Ref No: CP242

Sheffield Children's NHS Foundation Trust

Corporate Policy

Information Security Policy

Author and Contact Person	Date Approved By Information Governance Committee	Version number	Issue Date	Review Date
Russell Banks	10 January 2019	5	January 2019	January 2022

REQUIREMENT	ACTION
Who should be aware of this policy and where to access it	All staff
Who should understand the policy	All staff
Who should have a good working knowledge of this policy	All IT staff, all Managers.
Whether the policy should be included in the General Trust Induction Programme and/or departmental specific induction programme.	Be available to all service users
Where is the policy available	Trust Intranet
Copy to be sent to HR with a request for inclusion in induction documents	No
Copy to:	Legal & 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	Pre-requisite for access to Trust IT network and information systems. Key content is covered through mandatory training (Data Security Awareness, national 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, (hereafter referred to as the Trust) overall information security management framework and should be considered alongside the more detailed information security documentation listed in sections 5.1 and 5.2, including, system level security policies, security guidance and protocols and/or procedures.

This policy document will be followed by all the Trust's employees to ensure adequate safeguards are in place to maintain confidentiality, integrity and availability of information held on individuals and wider Trust matters.

This Information Security Policy update also incorporates the requirements of other related policies that had previously existed within the Trust, namely:

CP809	Network Security Policy
CP1507	Mobile Computing Policy
CP1508	Remote Access Policy

2. PURPOSE

2.1 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:

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

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

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

2.2 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:

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

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

2.2.3 Introducing a consistent approach to security, ensuring that all members of staff fully understand their own and others responsibilities.

2.2.4 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.

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

2.3 Scope

This policy applies to all Trust IT network infrastructure, information systems, interfaces, information processing, data and users - across all locations this infrastructure and data is hosted and accessed from.

The General Data Protection Regulation is closely aligned to the security of information and a responsibility of the Trust is to ensure its security arrangements are robust and enough to ensure the safety of individuals' data.

3. ROLES AND RESPONSIBILITIES

3.1 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 Finance & Resources Committee. The Trust's Chief Information Officer is responsible for the effective management of the Information Governance Committee, including appropriate reporting up through the Finance & Resources Committee.

3.2 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.

3.3 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.

3.4 Clinical Safety Officer (CSO)

The Clinical Safety Officer has lead responsibility for ensuring information systems are safe for use in a clinical setting and therefore will have an important role in assessing information security within clinical applications and systems.

3.5 Data Protection Officer (Head of IM&T)

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 staff 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.

3.6 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. This review will take place every three years, unless significant developments prompt policy amendment.

3.6 Head of IM&T

The Head of IM&T leads the implementation and monitoring of the Information Security Policy within the Trust, which includes performing the following tasks:

- 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 staff.

3.7 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 staff are aware of and comply with information governance and record management standards for the effective use of information assets.

3.8 Information Asset Administrators (IAAs)

IAAs, often referred to as 'System Managers' are operational members of staff 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. senior managers within the Trust, as designated for specific information assets within the Trust (e.g. databases, clinical and business information systems).

IAOs and IAAs are together responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies, procedures applicable in their work areas
- Their personal responsibilities for information security and ensure they comply with training requirements
- Manage user access to information systems they control in accordance with the Trust standards
- How to access advice on information security matters
- Identifying those assets that have not complied with the Trust standard for managing assets.

Line managers/IAOs are also responsible for ensuring the security of their physical environments where information is processed or stored locally.

3.9 All Staff

All staff 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 member of staff 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 training to improve compliance with Trust requirements and reinforcement of understanding.

4. CONTRACTORS/AGENCY/TEMPORARY STAFF

These staff will have a contract either via Agency/Contractor or via a supplies purchase order. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with this Policy.

Access to Trust IT network and information systems will be restricted and on a need to know basis. Any authorisation will be de-registered once the contract/employment ends. Should these individuals have administrative access to systems these must be changed once contract/employment ends.

5. LEGAL AND PROFESSIONAL OBLIGATION

5.1 Legal Framework

The Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of the Trust, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Trust will comply with the following legislation and other legislation/requirements as appropriate:

- 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

5.2 Management of Security

- Reporting to Trust Board level, responsibility for Information Security will reside with the Chief Information Officer (SIRO).

- The Head of IM&T will be responsible for implementing, monitoring, documenting and communicating security requirements for the Trust. Management of tasks associated with this may be delegated to other IT Leads.

5.3 Information Security Awareness Training

- Information security awareness training will be included in the staff induction process and in staff ongoing mandatory training.
- An ongoing awareness programme is in place and maintained in order to ensure that staff awareness is refreshed and updated as necessary.
- The Information Governance/Security Officers will deliver mandatory annual training using standard tools provided by NHS Digital through the CareCERT and CSP programme.

5.4 Contracts of Employment and Procurements

- Staff security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause.
- Information security expectations of staff will be included within appropriate job definitions.
- Contracts for goods and services will contain appropriate governance clauses through NHS Supplies.
- Contracts outside this process will require Data Sharing Agreements acting as contracts.

5.5 Security Control of Assets

Each IT asset, (hardware, software, application or data) will have named Information Asset Owners and Information Asset Administrators who will be responsible for the information security of that asset. An asset register is maintained for key assets.

5.6 Access Controls

Only authorised personnel who have a justified and approved business need will be given access to restricted areas containing network infrastructure, information systems or stored data. Procedures for IT access controls are managed by the Head of IM&T.

5.6 Access Control to the Network

Other access to information will be restricted to authorised users who have a bona-fide business need to access the information via the IT network access form. Where access to systems is controlled by IAOs this will be achieved through a similar process.

- Access to the restricted network resources will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- A formal, documented user registration and de-registration procedure for access to the network will be maintained and all information assets will conform to this registration process.
- Security privileges (i.e. 'Admin' or network administrator rights) to the network resources will be allocated on the requirements of the user's job and need for access.
- All users to the network and resources will have their own individual user identification and password and will be provided by the IT department (or System IAO) through their user access procedure. Shared logins will only be allowed on an exceptional basis and only with the specific authorisation of the Head of IM&T.
- Users are responsible for ensuring their passwords are kept secret and IT will maintain a user guide for passwords which IAO controlled systems must conform to.
- User access rights will be removed from any system as soon as practically possible for staff who have left the Trust (or reviewed for those who have changed role).
- Passwords will conform to the password guidance document and will include a lock out facility for repeated attempts.
- Incidents involving Trust staff where access needs to be changed must be done with coordination with the Head of IM&T and HR department.

5.7 External Access Controls

External network connections and all third party access to the network and or resources connected to the network must be approved through an appropriate data sharing agreement and must also be based on a formal contract that satisfies all necessary NHS security conditions.

In practical terms, all third party access to these resources must be authorised by the Head of IM&T as a central point of control and will follow completion of the relevant third party access documentation.

5.8 Remote Access to the Trust Network and Telephony Services

Remote Access (in this instance) refers to any technology that enables the Trust to connect users in geographically dispersed locations to the Trust network and its resources. Risks to network resources must be mitigated by:

- Remote access will only be permitted through the IT managed VPN mechanism unless it has been agreed this will happen via the NHS network or services are managed via a demilitarised zone.
- No external modem type access will be permitted.
- Having a clear authorisation mechanism for all remote access users.
- Periodic review of this access, which could include but is not limited to independent third party penetration testing will be undertaken.
- Dial in access tokens (which are used to enable secure access) will be maintained and logged by IT and enable users via a cisco VPN to connect to a virtual desktop session and gain access to Trust resources.

5.9 Remote diagnostic services and 3rd parties

Suppliers of central systems/software expect to have dial up access to such systems on request to investigate/fix faults. The Trust will permit such access subject to it being initiated by the appropriate IAO and authorised by the Head of IM&T. A physical or software token for strong authentication will be used and maintained by the IT department. Software applications used to enable access will only be permitted by the Head of IM&T.

Each supplier or Trust user requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified representatives and software. Completion of the relevant IT documentation is also required.

Each request for dial up access will be authorised by approved computer services staff, who will only make the connection when satisfied of the need.

5.10 Computer Access Control

Access to network infrastructure, information systems or stored data will be restricted to authorised users who have business need to use the facilities.

5.11 Application Access Control

Access to infrastructure, data, system utilities and program source libraries will be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application will depend on the availability of a licence from the supplier.

5.12 Computer and Network Procedures

Management of key computers and networks will be controlled through standard documented procedures that have been authorised by the Trust's Information Governance Committee.

5.13 Information Risk Assessment

The core principles of risk assessment and management require the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks will be managed on a formal basis. They will be recorded within the Trust risk register and action plans will be put in place to effectively manage those risks. The Trust risk register and all associated actions will be reviewed at regular intervals. Any implemented information security arrangements will also be a regularly reviewed feature of the Trust's risk management programme. These reviews will help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.14 Information security events and weaknesses

All information security events and suspected weaknesses are to be reported through the Trust's incident reporting system. All information security events will be investigated to establish their cause and impacts with a view to avoiding similar events.

5.15 Classification of Sensitive Information.

A consistent system for the classification of information within the NHS organisations enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-NHS bodies

The Trust will implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Security and Protection Toolkit to secure the Trust's information assets.

Classification of records will conform to the NHS Records Management Code of Practice for Health and Social Care 2016.

5.16 Protection from Malicious Software

The Trust will use software counter measures and management procedures to protect itself against the threat of malicious software, including virus and malware checks.

Users will not install software on the organisation's property and equipment without permission from the Head of IM&T. Users breaching this requirement may be subject to disciplinary action.

The IT department will react to threats as quickly as possible and will take appropriate action followed by formal reporting of actions to the IG Committee.

5.17 Portable Devices

The Trust will only issue network portable devices which meet its security standards and have appropriate security mechanisms installed. This will include:

- Password and encryption measures as appropriate to the device and meeting NHS requirements. All appropriate security measures will be activated before the device is issued or permitted access.
- Corporate data stored on portable devices must be backed up to a network file server as frequently as possible.
- Sensitive data, including that relating to patients, must be kept to the minimum required for effective business use in order to minimise risks should a breach of security or confidentiality occur and maintained in a secure state.
- Corporate portable devices will be issued to staff only through IT.
- A register of corporate portable device users and equipment will be maintained by IT.

- Mobile devices must be protected from theft and malicious software (e.g. viruses). They must never be left unattended, particularly in vehicles or other easily accessible areas. If at all possible devices should be kept under lock and key when not in use. Care must also be taken in public places as highly visible equipment can attract the attention of thieves.
- Connection must occur once in a maximum of 3 months otherwise the device may cease to function and will then warrant a return to IT.

5.18 Monitoring System Access and Use

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

5.19 Security Monitoring

Network service reviews will be undertaken to identify areas of weakness, and intrusion detection systems may be used to monitor and reactively respond to security events as they occur. Network Penetration Testing will be undertaken on an annual basis.

The Trust will action CareCert notifications from the NHS and have a programme of software updates to minimise Cyber risks.

The IT Security Group will monitor and manage methods used to support these activities.

5.20 Accreditation of Information Systems

The organisation will ensure that all new information systems, applications, processes and networks which hold or process individuals information will be subject to Data Protection Impact Assessment (DPIA) process, and the completion of Systems Safety Checklists (SSD) as required.

5.21 System Change Control

Configuration changes to networks, information systems or applications (including installation of additional devices or systems) must be reviewed and approved by the IT 'Change Advisory Board', as set out in the IT Change Management Policy.

5.22 Intellectual Property Rights

The Trust will ensure that all information products are properly licensed, supported and approved by the Head of IM&T. Users will not install software on the organisation's property without permission from the Head of IM&T. Users breaching this requirement may be subject to disciplinary action.

5.23 Data Backup and Restoration

- The Head of IM&T and IAOs must ensure that backup copies of network configuration data and their managed information assets are taken regularly.
- Recovery of sampled material should be undertaken to ensure viability of the backups.
- Documented procedures for the backup process and storage of backup tapes will be maintained and communicated to relevant staff.
- All IT core backups will be stored securely. Ad hoc and standalone systems managed by IAOs will have backups maintained in the same manner.
- Backups of users PC/remote drives will not be undertaken by IT and are seen as transient as all relevant information should be kept on the Trust network drives. A general standard network drive backup schedule will be maintained of nightly snapshots of changes, unless differently agreed with specific IAOs.

5.24 Secure Disposal or Re-use of Equipment

- All hard discs will be physically destroyed or kept in the IT department until destruction is possible. Use of overwriting will not be undertaken due to the risks associated with disclosure of sensitive data.
- All departments will dispose of IT equipment through the IT department.
- Hard disks will not be allowed off site for repair by third parties unless they have been approved by the Head of IM&T and then only under strict control.
- Floppy discs, CD/DVDs, video tapes, flash cards and other memory storage devices not mentioned above will be physically destroyed when no longer required.

5.25 Business Continuity Planning

Business Continuity planning with respect to IT infrastructure and information assets is partially, but not wholly, an IT issue. IAOs must ensure that all of the following contingency actions are carried out, for all key information assets:

- Documented assessment of how long users could manage without access to each key IT system
- Documented assessment of the criticality of each system, including the impact of a short, medium or long term loss of each system upon the Trust's business activities
- Identification and agreement of all responsibilities and emergency arrangements
- Documentation of agreed contingency procedures and processes
- Ongoing action plans to further mitigate potential risks, as far as possible.

5.26 IT Disaster Recovery

In addition to these contingency plans, it is equally essential that suitably detailed Disaster Recovery Plans are in place. This is to ensure that essential operations are restored as soon as possible, in the event of a 'disaster' - defined as: "An event that results in the loss of vital computer systems for a period of time that would significantly adversely affect the Trust's operations".

The Head of IM&T is responsible for ensuring disaster recovery plans are in place, and associated risk assessments are carried out, in respect of the Trust's hosted IT systems.

The Head of IM&T will ensure that the IT Disaster Recovery Plan is developed and reviewed annually, with updates made whenever new IT systems are introduced into the Trust's IT infrastructure. This Disaster Recovery Plan must include:

- Identification of areas of substantial risk and exposure to disaster, and subsequent risk mitigation strategies
- Available technical, operational and procedural documentation for IT staff to follow to ensure a controlled restoration of the Trust's IT infrastructure in the event of a disaster
- Assurance that appropriate communications protocols are in place and commonly understood throughout the period of IT downtime (consistent with departmental Business Continuity Plans as per above)
- Checklist of services that may be impacted and key contacts for reference by IT staff – either when organising periods of planned downtime or when responding to a significant incident ('disaster').

5.27 Reporting

The Heat of IM&T will keep the Information Governance Committee informed of the information security status of the Trust by means of reports and presentations with annual assessments such as the Data Security and Protection Toolkit, Network Patching Status, Incidents and Untoward Events.

5.28 Management of the Working Environment

Users must ensure that they protect information assets from unauthorised access or inappropriate disclosure. The Trust intends to operate a clear screen policy that means that users must ensure that any equipment "logged on" must be protected if they leave it unattended, even for a short time. Devices must be locked or have a screensaver password activated if the device is left unattended even if just for a short time.

6. PROCESS FOR MONITORING COMPLIANCE WITH THE POLICY

This policy will be subject to audits managed by the Information Governance Committee. The Information Governance Committee and Data Protection Officer will instigate annual announced and unannounced spot checks for monitoring and compliance. The Trust will also be externally checked for compliance through various audits by internal auditors.

7. REFERENCES

- CSP Cyber Security Programme (Data Security and Protection Toolkit)
- CareCERT (NHS Digital)
- Confidentiality: NHS Code of Practice
- Caldicott / Caldicott 2 Report (1997/2010)
- Information Security Management NHS Code of Practice 2007
- SCH Network Security Policy
- SCH Information Governance Policy
- SCH IG Key Points and Guidance for Staff
- Records Management Code of Practice for Health and Social Care 2016

8. ASSOCIATED DOCUMENTS

- SCH Clinical Records Management Policy
- SCH Non-Clinical Records Management Policy
- Data Security and Protection Toolkit

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
2.1	April 2011	Russell Banks	Archived	Minor changes
3	April 2013	Russell Banks	Archived	Cosmetic changes to bring in line with Policy format
4	December 2016	Russell Banks	Approved	Minor changes. Amended to reflect changes to SIRO and Sub-Committee reporting arrangements
5	December 2018	Russell Banks		Minor changes reflecting GDPR and related updates to associated Trust IG policies. Incorporation of additional content from previous related policies (CP809, CP1507, CP1508).