring

5.2.1 Audit Logs

Audit trails of system access and data use by colleagues are maintained by the IT Department and reviewed on a regular basis, in accordance with requirements of the Regulations of Investigatory Powers Act and the Data Protection Act 2018 (GDPR).

Where information security incidents occur, the Trust must have an established capability to apply digital forensic techniques that can examine and analyse the data collected and stored and determine if their systems and networks may have sustained any damage, and if sensitive data could or have been compromised.

These digital forensic techniques are incorporated into regular vulnerability assessment including:

- Troubleshooting operational issues, e.g. resolving a functional problem with an application.
- Log monitoring, e.g. assisting in incident handling and system auditing.
- Recovering lost data from systems.
- Acquiring data, for possible future use from hosts that are being redeployed or retired, e.g. when the user leaves the organisation.

- Protecting sensitive information and maintaining certain records for audit purposes: enabling the Trust to notify other agencies or individuals when protected information is exposed to other parties.

5.2.2 Forensic Readiness Procedures

Additionally, these forensic procedures may also be required to support the investigation of reported breach of internal policies and, in some cases, potential criminal activity. Examples may include: internet misuse; email mis-use; electronic bullying and harassment; formal Police requests; fraud and corruption; CCTV footage; network intrusion attempts. Any forensic investigations relating to employee activities must be authorised by a member of the Human Resources senior management team, in accordance with Trust disciplinary and conduct policy.

Standard operational digital forensic tasks will be carried out "in-house" by authorised members of the IT Department, where this can be undertaken through analysis of audit logs described at 5.2.1. above. All such forensic investigation activity will be subject to clear audit trails and scrutiny, to ensure no unauthorised use of 'elevated' IT account permissions.

External third-party organisations may only be used when specialised assistance is needed for complex tasks, such as sending physically damaged media to a data recovery firm for reconstruction or having specially trained law enforcement personnel or consultants collect data from mobile electronic storage devices. These tasks usually require the use of specialised software, equipment, facilities, and technical expertise that it is not viable for the Trust to acquire and maintain.

Any decision to commission external parties for a forensic investigation must be signed off by the Trust's Data Protection Officer or Senior Information Risk Owner.

5.3 <u>Colleague Training</u>

5.3.1 Information Governance Training

Data security awareness training is incorporated into the Trust's Information Governance mandatory training content, applicable to all colleagues and included within the induction programme for all new starters. An ongoing awareness programme will also be maintained to include learning from previous data security incidents and highlight any changes to associated data security procedures as necessary.

5.3.2 Contracts of Employment

All colleagues must remember that information security and data protection are part of our terms and conditions of employment. The requirement for adherence to this policy is also clearly stated in all job descriptions and contracts that allow for access to Trust information systems. This hence includes temporary and agency colleagues and those employed by sub-contractors providing a commissioned service to the Trust.

5.4 Access Controls

5.4.1 Physical Security

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

5.4.2 User Accounts

All IT user accounts and their permitted access levels must be relevant to user roles and business purpose.

User account privileges must be reviewed on a regular basis to ensure these remain current, i.e. access levels must be updated when a user changes their role in the organisation and disabled when a user leaves the organisation.

If colleagues have reason to suspect someone else has accessed their user account, or is trying to access, this must be reported to ICT Service Desk immediately.

Unauthorised use of Trust IT services and information systems will be considered an information governance breach and managed as such.

5.4.3 Remote Access

The Trust maintains a Virtual Private Network (VPN) infrastructure that allows authorised users to remotely connect to the Trust network over an Internet connection. This is secured using two factor authentication. Trust colleagues must only connect through VPN access when using Trust devices, or when accessing via Virtual Desktop Infrastructure (‘VDI’).

Third party suppliers shall also be enabled to connect to specific Trust IT systems, where this is covered in contractual terms, signed off by the Trust’s Data Protection Officer and strictly necessary in order to provide technical support.

Any unauthorised attempt to enable VPN connection from a personal device will be considered an information governance breach and managed as such.

5.4.4 Legitimate Purpose

You must have a legitimate reason and a permitted level of access to use the Trust’s information systems, including access to paper records. Unauthorised access will be considered an information governance breach and managed as such.

In accessing Trust information systems, core confidentiality principles must always be adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.

- If the decision is taken to disclose information, that decision must be justified and documented.

5.4.5 Passwords

Passwords / passcodes must comply with defined complexity requirements per system. Passwords / passcodes must never be shared or disclosed to others. The IT Department will never ask for your password / passcode.

One of the easiest ways to protect from cyber threats is by having a strong and varied password. They are the best form of defence we have to prevent unauthorised access, so all colleagues must make sure to keep their passwords private and out of sight of others.

Weak passwords risk breaches in patient and/or colleague confidentiality. The longer and more complex your password, the more difficult it is to crack. The National Cyber Security Centre have published guidance about how we can best approach passwords/passcodes, available here: The logic behind three random words - NCSC.GOV.UK

5.5 Management of Software

5.5.1 Protection from Malware

Users are prevented from installing software on Trust equipment. All requests for software installation must be made through the ICT Service Desk. Any requests for new software must be managed via a compliant procurement process and must be signed off by the designated Information Security Officer before a purchase order may be placed.

5.5.2 Accreditation of Information Systems

All new information systems must be Trust approved and confirmed by both the designated Information Security Officer and Data Protection Officer. These approvals are incorporated into procurement process and sign-off for relevant Data Privacy Impact Assessments.

5.5.3 Change Control

Changes to existing Trust IT network infrastructure or information systems, including software configuration changes and upgrades, must be reviewed and approved by the IT Change Advisory Board (CAB), as per IT industry standard practice.

All new information systems, applications and networks must include a system specific security plan, approved by the Trust's designated Information Security Officer, before starting live operation.

5.5.4 Software Licensing

All software installed for use via Trust devices must be appropriately licensed and supported by the software supplier. Users must not install software on Trust equipment without permission from the IT Department.

Web versions of the Office365 productivity applications may be used on personal devices, but “full client” versions of the software must not be installed on personal devices using Trust credentials.

Unauthorised software installation and use will be considered an information governance breach and managed as such.

5.6 End User Devices

5.6.1 Trust Devices

Trust owned devices have been purchased by the Trust and provided to an employee for work purposes. These include but are not limited to desktops, laptops, tablets and mobile phones.

Trust devices will have approved IT security software that protects the device from malware and other malicious activities.

Trust devices must be used wherever possible as the installed software has been designed to maintain the confidentiality, integrity and availability of Trust data. Where laptop devices have been allocated to Trust colleagues, these must be connected to the Trust network wherever possible, whether on-site or via VPN secure remote access when working off-site.

5.6.2 Portable Media

Any portable media must be Trust approved and virus checked. Colleagues 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 information asset register.

5.6.3 Personal Devices

A personal device is one that has been purchased by an individual for their personal use. These include but are not limited to desktops, laptops, tablets and mobile phones.

Personal devices may only be used to connect to the Trust's IT network and information systems in the following circumstances:

- Trust approved clinical and business applications may be installed as applications on personal devices, with the list of approved applications published on the intranet. These applications shall ensure that no data can be stored locally and/or enforce other security measures on the device. Virtual Desktop Infrastructure (VDI) is one such application, which allows users to access Trust information and applications remotely, secured using two factor authentication (something you know and something you have). Technical controls prevent data from being copied from the VDI environment to local storage on the personal device.
- Connection to NHS public WiFi is also available and permitted on Trust sites.

5.6.4 Medical Devices

Within this Policy, we are concerned with medical device appliances and/or software, connected to the Trust's IT network and/or internet. For such information assets, it is essential that these are managed in accordance with relevant national NHS England guidance, as here: Guidance on protecting connected medical devices - NHS Digital.

The Trust's Medical Equipment Management Group will maintain oversight on a Medical Devices Register, which will include the following information for each device: IP and MAC address, network connectivity, remote access arrangements for the supplier. This Register will also be periodically reviewed and risk assessed by the Trust's Cyber Security Group.

Procurement, installation and change management for connected medical devices must follow comparable processes as those in place for core network, servers and end user devices. This is reiterated in the Data Privacy Impact Assessment procedure and Medical Equipment Management Policy.

5.7 Data Management

5.7.1 Use of Trust Devices – working on-site:

For users working on site, you will be connected to the Trust IT network, so all created or modified data files should be saved either to a Trust network drive, or NHS 'OneDrive' storage, or NHS Teams file repositories.

For data files that you wish to keep private to yourself, save to your F: drive or your NHS 'OneDrive' storage.

For data files that you wish to share with others, save to the G: drive or to NHS Teams file repositories.

5.7.2 Use of Trust Devices - when working off-site:

For users working off-site, you are required to connect to the Trust IT network via secure Virtual Private Network (VPN) wherever possible, to ensure full access to network folders and to enable timely security 'patch' updates when these are pushed out to Trust devices.

When working off-site, you should save Trust data files to network folders in the same way as when working on-site.

All assigned Trust devices must be connected to the Trust network wherever possible, as per para 5.4.3 regarding secure remote access and para 5.6.1 regarding security updates for Trust devices. Where devices are identified as not having been connected to the network over a 30 day period, these may be temporarily disabled by the Trust's IT team, pending recall for installation of security software updates and re-allocation where applicable.

5.7.3 Storing data on computer hard drives (C: drive):

Data must only be saved to local storage in an emergency, i.e. when there are no Trust network, NHS OneDrive or NHS Teams options available. An example would be during IT network downtime or internet outage. In these circumstances, any data files that are temporarily saved to local storage must then be moved to the appropriate storage location as soon as possible once connectivity is re-established.

It is essential all users recognise that any data stored locally is not backed up, may not be fully encrypted and data could hence be removed automatically by IT maintenance activity or lost or stolen, without options for data recovery.

Any loss of Trust data must be reported on Datix as an information governance incident.

5.7.4 Secure Disposal of Trust Devices

All departments must identify all IT equipment no longer in use and notify this to the IT department, for secure disposal. All hard discs shall be physically destroyed by the IT Department. Use of overwriting shall not be undertaken due to the risks associated with disclosure of sensitive data.

Hard disks shall not be allowed off-site for repair by third parties unless this has been specifically approved by the Trust's designated Information Security Officer, and then only under strict oversight and controls.

Other memory storage devices not mentioned above will be physically destroyed when no longer required.

5.7.5 Use of Personal Devices

The following requirements relate to the management and storage of data files when using a personal device, i.e. where such use is permitted through provisions described at paragraph 5.6.2.

- Data files relating to Trust business must be saved to either NHS OneDrive storage, or NHS Teams file repositories, unless connecting through the Trust's Virtual Desktop (VDI) in which case data may be saved to appropriate network folders.
- For data files that you wish to keep private to yourself, save to your NHS 'OneDrive' storage.
- For data files that you wish to share with others, save to MS Teams file repositories.
- Trust data files must not be saved or synchronised to local storage on personal devices.

Unauthorised use of personal devices will be considered an information governance breach and managed as such.

5.8 <u>Transferring Sensitive Information</u>

5.8.1 Encryption

It is a legal requirement that person-identifiable data is not sent from the Trust to any external recipient unless the information is encrypted to the NHS Standard of AES256 at all stages of data transfer.

5.8.2 Email

Colleagues must use their Trust-issued NHSmail accounts for the purpose of all Trust business.

Web based personal email accounts (such as Hotmail, Gmail) must never be used for sending emails which contain person-identifiable information. Any such use must be reported as an information governance breach and managed as such.

5.8.3 Secure File Transfer

NHSmail fully supports secure transfer of person-identifiable information when sending to other NHSmail accounts, although colleagues are required to ensure that there is also a legitimate basis (in accordance with Data Protection Act 2018) for such data sharing before sending. Advice should be sought from the Trust’s Data Protection Officer wherever required.

NHSmail also enables secure transfer of person-identifiable data to non-NHSmail addresses, using the [secure] process described in procedural detail here: *Axe the Fax - Sheffield Children's NHS Foundation Trust Intranet (sch.nhs.uk).*

The Trust also allows the use of Egress for any large file transfers outside of NHSmail, subject to prior approval from the Trust’s Data Protection Officer.

5.8.4 Bulk Data Sharing

Bulk transfer of person-identifiable information, which may relate to either a one-off or a regular recurring data flow, is defined by NHS Digital as either:

One data file containing 50 or more pieces of person-identifiable information, or

Or 50+ separate data files each containing person-identifiable information.

If any such large quantities of paper or electronic data need to be transferred outside the organisation, where these are new data flows prior approval must be sought, the process for which will require completion of a Data Privacy Impact Assessment and sign-off from both the Trust’s Caldicott Guardian and Data Protection Officer.

Any unauthorised data flow involving transfer of person-identifiable data must be reported as an information governance breach and managed as such.

5.8.5 Transfers of personal information outside of the UK

A transfer of personal data to another country or international organisation that is covered by GDPR (i.e. within the EEA) does not require any specific authorisation, other than that described at 5.8.4. above, providing that the transfer process follows Trust data security requirements.

A transfer of personal data to any other country must be approved by the Trust’s Data Protection Officer in order to confirm how the data will be safeguarded.

5.8.6 Equipment Security

Trust devices must be protected from theft, or the risk of other unauthorised access, at all times. Mobile devices should be kept under lock and key when not in use and must not be left unattended in public places at any time.

6. PROCESS FOR MONITORING COMPLIANCE WITH THE POLICY

Minimum Requirement to be Monitored	Process for Monitoring	Designated Group	Frequency of Monitoring	Responsible Group for Reviewing Results	Allocated Group for Action Plans	Responsible Committee
All Policy requirements, as per Data	Self-Assessment	Cyber Security Group	Fortnightly	Information Governance Committee	Information Governance Committee	Performance Committee

Security & Protection Toolkit standards.						
All Policy requirements, as per Data Security & Protection Toolkit standards.	Internal Audit Review	360 Assurance	Annual	Information Governance Committee	Information Governance Committee	Risk & Audit Committee

7. REFERENCES

- NHS Data Security and Protection Toolkit
- Confidentiality: NHS Code of Practice
- Caldicott / Caldicott 2 Report (1997/2010)
- Information Security Management NHS Code of Practice 2007
- Records Management Code of Practice for Health and Social Care 2016
- The Data Protection Act 2018 (GDPR)
- Copyright Designs, and Patents Act 1988 (as amended by the Copyright Computer programs regulations 1992)
- Computer Misuse Act (1990) (amended in 2005)
- The Common Law of Duty of Confidentiality
- The Freedom of Information Act 2000
- Access to Health Records Act 1990 amended under GDPR
- Crime and Disorder Act 2000
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 and subsequent changes
- The Security of Network and Information Systems Regulations 2018

8. ASSOCIATED DOCUMENTS

- Information Governance Strategy
- Data Protection Policy
- Clinical Records Management Policy
- Non-Clinical Records Management Policy
- Medical Equipment Management Policy

9. EQUALITY IMPACT ASSESSMENT

This policy applies to all Trust employees irrespective of age, race, colour, religion, belief, disability, nationality, ethnic origin, sexual orientation or marital status, carer status, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner.

The Trust will take account of any specific access or specialist requirements (e.g. BSL Interpreter, documents in large print) for individual employees during the implementation of this policy.

10. VERSION CONTROL

Version	Date	Author	Status	Comment
1	August 2009	Russell Banks	Archived	Final Draft
2	November 2010	Russell Banks	Archived	Minor changes
3	April 2013	Russell Banks	Archived	Minor changes
4	December 2016	Russell Banks	Archived	Minor changes
5	December 2018	Russell Banks	Archived	Minor changes reflecting GDPR and related updates to associated Trust IG policies. Incorporation of additional content from previous related policies (CP809, CP1507, CP1508).
6	December 2021	Kevin Connolly	Archived	Minor changes
7	April 2022	Kevin Connolly	Archived	Major version change to reflect Trust-wide move to Office365 and extent for permitted use of personal devices.
8	June 2023	Kevin Connolly	Archived	Minor update to include section 5.6.4 regarding connected medical devices
9	November 2023	Kevin Connolly	Approved	Update to include line manager responsibilities (section 4.10) and strengthen requirements for legitimate access to confidential information (section 5.4.4) and device security (section 5.6.1).