Proud to care in Sheffield

NHS
Sheffield Health
and Social Care
NHS Foundation Trust

Policy:

IMST 003 - Data & Information Security

Executive Director Lead	Executive Director of Finance & SIRO
Policy Owner	Chief Digital Information Officer
Policy Author	Data Protection Officer

Document Type	Policy
Document Version Number	Version 3
Date of Approval By PGG	March 2025
Date of Ratification	May 2025
Ratified By	ARC
Date of Issue	March 2025
Date for Review	03/2028

Summary of policy

This policy sets out the security and protection requirements for all data, information and systems management within the Trust.

Target audience	SHSC staff and people authorised to access the SHSC network and systems.

Keywords	Security, Access, Data & Information, Network

Storage & Version Control

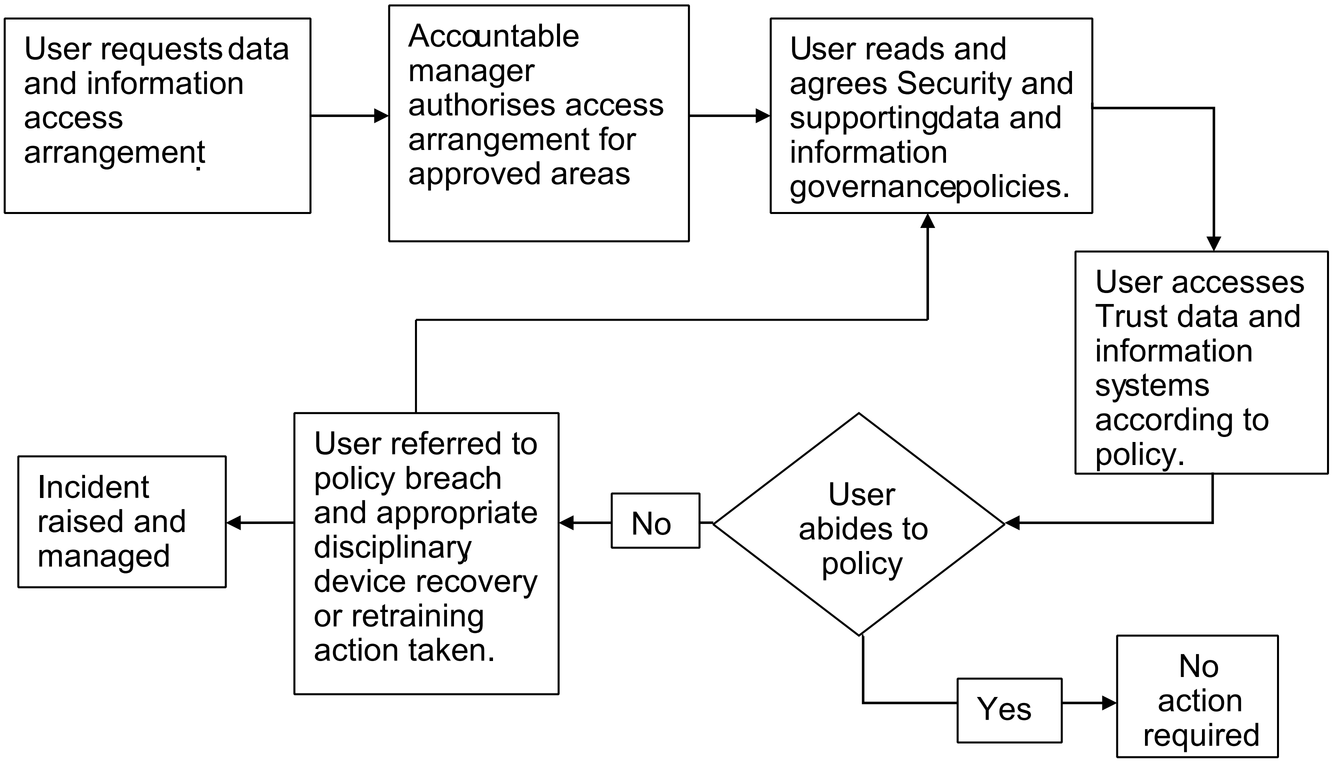
Version 3 of this policy is stored and available through the SHSC intranet/internet. This version of the policy supersedes the previous version (v2 April 2022). Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
1.0	New policy created	03/2018	New policy to replace the previous Information Security Policy as part of a comprehensive review of information governance policies.
1.1	Revision	10/2019	Updates for legislative and monitoring changes and contact details.
2	Scheduled Review	03/2022	Updates for organisational and technological change – roles clarified and updated based on Trust practice, meeting names updated, references to national guidance and legislation updated.
3	Scheduled Review	02/2025	Minor updates for organisational change

Contents

Flow Chart


User requests data and information access arrangement
Accountable manager authorises access arrangement for approved areas
User reads and agrees Security and supportingdata and information governancepolicies.
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

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 Sheffield Health & Social Care (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 England Guidance
- Data Security & Protection Toolkit
- Cyber-Security Best Practices
- Information Technology Service Management
- UK General Data Protection Regulation
- Caldicott Principles
- Data & Information Quality Management
- ISO27001 Information Security Management Systems

The policy supports the Trust's 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 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 through the appropriate management channels
- Controls and procedures will be produced to support this policy and implement the framework

4 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, PCs, USB memory devices and other forms of digital storage.

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

5 Detail of the policy

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

This policy is one of a suite of information governance policies which sit beneath the over-arching Data & Information Governance Policy:

Management:

- Records Management Policy
- Data & Information Quality Management Policy

Use

- Confidentiality Code of Conduct
- Data & Information Acceptable Use Policy
- Data & Information Sharing Policy including E-Mail

Access

- Data & Information Security Policy
- Password Policy
- Remote Working & Mobile Devices Policy

6 Duties

The strategy combines traditional Information Asset ownership (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
Senior Information Risk Owner	SIRO	Director Finance	Owns the Trust's information risk policy and risk assessment process.
Chief Digital Information Officer	CDIO	Chief Digital Information Officer	Responsible for the Information Technology that supports the overarching strategies of the Trust.
Chief Clinical Information Officer	CCIO	CCIO	Providing a vital voice for clinical strategy, allowing new IT, Data & Information products to help improve the provision of healthcare.
Caldicott Guardian	CG	Director, Medical	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.
Information Governance Manager			Responsible for the application of Information Governance throughout the Trust and compliance with the Data Security & Protection Toolkit
Data Protection Officer	DPO	DPO	Supporting Trust wide Data & Information governance in accordance with UK GDPR, NHS England and Data Security & Protection Toolkit.

Information Asset Owners	IAO	Directorate	Senior representatives of the directorates closely aligned to major stores of organisational data, information and systems.
Information Asset Managers	IAM	System/Service Managers	Primary administrative and management responsibilities for segments of data primarily associated with their functional area.

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.

7 Procedure

7.1 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.

7.2 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.

7.3 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 completing a DPIA and protected by encryption. Such information should be stored using approved Trust systems with access restricted to appropriate members of staff.
- Databases of personal data, that is, service user information and staff information, must not be created without the required completion of a DPIA.
- Current databases of personal information must be notified to the Information Governance team and included on the Record Of Processing Activity (ROPA).

7.4 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.

7.5 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 of information systems 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.

Workstations, laptops, tablets and other computing devices must be locked or a screensaver password activated if they are left unattended, even for a short time.

Computing devices will be configured to lock automatically after a specified time of inactivity.

7.6 NHS Smartcard Controls

For Healthcare Professionals to access certain national applications they need to be registered. The registration process for these applications is defined nationally. All the national 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 a national 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 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

The 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 registration 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.
- That the RA team members are adequately trained and familiar with the local and national RA processes.
- That an indexed and secure audit trail is maintained of applicants' registration information and profile changes.

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

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

7.7 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 IT infrastructure equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

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.

All staff with access to secure areas will ensure that they are aware of procedures for visitors and that visitors are escorted, when necessary.

7.8 Connection to the Trust Network

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.

- Line managers must request and 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 automatically following 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 IMST department registers a user.
- All users of 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 for those users who have left the Trust and reviewed for users who have changed jobs once IT Service Desk has been informed.

7.9 Wireless Connections

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

- The Trust will ensure that all connections to the Trust network and systems conform to NHS guidance.
- The CDIO 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 within the Trust will be protected with appropriate security measures.
- Wireless network authentication will be integrated into Active Directory authentication.
- Wireless networks within the Trust will be authorised and installed by the SHSC Digital department only.
- The wireless network will be tunnelled back to the data centre using appropriate security.

7.10 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).

Trust equipment may be connected to the internet via non-Trust services including home connections and services provided by partner organisations providing that it is protected by up-to-date anti-virus software and the connection is made via the Trust's approved VPN solution.

7.11 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. Other drives connected to SHSC computers will be prevented from writing unless specifically approved by the IT department.

7.12 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 completion of the DPIA process 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.

7.13 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.

7.14 Monitoring System Access and Use

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

7.15 Business Continuity

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

The plans must be reviewed by the CDIO and CSO and tested on a regular basis.

7.16 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 confidential 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 with local or national RA policy.
- Any unauthorised access of national applications.
- Any unauthorised alteration of patient data.

The Trust handles considerable amounts of patient data, much of which is 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.

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

Information Governance, Cyber Security & Artificial Intelligence Group
The Information Governance Manager will keep the SIRO and CG informed of the information incidents status by means of regular reports and immediate alerts where an immediate risk is identified.

8 Development, Consultation and Approval

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

[1] In the case of suspected incidents of fraud, refer to the Trust’s Counter Fraud, Bribery and Corruption Policy

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.

This policy was updated in March 2022 for changes to references, job roles and governance structures.

This policy was updated in February 2025 to reflect organisational change, and approved by the Information Governance, Cyber Security & Artificial Intelligence Group.

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 SHSC systems	Review in light of any incidents, staff requests and suggestions	Information Governance Team	Annual	Information Governance, Cyber Security & Artificial Intelligence Group	Information Governance Team	Information Governance, Cyber Security & Artificial Intelligence Group

Policy review date: 31 March 2028

10 Implementation Plan

Action / Task	**Responsible Person**	**Deadline**	**Progress update**
Upload to Intranet	Corporate Affairs		
Distribute communications	Corporate Affairs		
Provide training and awareness	Digital	Ongoing	
Review against progress and operational need	IG, Cyber & AI	Ongoing	

Action planning and monitoring against DSPT[2]	Information Governance	Annual (June)	

11 Dissemination, Storage and Archiving (Control)

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1	August 2018	August 2018	August 2018	
1.1	December 2019	December 2019	December 2019	
2	April 2022	April 2022	April 2022	
3				

[2] DSPT – Data Security and Protection Toolkit - https://www.dsptoolkit.nhs.uk/

12 Training and Other Resource Implications

Information Governance training is mandatory for all staff on induction and on an annual basis.

The Information Governance Team works with the Training team and managers to ensure that appropriate additional training is available to support staff.

The Information Governance team will work with the SIRO, IAOs, IAMs 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.

13 Links to Other Policies, Standards (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:

- The Data Protection Act 2018
- UK General Data Protection Regulations (UK GDPR)
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- The Eight Caldicott Principles (National Data Guardian 2020)
- Regulation of Investigatory Powers Act 2000
- Confidentiality: NHS Code of Practice (2003)
- Records Management Code of Practice (NHS 2023)
- SHSC Data & Information Governance Policy
- SHSC Password Policy
- SHSC Remote Working & Mobile Devices Policy
- SHSC Confidentiality Code of Conduct
- SHSC Fraud, Bribery and Corruption Policy

And any relevant guidance related to the following:

- Information Quality Assurance
- Information Security
- Information Governance Management

14 Contact Details

Title	***Name***	***Phone***	***Email***
Senior Information Risk Owner (SIRO)	Phillip Easthope	0114 3050765	Phillip.easthope@shsc.nhs.uk
Chief Digital Information Officer	Chris Reynolds	0114 2664960	chris.reynolds@shsc.nhs.uk
Head of Service Delivery & Infrastructure, Digital	Adam Handley	0114 3050770	Adam.handley@shsc.nhs.uk
Information Governance Manager	Katie Hunter	0114 2716723	Katie.hunter@shsc.nhs.uk
Data Protection Officer	John Wolstenholme	0114 3050749	John.wolstenholme@shsc.nhs.uk

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - **I**s the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement. **I confirm that this policy does not impact on staff, patients or the public.**	***I confirm that this policy does not impact on staff, patients or the public.*** Name/Date: J Wolstenholme, 11 Feb 2025	**YES,** Go to **Stage 2**

Stage 2 Policy Screening and Drafting Policy - 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 and Flow Chart.

Stage 3 – **Policy Revision** - Make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section

SCREENING RECORD	Does any aspect of this policy 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			
Marriage or Civil Partnership			

Please delete as appropriate: - Policy Amended / Action Identified (see Implementation Plan) / no changes made.

Impact Assessment Completed by:
Name /Date

Appendix B

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	✓
2.	Is the local Policy Champion member sighted on the development/review of the policy?	✓
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	N/A
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	✓
5.	Has the policy been discussed and agreed by the local governance groups?	✓
6.	Have any relevant recommendations from Internal Audit or other relevant bodies been taken into account in preparing the policy?	✓
	Template Compliance	
7.	Has the version control/storage section been updated?	✓
8.	Is the policy title clear and unambiguous?	✓
9.	Is the policy in Arial font 12?	✓
10.	Have page numbers been inserted?	
11.	Has the policy been quality checked for spelling errors, links, accuracy?	✓
	Policy Content	
12.	Is the purpose of the policy clear?	✓
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	✓
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	✓
15.	Where appropriate, does the policy contain a list of definitions of terms used?	✓
16.	Does the policy include any references to other associated policies and key documents?	✓
17.	Has the EIA Form been completed (Appendix 1)?	✓
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	✓
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	✓
20.	Is there a plan to i. review ii. audit compliance with the document?	✓
21.	Is the review date identified, and is it appropriate and justifiable?	✓