Policy:

IMST 007 Data & Information Sharing including E-Mail

Executive Director Lead	Executive Director of Finance & SIRO
Policy Owner	Assistant Deputy Director of IMS&T (Informatics and Architecture)
Policy Author	Data Protection Officer

Document Type	Policy
Document Version Number	Version 1.3
Date of Approval By PGG	28/11/2022
Date of Ratification	January 2023
Ratified By	ARC
Date of Issue	November 2022
Date for Review	30/11/2023

Summary of policy

This policy provides guidance on the governance and mechanisms for sharing confidential information within and externally to the Trust.

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

Keywords	Data, Sharing, GDPR, Safeguarding, Disclosure, e-mail

Storage & Version Control

Version 1.3 of this policy is stored and available through the SHSC intranet/internet.. This version of the policy supersedes the previous version (V1.2 11/2019). Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

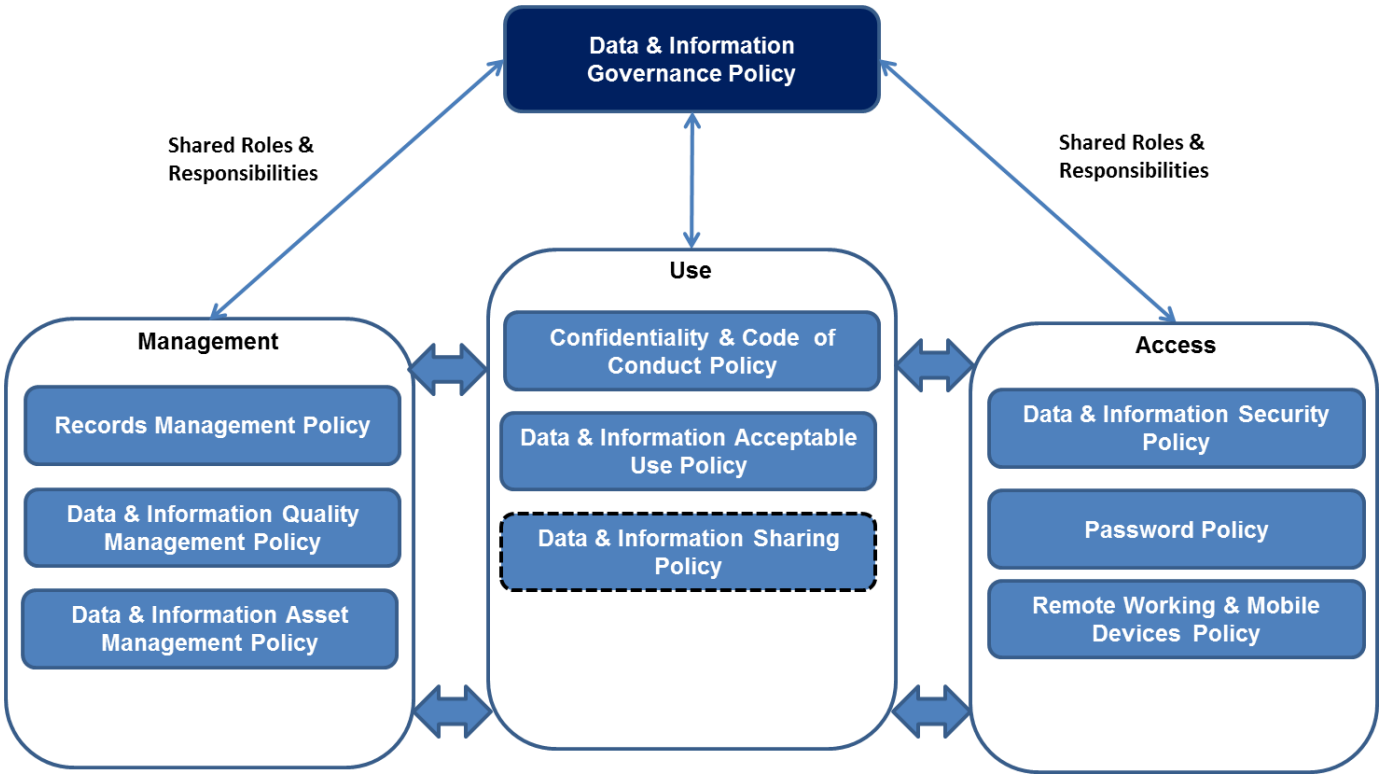
Version No.	Type of Change	Date	Description of change(s)
1	New policy	03/2018	New policy created aligning to the Data & Information Governance Strategy
1.1	Amended and approved	05/2018	Minor amendments and approval by Data & Information Governance Board (DIGB)
1.2	Revision	10/2019	Updates for legislative and monitoring changes and contact details. Inclusion of Data Minimisation, reference to the Inter-Agency Information Sharing Protocol and the National Data Opt-Out.
1.3	Revision	11/2022	Updates for organisational change and external circumstances, simplification of specified roles. Inclusion of E-Mail in title.

Contents

Flowchart

Due to the complex and sensitive nature of data & information sharing, no workflow is available.

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



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 the sharing of confidential, personal information and includes the operation of e-mail within the Trust.

This policy applies to all staff and services within the 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 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 Purpose

This document is a statement of the approach and intentions of the SHSC to fulfil its statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

Information sharing is a vital component of an effective health and social care system. Local organisations are increasingly working together. To work together effectively organisations need to be able to share data about the services they provide and the people to whom they provide these services.

In a healthcare setting, sharing information in line with agreed protocols can add a number of benefits. It can contribute towards making services more efficient and accessible to those in need. It ensures that all patients including the vulnerable are provided with the protection they need. It also enables collaboration amongst different organisations so that they can deliver the care that all patients, including those with complex needs, may be reliant upon.

4 Definitions

Personal Information

Personal information is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name and private address, name and home telephone number etc.

Sensitive personal information

Sensitive personal information is where the personal information contains details of that person's:

- Health or physical condition
- Sexual life or sexual orientation
- Racial or ethnic origin
- Religious or philosophical beliefs
- Political views
- Trade union membership
- Genetic or biometric data

These are classified as **Special Category** data under UK GDPR

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

Criminal offence data is treated separately under the law but should have similar levels of protection.

Safe Haven

The term safe haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.

General Data Protection Regulation (UK GDPR)

A regulation for increased data protection and privacy for individuals, giving regulatory authority greater powers to take action against organisations that breach the law. As a Trust we all play a part in continually protecting, securing and ensuring data is appropriately used, stored and processed correctly and in accordance with GDPR & DSPT compliance.

Data Security & Protection Toolkit (DSPT)
An annual self-assessment which the Trust must make to ensure that confidential information is used and protected in line with the requirements of law, and national guidance, including the National Data Guardian's data security standards.

5 Detail of the policy

This policy covers Trust use (including collection, processing, storage and sharing) of confidential personal information in line with the requirements of data protection legislation and national guidance.

6 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 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 and 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 Medical	Responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.
Data Protection Officer	DPO	DPO	Supporting Trust - wide Data & Information governance in accordance with UK GDPR, NHS Digital & England and Data Security & Protection Toolkit.
Cyber Security Officer	CSO	Assistant Deputy Directors, IMST	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.

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 Information Disclosure

The circumstances under which information is requested will vary between routine sharing, one off requests, individual requests and request for bulk data. If the circumstances are not covered within this document and you require clarity whether to disclose or not, please contact the Data Protection Officer & Informatics and Information Systems team.

In all circumstances, disclosures of personal information must be documented to record what information was disclosed, to whom it was disclosed and how it was disclosed. Information to be disclosed must be disclosed securely, in accordance with the Trust Safe Haven Procedure for transferring information.

The rules for sharing and disclosure were changed by the introduction of the General Data Protection Regulation (GDPR) which came into effect in May 2018, enacted by the Data Protection Act 2018. On leaving the EU, the UK adopted the UK GDPR with equivalent protection for information.

Where an organisation holds inaccurate personal data and has shared that with another organisation, the holder will have to advise the other organisation so that it can correct its own records.

7.2 Information Sharing

In all circumstances, sharing of personal information must be documented to record what information was disclosed, to whom it was disclosed and how it was disclosed.

Agreement and approval of information sharing will follow Trust Information Sharing protocol, assessing rules, laws, principles and standards adopted by partner agencies and the completion of Data Protection Impact Assessments.

7.3 Deciding whether to share or withhold personal information

Any information sharing must be both absolutely necessary and authorised. Information that is shared must be relevant and not excessive. Before sharing information with anyone you should decide:

- What is the purpose of sharing personal information?
- Who will be a party to the sharing?
- What types of information are proposed to be shared?
- What is the basis for sharing e.g. consent/legal basis
- How will the information be shared?

In order for the SHSC to meet its legal obligations, and to achieve compliance with the standards stipulated within the Data Security & Protection Toolkit, the Trust will agree appropriate information sharing agreements with external organisations.

Prior to sharing person identifiable information, all staff must ensure that a protocol exists and that it is in effect valid before any information is released.

7.4 Information Sharing Agreements

Information sharing protocols should, at least, document the following:

- the purpose of the data sharing;
- recipients and the circumstances in which they will have access;
- the data to be shared;
- data security;
- individuals rights – procedures for dealing with subject access requests, complaints etc;
- termination of the sharing agreement;

The NHS has developed a template for Information Sharing Agreements which will be used by the Trust. The Information Commissioner's Office has also produced a statutory code of practice on data sharing which the Trust will follow.

Specific Information Sharing Agreements will be developed with partner organisations as necessary to cover individual data flows.

7.5 Data Minimisation

Data protection legislation and national guidance require that when sharing information the amount of person-identifiable data should be limited to what is necessary to achieve the intended purpose and excessive or irrelevant data should not be included.

Anonymised data should be used instead of identifiable data where it is sufficient to meet the purpose. Similarly, pseudonymised data should be used in preference to identifiable data where anonymised data is not sufficient but identifiable data is not necessary (pseudonymisation is a process that means that personal data cannot be attributed to specific data subjects without reference to additional information which is held separately).

7.6 Sharing for non–care purposes

Where information is to be shared for non-care purposes, the purposes for sharing need to be defined and limited, and additional requirements, such as informed consent or evidence of support under section 251 of the NHS Act 2006, must be addressed.

De-identified data should still be used within a secure environment and with staff access on a need to know basis, where this would meet the identified purpose. This is reflected in the Caldicott Principles. This principle applies to the use of PCD for secondary or non-direct care purposes.

With other organisations, eg research or other secondary use organisations, the protocols will need to address both the basic information governance standards that should apply and the additional ones associated with the secondary uses in question – i.e. purpose, constraints on re-use of information, retention periods and destruction policies.

Where person-identifiable data is released for non-care purposes on the basis of a section 251 approval, it must be checked against the National Data Opt-Out system and data subjects who have declined to have their information shared for non-care purposes must be removed before the data is released.

See https://digital.nhs.uk/services/national-data-opt-out for further details.

7.7 Safeguarding

Where health professionals have concerns about a child, young person or adult who may be at risk of abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm occurring.

The best interests of the child/children, young person(s) or adult(s) at risk must guide decision-making at all times.

Further guidance can be found in the Department of Health Information Sharing advice for practitioners providing safeguarding services to children, young people, parents and carers.

7.8 Sharing and disclosure in the public interest

Public interest is the general welfare and rights of the public that are to be recognised, protected and advanced. Disclosures made in the public interest based on the common law are made where disclosure is essential to prevent a serious and imminent threat to public health, national security, the life of an individual or a third party or to prevent or detect other serious crime.

There is no legal definition as to what constitutes a ‘serious crime’. In the Police and Criminal Evidence Act 1984 a ‘serious arrestable offence’ is an offence that has caused or has the potential to cause:

a) Serious harm to the security of the state or to public order
b) Serious interference with the administration of justice or with the investigation of offences or of a particular offence
c) The death of any person
d) Serious injury to any person
e) Substantial financial gain to any person; and
f) Serious financial loss to any person

This includes crimes such as murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people. Serious harm to the security of the state or to public order and serious fraud will also fall into this category. In contrast, theft, minor fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

Any suspected fraud should be reported in line with the Counter Fraud, Bribery and Corruption Policy. The Trust will co-operate with the Counter Fraud Specialist in the investigation of suspected fraud and will share information for this purpose where appropriate.

Where the police or other 'competent authorities' request information for the purposes of prevention or detection of crime; apprehension or prosecution of offenders or other law enforcement processing they should specify the information needed with sufficient explanation of the matter being investigated to allow the Trust to judge whether breaching service user confidentiality is justified. South Yorkshire Police have a specific form for submitting requests, as do most other police forces, so these should be used wherever possible. If the police or other requester supply a consent form signed by the data subject the Trust may check with the data subject if there is any doubt that the data subject understands the consequences of the request.

Where disclosure is justified it should be limited to the minimum necessary to meet the need and patients should be informed of the disclosure unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk.

7.9 Prevent Duty

There is specific guidance in the Counter-Terrorism and Security Act 2015 for specified authorities in England and Wales on the duty to have due regard to the need to prevent people from being drawn into terrorism.

https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales

There is specific guidance on the sharing of information and information governance for NHS organisations specifically for Prevent, a copy is referenced below.

https://www.england.nhs.uk/wp-content/uploads/2017/09/information-sharing-information-governance-prevent.pdf

7.10 Process for Sharing

When considering a new project or process which will involve sharing of information between parties, a Data Protection Impact Assessment should be completed in order to capture the information required to determine if and how the sharing may take place.

The Data Protection Impact Assessment (DPIA) template can be requested from the Informatics & Information Team.

7.11 Restrictions on Information sharing

It is also important to ascertain whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.

7.12 Physical Transfer

Any information that is to be shared in an electronic format, (e.g., by e-mail or on disc etc.) must first be encrypted in line with NHS Digital standards. When submitting an information sharing protocol request for consideration, staff should provide all details of the methods in which data may be shared so that the Trust can ensure the information is secured in transit.

7.13 Protection of information sent by email/electronically

There are a number of considerations when sharing information electronically:

- What are the implications of the information being released into the public domain?

- Does the information contain personal information about patients or staff and/or in such a way as the identity of the data subject could be guessed by looking at the information contained?
- Does the information need to be sent by email?
- Is there a need to stipulate that the information must not be forwarded on?
- Is there a need to anonymise the information contained?

If information does need to be shared and email is considered the most appropriate method, any identifiable information should only be sent via secure, encrypted email services. The main email service for the NHS is NHS.net, as this provides a guarantee that the information contained will be safe in transit.

Confidential or sensitive information, including information about service users and staff, must not be sent outside the Trust by unencrypted e-mail.

Do not send confidential information via e-mail unless it is absolutely necessary. Use anonymised information whenever possible and where it is necessary to include person identifiable information use the minimum necessary.

Where it is necessary to send person identifiable information from a SHSC e-mail address (ending in @shsc.nhs.uk) the text “[encrypt]” must be included in the subject line. The square brackets are part of the mandatory text. Any such messages will then be encrypted if they pass outside the boundaries of the SHSC network. The recipient will then be required to register with a secure website to generate a password which will allow the encrypted message and any future encrypted messages from the Trust to be opened. Messages sent by replying to an encrypted e-mail will also be encrypted. A password will not be required to open messages sent within the Trust or the City Council network but the “[encrypt]” text must still be included to protect the message should it be forwarded outside the network. A guide on using this encryption facility is available on the Intranet.

Sheffield City Council has its own policy on how confidential information may be sent via email – check with the intended recipient before sending.

Messages sent from NHSmail e-mail addresses (ending in @nhs.net) are encrypted during transmission to other NHSmail addresses and to certain other public sector addresses belonging to linked networks.

Gov.uk
SCN (*scn.gov.uk) CJX (*.police.uk or .pnn.police.uk)
CJSM (*cjsm.net) GSE (*.gse.gov.uk)
MoD (*.mod.uk)
GSX (*.gsx.gov.uk)

Some public sector organisations insist on the use of NHSmail addresses for the transfer of person identifiable information – the IT Department can advise on how to get an NHSmail account.

To provide added protection when sending information within the Trust it can be attached to the e-mail as a password-protected document. When using this method make sure that the password is given to the recipient separately, not included in the same message.

Confidential or sensitive Trust information must not be processed on non-NHS devices without authorisation from the IT Department. Where members of staff process information under:

Any computer that is used for work purposes must be protected by up to date, approved antivirus software. (Advice about anti-virus software can be obtained from the IT Service Desk).

7.14 Referrals by E-mail

E-mails sent from NHSmail addresses to SHSC addresses are not encrypted in transit so where SHSC services wish to accept referrals by e-mail they must adopt and publicise a generic NHSmail address for the receipt of confidential referral details from other secure e-mail accounts. In such cases, a standard operating procedure (SOP) must be developed to ensure that the e-mails are processed promptly and are not dependent on a single member of staff.

7.15 E-mail correspondence with Service Users or Carers

SHSC has no control over access to the service user's PC. E-mails will be encrypted as long as the text "[encrypt]" is included in the subject line as described above but the recipient is responsible for who has access to their PC and what they do with the password generated by the encryption software. They are also responsible for the secure storage and eventual disposal of any e-mails they receive, whether in electronic or printed format.

If service users request communication via unencrypted e-mail they must be made aware of and accept the higher risk of unauthorised access to messages. By default emails sent to service users should be encrypted.

7.16 Data Protection Impact Assessment

Before entering into any data sharing arrangement, it is good practice to carry out a Data Protection Impact Assessment. This will help to assess the benefits that the information sharing might bring to particular individuals or society more widely. It will also help to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals.

As well as harm to individuals, staff should consider potential harm to the organisation's reputation which may arise if information is shared inappropriately, or not shared when it should be.

Any new information assets and data flows that arise out of a new project or procurement where the Trust is the data controller or receives personal, confidential, and sensitive or business sensitive information will need to be recorded on the Data & Information Asset Register.

7.17 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 sensitive 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 NHS 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 (see Trust Incident Reporting Policy).

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

SIRO & Data & Information Governance Group (DIGG) Reporting
The Data Protection Officer will keep SIRO & DIGG informed of the information incidents and status by means of regular reports and immediate escalation 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 the Information Governance Toolkit to the Data Security & Protection Toolkit which takes account of the National Data Guardian's data security standards.

It incorporates and replaces the previous e-mail policy.

[1] Where any incidents involving suspected fraud are identified, the Trust's Counter Fraud, Bribery and Corruption Policy should be followed and advice sought from the Local Counter Fraud Specialist (christaylor2@nhs.net)

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 revised in August 2022 following discussion within IMST and in preparation for submission to the September 2022 Data & Information Governance 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 Trust systems	Review in light of any incidents, staff requests and suggestions	Information Governance Manager; Assistant Deputy Director of IMS&T (Informatics and Architecture), Data Protection Officer, IT Dept.	Annual	Data & Information Governance Group	Information Governance Manager; Assistant Deputy Director of IMS&T (Informatics and Architecture), Data Protection Officer	Data & Information Governance Group

Policy documents should be reviewed every three years or earlier where legislation dictates or practices change. The policy review date should be written here – 30/11/2023

10 Implementation Plan

Action / Task	Responsible Person	Deadline	Progress update
Upload to Intranet	Communications Dept.	TBC	
Distribute communications	Communications Dept.	TBC	
Provide training and awareness	IMST	TBC	
Review against progress and operational need	DIGBG	TBC	

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)
1.1	August 2018	August 2018		
1.2	November 2019	November 2019		
1.3	November 2022	November 2022	November 2022	N/A

12 Training and Other Resource Implications

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

The Information Governance Team will work with the Training Dept. 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.

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:

- Common Law Duty of Confidentiality
- Data Protection Act 2018/UK GDPR
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1998
- Confidentiality: NHS Code of Practice
- Records Management Code of Practice 2021
- Counter 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
Assistant Deputy Director of IMS&T	Ben Sewell	0114 2711144	Ben.sewell@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** - Is 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, 18 Nov 2022	**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?	✓