# Policy:

## IMST 003 - Data & Information Security

*(Review Date Amended)*

| | |
|---|---|
| Executive or Associate Director lead | Executive Director of Finance & SIRO |
| Policy author/ lead | Assistant Deputy Director of IMS&T (Informatics and Architecture) |
| Feedback on implementation to | Assistant Deputy Director of IMS&T (Informatics and Architecture) |

| | |
|---|---|
| Document type | Final Draft |
| Document status | Version 1.1 |
| Date of initial draft | 18/10/2019 |
| Date of consultation | |
| Date of verification | 11/11/2019 |
| Date of ratification | 21/11/2019 |
| Ratified by | Executive Directors' Group (EDG) |
| Date of issue | 26/11/2019 |
| Date for review | 31/3/2022<br>*(Amended from 31/3/2020 as instructed by Policy Governance)* |

| | |
|---|---|
| Target audience | SHSC staff and people authorised to access the SHSC network |

| | |
|---|---|
| Keywords | Security, Access, Data & Information, Network |

**Policy Version and advice on document history, availability and storage**

Expands Information Security Policy 1.5, aligning with new overarching Data & Information Governance and supporting policies including security for data, information and systems.

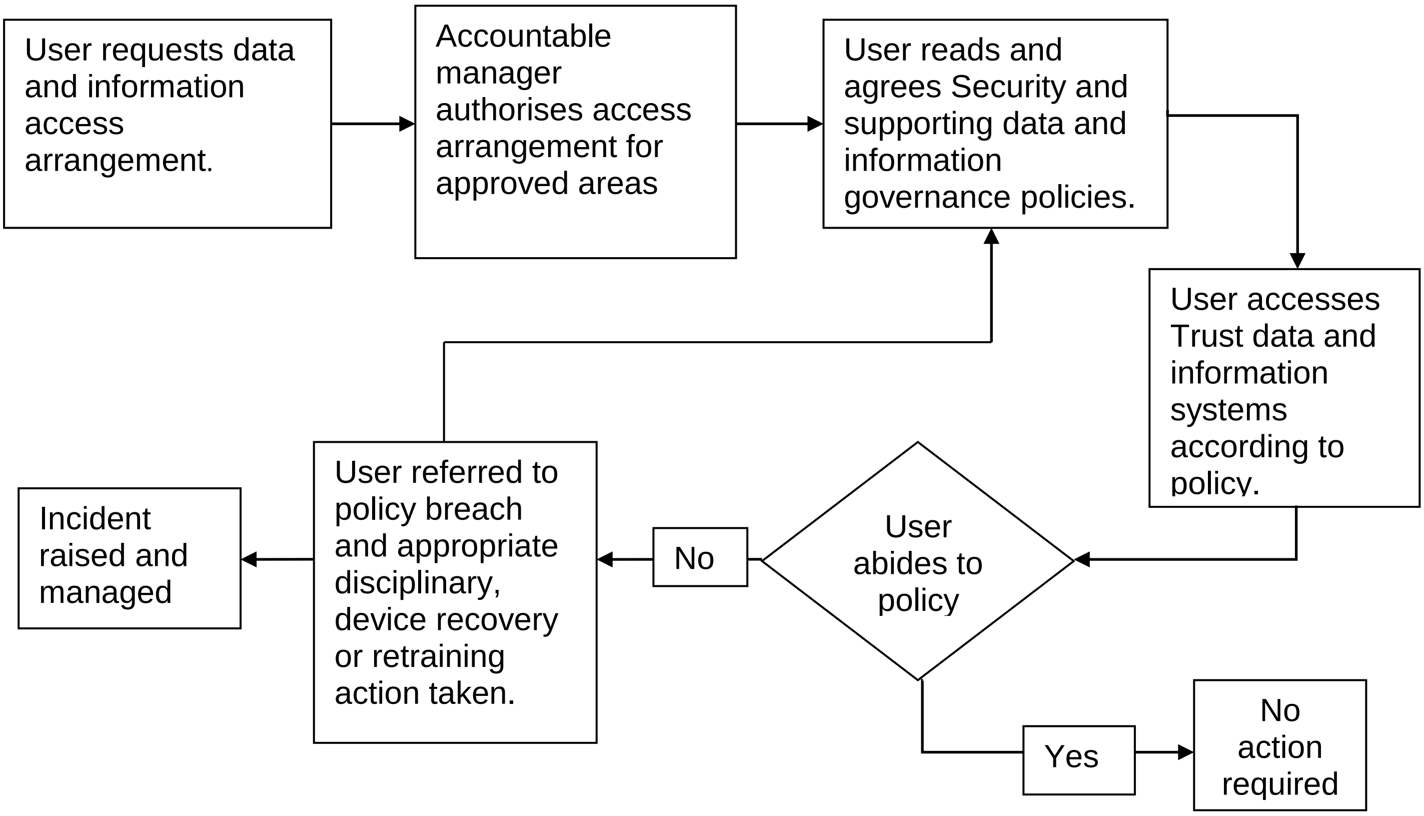
Replaces Network & Wireless Policy version 1.1

Revised October 2019

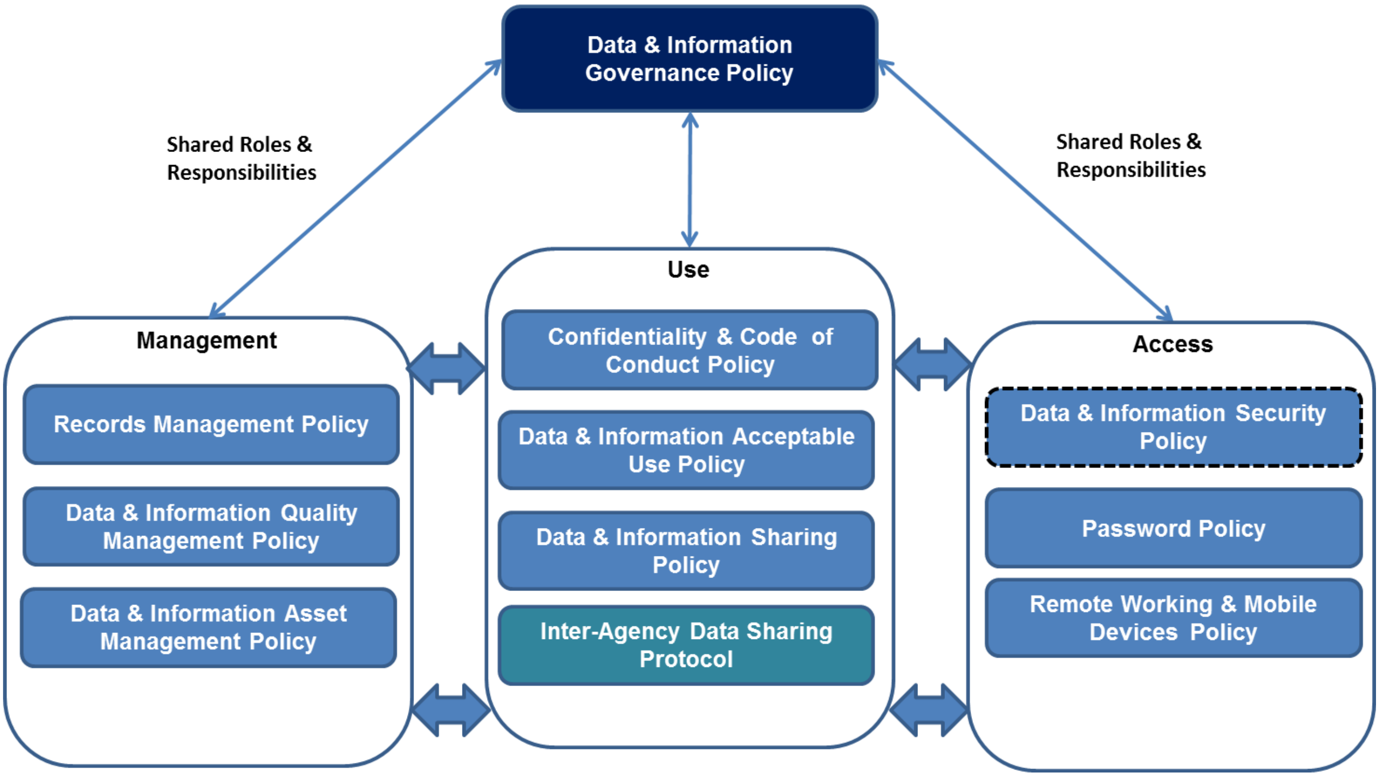
**Contents**

| Section | | Page |
|---|---|---|
| | Flowchart | 1 |
| 1 | Introduction | 2 |
| 2 | Scope | 2 |
| 3 | Definitions | 3 |
| 4 | Purpose | 3 |
| 5 | Duties | 3 |
| 6 | Process – i.e. Specific details of processes  to be followed | 5 |
| | 6.1 Contracts of Employment | 5 |
| | 6.2 Information Security Awareness Training | 5 |
| | 6.3 Information Security Procedures | 5 |
| | 6.4 Location Access Controls | 5 |
| | 6.5 User Access Controls | 5 |
| | 6.6 NHS Smartcard Controls | 6 |
| | 6.7 Information Communication Technology (ICT) Access Controls | 7 |
| | 6.8 Connection to the Trust Network | 7 |
| | 6.9 Wireless Connections | 8 |
| | 6.10 Remote Working | 8 |
| | 6.11 Portable Storage Devices | 9 |
| | 6.12 Bulk Transfers of Person Identifiable Information | 9 |
| | 6.13 Malicious and Unauthorised Software | 9 |
| | 6.14 Monitoring System Access and Use | 9 |
| | 6.15 Business Continuity | 9 |
| | 6.16 Reporting Security Incidents and Weaknesses | 9 |
| 7 | Dissemination, storage and archiving | 10 |
| 8 | Training and other resource implications | 10 |
| 9 | Audit, monitoring and review | 12 |
| 10 | Implementation plan | 13 |
| 11 | Links to other policies, standards and legislation (associated documents) | 14 |
| 12 | Contact details | 14 |
| 13 | References | 14 |
| Appendices | Appendix A – Version Control and Amendment Log | 16 |
| | Appendix B – Dissemination Record | 17 |
| | Appendix C – Equality Impact Assessment Form | 18 |
| | Appendix D -  Human Rights Act Assessment Checklist | 19 |
| | Appendix E – Development, Consultation and Verification Record | 21 |
| | Appendix F – Policy Checklist | 22 |

**Flowchart**


User requests data and information access arrangement.
Accountable manager authorises access arrangement for approved areas
User reads and agrees Security and supporting data and information governance policies.
User accesses Trust data and information systems according to policy.
User abides to policy
No
User referred to policy breach and appropriate disciplinary, device recovery or retraining action taken.
Incident raised and managed
Yes
No action required

The Data & Information Governance Policy provides the overarching shared roles and responsibilities needed to satisfy complete trust Data, Information and System ownership and management.


Data & Information Governance Policy
Shared Roles & Responsibilities
Shared Roles & Responsibilities
Management
Records Management Policy
Data & Information Quality Management Policy
Data & Information Asset Management Policy
Use
Confidentiality & Code of Conduct Policy
Data & Information Acceptable Use Policy
Data & Information Sharing Policy
Inter-Agency Data Sharing Protocol
Access
Data & Information Security Policy
Password Policy
Remote Working & Mobile Devices Policy

## 1. Introduction

The objective of Data & Information security is to protect the Trust's information assets from a wide range of threats, whether deliberate or accidental, internal or external, in order to ensure business continuity and minimise the impact of adverse events on service users, staff and the Trust. Information security is achieved through the implementation of controls and procedures that ensure the secure use of information and the identification and effective management of risk.

## 2. Scope

The scope of this document is to outline the Trust's policy for Data & Information Security for all data, information and system management and protection.

This policy applies to all staff and services within the Sheffield Health & Social Care FT (SHSC), including private contractors, volunteers and temporary staff and to those organisations where we provide commissioned services.

Shared governance and compliance areas for data and information include:

- NHS Digital & England Guidance
- Data Security & Protection Toolkit
- Cyber-Security Best Practices
- Information Technology Service Management
- General Data Protection Regulation
- Caldicott Principles
- Data & Information Quality Management
- ISO27001 Information Security Management Systems

The policy supports the Trusts needs to continually improve, protect and manage all digital, data and information assets according to legislation and best practice through a collaborative approach.

### Systems

All manual and electronic information systems owned, operated or managed by the Trust, including networks and application systems, whether or not such systems are installed or used on Trust premises.

Other systems brought onto Trust premises including, but not limited to, those of contractors and third party suppliers, which are used for Trust business.

### Users

All users of Trust information and/or systems including Trust employees and non-Trust employees who have been authorised to access and use such information and/or systems.

### Data & Information

All information collected or accessed in relation to any Trust activity whether by Trust employees or individuals and organisations under a contractual relationship with the Trust.

All information stored on facilities owned or managed by the Trust or on behalf of the Trust.

All such data & information belongs to the Trust unless proven otherwise.

## 3. Definitions

**Remote Working**
Mobile and remote working is the term used to describe working away from your usual workplace. New technology has made this easier. Within the context of the Trust, mobile computing is a term used to describe the use of mobile devices that process Trust data. Typically, this will include items such as laptops, tablets (such as iPads) and mobile telephones (smart phones) where these are capable of storing data.

**Portable Equipment**
Includes, but is not limited to, Laptops, Mobile Phones and Smart phones, Tablet devices, PC's, USB Memory devices and other forms of digital storage.

Technology continues to evolve and thus this is not intended to be an exhaustive definition/list. However, it includes all battery powered and mains adapted personal computing and storage devices.

## 4. Purpose

The purpose of this policy is to enable the Trust to protect its information assets by:

- Setting out a framework for information security
- Promoting a culture of information security within the Trust
  Ensuring staff understand their responsibilities in relation to information security

The information security policy will ensure that:

- Information is protected against unauthorised access and/or misuse
- The confidentiality of information is assured
- The integrity of information is maintained
- Information is available when required
- Business continuity plans are produced, maintained and tested
- Regulatory, legal and contractual requirements are complied with
- Training around information security is provided to all staff
- All breaches of information security, actual or suspected, are reported and investigated (line below moved to this line).through the appropriate management channels
- Controls and procedures will be produced to support this policy and implement the framework

## 5. Duties

The strategy combines traditional Information Asset (IAO / IAA), data governance, data quality and (ITSM) system management roles and responsibilities into a single accountable shared Business Information Management framework.

| Role | | Responsibility | Description |
|---|---|---|---|
| Chief Information Officer | CIO | Director IMST | Responsible for the Information Technology that supports the overarching strategies of the Trust. |
| Chief Clinical Information Officer | CCIO | Director Medical | Providing a vital voice for clinical strategy, allowing new IT, Data & Information products to help improve the provision of healthcare. |

|  |  |  |  |
|---|---|---|---|
| Senior Information Risk Owner | SIRO | Director Finance | Owns the Trust's information risk policy and risk assessment process. |
| Caldicott Guardian | CG | Director Nursing | Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing. |
| Data Protection Officer | DPO |  | Supporting Trust wide Data & Information governance in accordance with GDPR, NHS Digital & England and Data Security & Protection Toolkit. |
| Clinical Information Officer | CLIO |  | Supporting the Chief Clinical Information Officer and trust wide clinical initiatives for increased data and information usage and opportunities, supported by data and information governance framework. |
| Cyber Security Officer | CSO |  | Supporting the Trust to continuously assess, implement and manage Trust wide cyber-security, and removing identified vulnerabilities with support from all technical and business managers and users. |
| Data & Information Asset Owners | DIAO | Directorate | Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems. |
| Data & Information Asset Managers | DIAM | Service Managers | Primary administrative and management responsibilities for segments of data primarily associated with their functional area. |
| Data & Information Asset Supervisors | DIAS | Supervisors / Team Leaders | Supervisors have responsibility for the day-to-day maintenance and protection of data & information when they are affected by the processes that they manage. |
| Data & Information Asset Users | DIAU | All Users | Responsibility lies with all staff to make sure that all policies and security measures are adhered to. |
| Data & Information Asset Stewards | DIAS | IMST & Suppliers | Trust and third party IMST enabling and supporting secure & compliant data and information technical implementation, governance and guidance throughout the Trust and in accordance to trust policy, national guidelines and regulations. |

Each Data and Information role has clear responsibilities for data, information and system management within their respective service domains and role accountability, supported by natural hierarchy escalation and incident management.

All staff who use Trust information systems (including manual systems as well as electronic ones) plus other authorised users of systems are required to adhere to this policy.

## 6 Process

### 6.1 Contracts of Employment

Security requirements are addressed at the recruitment stage and all contracts of employment contain a clause relating to confidentiality and data protection.

### 6.2 Information Security Awareness Training

Information security awareness training is included in the staff induction process. An on-going programme of awareness is established to ensure that staff awareness is refreshed and updated.

### 6.3 Information Security Procedures

The security of paper and electronic records, computers and networks is controlled by procedures that have been authorised by the appropriate authority within the Trust.

Areas of information security covered include, but are not limited to:

- In order to minimise loss of, or damage to, all assets, all equipment and information storage areas must be physically protected from security threats and environmental hazards.
- Confidential information held in hard copy (paper) must be kept secure at all times.
- Confidential Trust information must not be stored on local hard drives such as PCs, laptops or other mobile devices unless authorised by the Information Manager and protected by encryption. Such information should be stored on a secure Trust server with access restricted to appropriate members of staff (server space can be allocated by the IT Department).
- Databases of personal, that is, service user information and staff information, must not be created without prior permission from the Information Manager.
- Current databases of personal information must be notified to the Information Manager.

### 6.4 Location Access Controls

Only authorised personnel who have an identified need should be given access to restricted areas containing information systems such as server rooms.

### 6.5 User Access Controls

Access to information and information systems, whether electronic or manual, must be restricted to authorised users who have an identified need as agreed with their line manager or sponsor.

Access to electronic information systems must be given at the appropriate level for the agreed need. Users must not share their passwords with other people.

Users must ensure that they protect the network from unauthorised access. They must log off the network when they have finished working.

The Trust operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked or a screensaver password activated if a workstation is left unattended for a short time.

An automatic screen lock will be initiated after 15 minutes of inactivity.

### 6.6 NHS Smartcard Controls

For Healthcare Professionals to access HSCIC applications they need to be registered. The registration process for the National Programme has to meet the current Government requirements and will be applied nationally. All the HSCIC applications use a common security and confidentiality approach. This is based upon the NHS professional's organisation/s role/s, area/s of work and business function. The primary method by which users will be enabled to access an HSCIC application is via a Smartcard issued during the Registration Process. Once an applicant has been successfully registered they will have a User ID, pass-codes and Smartcard – which will permit their access to the appropriate application/s and information. The process of gaining access to the National Programme applications is called National Programme Registration.

The Registration Process is operated at a local level by a Registration Authority who is required to conform to the National Registration Policy and Practices identified below.

**Registration Authority**

SHSC Registration Authority will manage the distribution and use of Smartcards.

Assigned Registration Authority will ensure:

- That the National Registration processes are adhered to in full.
- That the RA01, RA02 and RA03 forms are appropriately used.
- That any local processes developed to support the National Registration processes are adhered to in full.
- That there is sufficient availability of resources to operate the registration processes in a timely and efficient manner in order to meet their organisational responsibilities.
- Ensuring that the RA team members are adequately trained and familiar with the local and national RA processes.
- Ensuring that an indexed and secure audit trail is maintained of applicant's registration information (RA01) and profile changes (RA02, RA03).

SHSC will ensure that processes supporting the identification, registration and management of staff will be integrated with other SHSC processes as appropriate.

All our RA policies and procedures will be auditable by internal auditors as well as external auditors. Audits would typically cover:

- The issuance of Smartcards
- The management of Smartcards
- The profiles associated with users in relation to what they do
- The use of Smartcards
- The use of HSCIC applications
- Identity management
- Security of supplies and equipment

Further details can be found in Registration Authority (Smartcard) policy.

### 6.7 Information Communication Technology (ICT) Access Controls

Access to ICT equipment, for example PCs and terminals, must be restricted to authorised users who have an agreed requirement to use those facilities.

Network computer equipment will be housed in a controlled and secure environment.

Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

Critical or sensitive network equipment is equipment that stores patient or staff personal identifiable information.

Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

The IT Service Manager is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if s/he suspects the code has been compromised, or when required to do so by the Information Security Manager (ISM).

Critical or sensitive network equipment will be protected from power supply failures.

Critical or sensitive network equipment will be protected by intruder alarms and environment monitoring systems.

Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

All visitors to secure network areas must be authorised by the IT services manager.

All visitors to secure network areas must be made aware of network security requirements.

All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

The IT services manager will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

### 6.8 Connection to the Trust Network

All devices connected to the Trust network are governed by the NHS Code of Connection.

The connection of any equipment to the Trust network requires authorisation from the IT department.

All electronic processing devices connecting to the Trust network must be protected by up to date anti-virus software. Where the device does not update automatically, it is the responsibility of the user to ensure that the anti-virus software is up to date.

Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to the Remote Working and Mobile Devices Policy stored on the SHSC intranet.

There must be a formal, documented user registration and de-registration procedure for access to the network - this is stored on the SHSC intranet.

- Line managers and the IT services manager must approve user access.
- Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis and will be detailed on the request form following approval.
- All Personal computing devices in use on the network will be protected by a secure screensaver that will initiate within 15 minutes of inactivity by the user.
- Security privileges (i.e. 'superuser' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- Access will not be granted until the IM&T department registers a user.
- All users to the network will have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret (see User Responsibilities).
- User access rights will be immediately removed or reviewed for those users who have left the Trust or changed jobs once IT helpdesk has been informed.

### 6.9 Wireless Connections

Electronic devices provided by the Trust (plus any other devices which hold or store Trust data) must not use wireless network connections to the Trust or any other network unless approved by the trust IT department.

The Trust will ensure that all connections to external networks and systems have been documented.

- The Trust will ensure all wireless connections have been documented.
- The Trust will ensure that all connections to external networks and systems conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance.
- The Director of IM&T must approve all connections to external networks, systems and wireless connectivity before they commence operation.
- Any data exchanged across organisations must conform with the Trust’s information security policies.
- Wireless Networks will be protected with Certificate based WPA2 security.
- The wireless network authentication will be integrated into Active Directory authentication.
- Wireless networks will be authorised and installed by the SHSC IM&T department only.
- The wireless network will be tunnelled back to the data centre using IPSEC VPN security.

### 6.10 Remote Working

Information that is taken off site must be protected by encryption which meets national requirements and, where held on mobile computers, backed up regularly. Mobile devices must be protected by appropriate security (see the Remote Working and Mobile Devices Policy).

### 6.11 Portable Devices

Portable storage devices (including laptops, tablets, mobile phones, CDs, DVDs and USB drives) containing software or data from external sources, or that have been connected to external equipment, must be fully virus checked before being used on Trust equipment.

Portable storage devices containing confidential information must be encrypted to national standards. Writing to USB devices from SHSC computers will only be allowed for devices purchased via the IT department and registered by them. Other USB devices will be restricted to read-only. CD/DVD drives on SHSC computers will be prevented from writing to disc unless specifically approved by the IT department.

### 6.12 Bulk Transfers of Person Identifiable Information

All bulk transfers of person identifiable information, whether of electronic or manual records, must be notified to and approved by the Director of IM&T before they can begin. Electronic bulk transfers of person identifiable information must be protected by encryption which meets national requirements or use other approved transfer methods such as secure FTP.

### 6.13 Malicious and Unauthorised Software

The Trust will use countermeasures and management procedures to protect itself against the effects of malicious software. All staff are expected to co-operate fully with this requirement.

Users must not install software on Trust equipment without permission from the IT department.

### 6.14 Monitoring System Access and Use

Audit trails of system access and use are maintained and reviewed on a regular basis.

### 6.15 Business Continuity

The Trust will ensure that business continuity plans and disaster recovery plans are produced for the networks.

The plans must be reviewed by the IM&T Director and IT Services Manager and tested on a regular basis.

### 6.16 Reporting Incidents and Weaknesses

An Information Incident is an event that could compromise the confidentiality of information (if it is lost or could be viewed by or given to unauthorised persons), the integrity of the data (if it could be inaccurate or content could have been changed) or the availability of the information (access).

Examples of information incidents are:

- Potential and suspected disclosure of NHS information to unauthorised individuals.
- Loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored.
- Disruption to systems and business processes.
- Attempts to gain unauthorised access to computer systems, e.g. hacking.

- Records altered or deleted without authorisation by the data “owner”.
- Virus or other malicious malware attacks (suspected or actual).
- “Blagging” offence where information is obtained by deception.
- Breaches of physical security e.g. forcing of doors or windows into secure rooms or filing cabinets containing NHS sensitive or other UK Government information left unlocked in an accessible area.
- Leaving a desktop or laptop unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Human error such as emailing data by mistake.
- Covert or unauthorised recording of meetings and presentations.
- Damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges.
- Deliberate leaking of information.
- Insider fraud. [1]
- Smartcard or application misuse.
- Smartcard theft.
- Non-compliance of local or national RA policy.
- Any unauthorised access of HSCIC applications.
- Any unauthorised alteration of patient data.

The Trust handles considerable amounts of patient data and this can be sensitive. An information incident involving sensitive data, especially patient confidential information, is considered to be a data/information breach and must be reported.

All information management and technology security incidents and weaknesses must be reported via Trust incident reporting procedures (see Trust Incident Reporting Policy).

Incidents that present an immediate risk to the Trust should be escalated through local supervisor & manager, IT Helpdesk & Data Protection Officer.

**SIRO & Data & Information Governance Group Reporting (DIGB)**
The Data Protection Officer will keep SIRO & DIGB informed of the information incidents status by means of regular reports and immediate alerts where an immediate risk is identified.

## 7. Dissemination, storage and archiving (Control)

This policy replaces version 1.5 Information Security Policy. The policy is to be made available on the Trust intranet and available to all staff.

## 8. Training and other resource implications

Information Governance training is mandatory for all staff on induction and on a yearly basis.

[1] Where any incidents involving suspected fraud are identified, the Trust’s Fraud, Bribery and Corruption Policy should be followed and advice sought from the Local Counter Fraud Specialist (robert.purseglove@nhs.net).

The Information Governance Team will work with the Learning Development team and managers to ensure that appropriate additional training is available to support staff.

The Information Governance team will work the Senior Information Risk Owner, Data & Information Managers and other appropriate managers and teams to maintain continued awareness of confidentiality and security issues to both the organisation and staff through staff emails, newsletters, intranet etc.

## 9. Audit, monitoring and review

*This section should describe how the implementation and impact of the policy will be monitored and audited. It should include timescales and frequency of audits.*

*If the policy is required to meet a particular standard, it must say how and when compliance with the standard will be audited.*

**Monitoring Compliance Template**

| Minimum Requirement | Process for Monitoring | Responsible Individual/ group/committee | Frequency of Monitoring | Review of Results process (e.g. who does this?) | Responsible Individual/group/ committee for action plan development | Responsible Individual/group/ committee for action plan monitoring and implementation |
|---|---|---|---|---|---|---|
| Compliance with this policy in terms of use of the Internet and related systems | Review in light of any incidents, staff requests and suggestions | Information Manager; Head of Informatics and Information Systems; IT Dept. | Annual | Data & Information Governance Board | Information Manager; Head of Informatics and Information Systems; IT Dept. | Data & Information Governance Board |

*Policy documents should be reviewed every three years or earlier where legislation dictates or practices change. The policy review date should be written here – 31/3/2020.*

## 10. Implementation plan

*The implementation plan should be presented as an action plan and include clear actions, lead roles, resources needed and timescales. The Director of Corporate Governance team can provide advice on formats for action plans however; an example layout for the plan is shown below:*

| Action / Task | Responsible Person | Deadline | Progress update |
|---|---|---|---|
| Upload to Intranet | Corporate Affairs | TBC | 26/11/2019 |
| Distribute communications | Corporate Affairs | TBC | 05/12/2019 |
| Provide training and awareness | IMST | TBC | |
| Review against progress and operational need | DIGB | TBC | |

## 11. Links to other policies, standards and legislation (associated documents)

The Trust and its employees, including non-Trust employees authorised to access Trust Information and systems, are obliged to comply with the following legislation and requirements:

- Common Law Duty of Confidentiality
- Data Protection Act/GDPR
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1998
- NHS Code of Connection
- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Fraud, Bribery and Corruption Policy

And any relevant guidance related to the following:

- Information Quality Assurance
- Information Security
- Information Governance Management

## 12. Contact details

*The document should give names, job titles and contact details for any staff who may need to be contacted in the course of using the policy (sample table layout below). This should also be a list of staff who could advise regarding policy implementation.*

| ***Title*** | ***Name*** | ***Phone*** | ***Email*** |
|---|---|---|---|
| Senior Information Risk Owner (SIRO) | Phillip Easthope | 0114 3050765 | Phillip.easthope@shsc.nhs.uk |
| Assistant Deputy Director of IMS&T | Ben Sewell | 0114 2711144 | Ben.sewell@shsc.nhs.uk |
| Information Manager | John Wolstenholme | 0114 3050749 | John.wolstenholme@shsc.nhs.uk |

## 13. References

*The document should include key references for the evidence base, and relevant legislation or government policy.*

- The Data Protection Act (2018)
- General Data Protection Regulation (GDPR)
- The Freedom of Information Act (2000)
- Environmental Information Regulations (2004)
- European Directive 2003/4/EC
- Access to Health Records Act (1990)
- Human Rights Act (1998)
- Crime and Disorder Act (1998)
- Criminal Procedures and Investigations Act (1996)

- Regulatory and Investigatory Powers Act (2000)
- ICO Framework Code of Practice for Sharing Personal Information
- (2007)
- Children Act (2004)
- Working together to Safeguard Children (2006)
- NHS Act (2006)
- Multi-Agency Public Protection Arrangements (MAPPA)
- Mental Capacity Act 2005 and Code of Practice (2007)
- Information Sharing Guidance for Practitioners and Managers
- (2008)
- Confidentiality NHS Code of Practice (2003)
- Confidentiality Guidance for Doctors (GMC 2009)
- Confidentiality and Disclosure of Health Information Toolkit (BMA
- 2008)
- The NMC Code of Professional Conduct: Standards for Conduct,
- Performance and Ethics (NMC 2004)
- No Secrets: Guidance on developing and implementing multiagency policies and procedures to protect vulnerable adults from abuse.
- Data Protection and Sharing – Guidance for Emergency Planners and Responders (HMG 2007)
- Data Sharing Review Report (Thomas and Walport 2008)
- Health and Social Care Act (2012)
- Caldicott Guidance (2010)
- To Share or Not to Share – The Information Governance Review (2013)
- Computer Misuse Act 1990
- Department of Health, Records Management: NHS Code of Practice (2006)
- NHS Connecting for Health
- NHS Information Governance, Guidance on Legal and Professional Obligations (Department of Health, 2007)

## Appendix A – Version Control and Amendment Log

| Version No. | Type of Change | Date | Description of change(s) |
|---|---|---|---|
| 1 | Policy created | March 2018 | New policy to replace the previous Information Security Policy as part of a comprehensive review of information governance policies. |
| 1.1 | Revision | Apr – Oct 2019 | Updates for legislative and monitoring changes and contact details. |

# Appendix B – Dissemination Record

| Version | Date on website (intranet and internet) | Date of “all SHSC staff” email | Any other promotion/ dissemination (include dates) |
|---|---|---|---|
| 1 | August 2018 | | |

# Appendix C – Stage One Equality Impact Assessment Form

## Equality Impact Assessment Process for Policies Developed Under the Policy on Policies

**Stage 1** – Complete draft policy

**Stage 2** – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? If **NO** – No further action required – please sign and date the following statement. If **YES –** proceed to stage 3

This policy does not impact on staff, patients or the public (insert name and date) No. J Wolstenholme, 21 Oct 2019

**Stage 3** – **Policy Screening** - Public authorities are legally required to have 'due regard' to eliminating discrimination , advancing equal opportunity and fostering good relations , in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance on equality impact assessment for examples and detailed advice. This is available by logging-on to the Intranet first and then following this link https://nww.xct.nhs.uk/widget.php?wdg=wdg_general_info&page=464

| | **Does any aspect of this policy actually or potentially discriminate against this group?** | **Can equality of opportunity for this group be improved through this policy or changes to this policy?** | **Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?** |
|---|---|---|---|
| **AGE** | | | |
| **DISABILITY** | | | |
| **GENDER REASSIGNMENT** | | | |
| **PREGNANCY AND MATERNITY** | | | |
| **RACE** | | | |
| **RELIGION OR BELIEF** | | | |
| **SEX** | | | |
| **SEXUAL ORIENTATION** | | | |

**Stage 4** – **Policy Revision** - Make amendments to the policy or identify any remedial action required (action should be noted in the policy implementation plan section)

Please delete as appropriate: Policy Amended / Action Identified / no changes made.

Impact Assessment Completed by (insert name and date)

## Appendix D - Human Rights Act Assessment Form and Flowchart

You need to be confident that no aspect of this policy breaches a person's Human Rights. You can assume that if a policy is directly based on a law or national policy it will not therefore breach Human Rights.

If the policy or any procedures in the policy, are based on a local decision which impact on individuals, then you will need to make sure their human rights are not breached. To do this, you will need to refer to the more detailed guidance that is available on the SHSC web site
http://www.justice.gov.uk/downloads/human-rights/act-studyguide.pdf
(relevant sections numbers are referenced in grey boxes on diagram) and work through the flow chart on the next page.

1. **Is your policy based on and in line with the current law (including case law) or policy?**

✓ **Yes. No further action needed.**

□ **No. Work through the flow diagram over the page and then answer questions 2 and 3 below.**

2. **On completion of flow diagram – is further action needed?**

□ **No, no further action needed.**

□ **Yes, go to question 3**

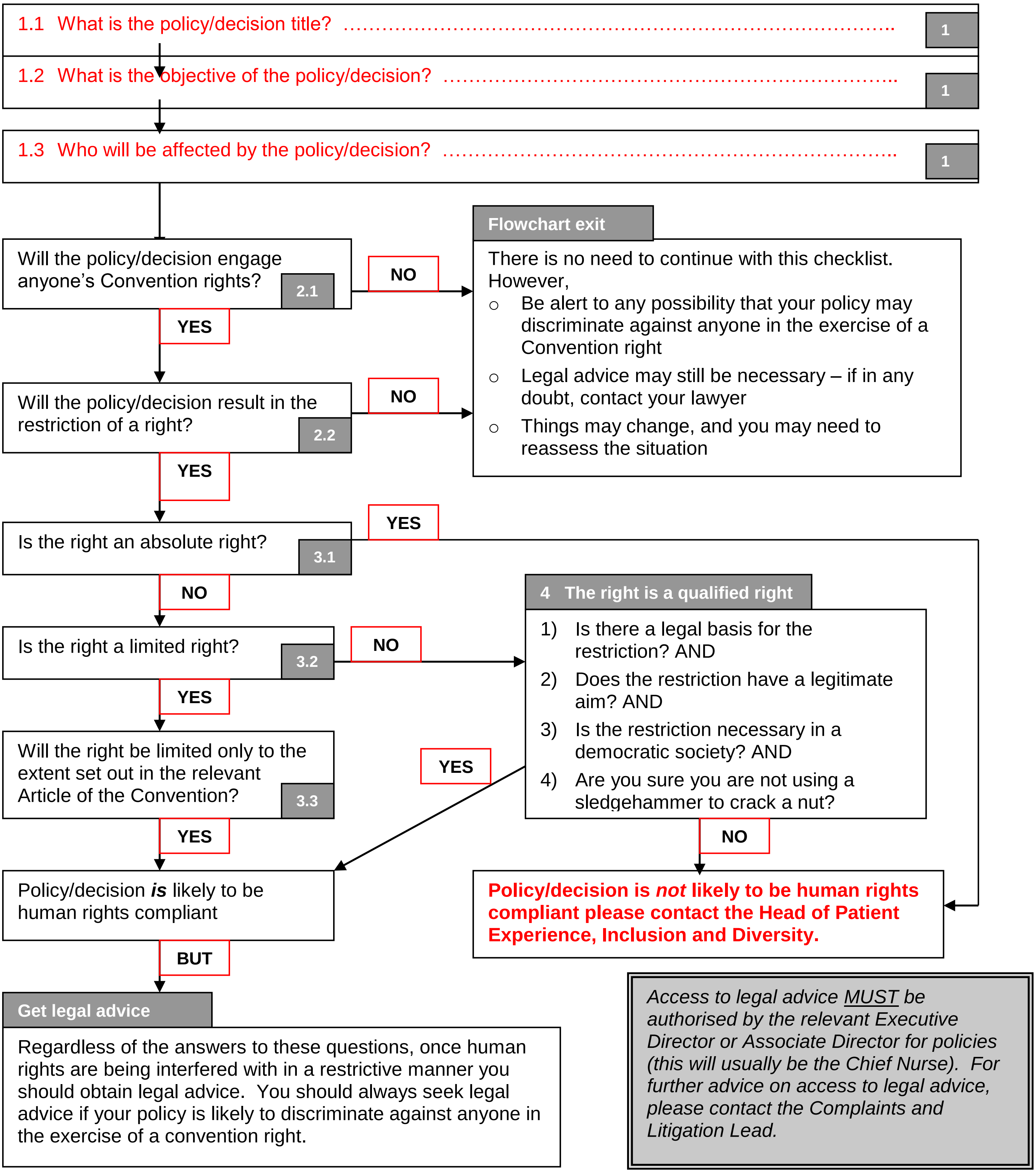
3. **Complete the table below to provide details of the actions required**

| Action required | By what date | Responsible Person |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

## Human Rights Assessment Flow Chart

**Complete text answers in boxes 1.1 – 1.3 and highlight your path through the flowchart by filling the YES/NO boxes red** (do this by clicking on the YES/NO text boxes and then from the Format menu on the toolbar, choose ‘Format Text Box’ and choose red from the Fill colour option).

**Once the flowchart is completed, return to the previous page to complete the Human Rights Act Assessment Form.**



1.1 What is the policy/decision title? ……………………………………………………………………….. 1

1.2 What is the objective of the policy/decision? ………………………………………………………….. 1

1.3 Who will be affected by the policy/decision? ………………………………………………………….. 1

Will the policy/decision engage anyone’s Convention rights? 2.1

NO

YES

Will the policy/decision result in the restriction of a right? 2.2

NO

YES

**Flowchart exit**

There is no need to continue with this checklist. However,

- Be alert to any possibility that your policy may discriminate against anyone in the exercise of a Convention right
- Legal advice may still be necessary – if in any doubt, contact your lawyer
- Things may change, and you may need to reassess the situation

Is the right an absolute right? 3.1

YES

NO

Is the right a limited right? 3.2

NO

YES

**4 The right is a qualified right**

1) Is there a legal basis for the restriction? AND
2) Does the restriction have a legitimate aim? AND
3) Is the restriction necessary in a democratic society? AND
4) Are you sure you are not using a sledgehammer to crack a nut?

Will the right be limited only to the extent set out in the relevant Article of the Convention? 3.3

YES

YES

NO

Policy/decision *is* likely to be human rights compliant

**Policy/decision is *not* likely to be human rights compliant please contact the Head of Patient Experience, Inclusion and Diversity.**

BUT

**Get legal advice**

Regardless of the answers to these questions, once human rights are being interfered with in a restrictive manner you should obtain legal advice. You should always seek legal advice if your policy is likely to discriminate against anyone in the exercise of a convention right.

*Access to legal advice MUST be authorised by the relevant Executive Director or Associate Director for policies (this will usually be the Chief Nurse). For further advice on access to legal advice, please contact the Complaints and Litigation Lead.*

# Appendix E – Development, Consultation and Verification

This policy was developed as part of a major review of Information Governance policies in 2018 to meet the requirements of legislative change (introduction of the General Data Protection Regulation (GDPR) and Data Protection Act 2018) and the migration from the Information Governance Toolkit to the Data Security & Protection Toolkit which takes account of the National Data Guardian's data security standards.

The policies were approved by the Data & Information Governance Board in May 2018.

This policy was updated in October 2018 to update references and contact details for submission to the November 2019 Data & Information Governance Board.

## Appendix F –Policies Checklist

***Please use this as a checklist for policy completion. The style and format of policies should follow the Policy template which can be downloaded on the intranet (also shown at Appendix G within the Policy).***

1. **Cover sheet** ☒

All policies must have a cover sheet which includes:

- The Trust name and logo ☒
- The title of the policy (in large font size as detailed in the template) ☒
- Executive or Associate Director lead for the policy ☒
- The policy author and lead ☒
- The implementation lead (to receive feedback on the implementation) ☒
- Date of initial draft policy ☒
- Date of consultation ☒
- Date of verification ☒
- Date of ratification ☒
- Date of issue ☒
- Ratifying body ☒
- Date for review ☒
- Target audience ☒
- Document type ☒
- Document status ☒
- Keywords ☒
- Policy version and advice on availability and storage ☒

2. **Contents page**

3. **Flowchart** ☒

4. **Introduction** ☒

5. **Scope** ☒

6. **Definitions** ☒

7. **Purpose** ☒

8. **Duties** ☒

9. **Process** ☒

10. **Dissemination, storage and archiving (control)** ☒

11. **Training and other resource implications** ☒

12. **Audit, monitoring and review** ☒

This section should describe how the implementation and impact of the policy will be monitored and audited and when it will be reviewed. It should include timescales and frequency of audits. It must include the monitoring template as shown in the policy template (example below).

**Monitoring Compliance Template**

| Minimum Require-ment | Process for Monitoring | Responsible Individual/ group/ committee | Frequency of Monitoring | Review of Results process (e.g. who does this?) | Responsible Individual/group/ committee for action plan development | Responsible Individual/group/ committee for action plan monitoring and implementation |
|---|---|---|---|---|---|---|
| A) Describe which aspect this is monitoring? | e.g. Review, audit | e.g. Education & Training Steering Group | e.g. Annual | e.g. Quality Assurance Committee | e.g. Education & Training Steering Group | e.g. Quality Assurance Committee |

**13. Implementation plan** ☒

**14. Links to other policies (associated documents)** ☒

**15. Contact details** ☒

**16. References** ☒

**17. Version control and amendment log (Appendix A)** ☒

**18. Dissemination Record (Appendix B)** ☒

**19. Equality Impact Assessment Form (Appendix C)** ☒

**20. Human Rights Act Assessment Checklist (Appendix D)** ☒

**21. Policy development and consultation process (Appendix E)** ☒

**22. Policy Checklist (Appendix F)** ☒