Policy:

IMST 006 Data & Information Quality Management

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 1.7
Date of Approval By PGG	28/11/2022
Date of Ratification	January 2022
Ratified By	ARC
Date of Issue	November 2022
Date for Review	30/09/2023

Summary of policy

This policy promotes the maintenance of good data quality throughout the Trust.

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

Keywords	Data Quality, quality reporting

Storage & Version Control

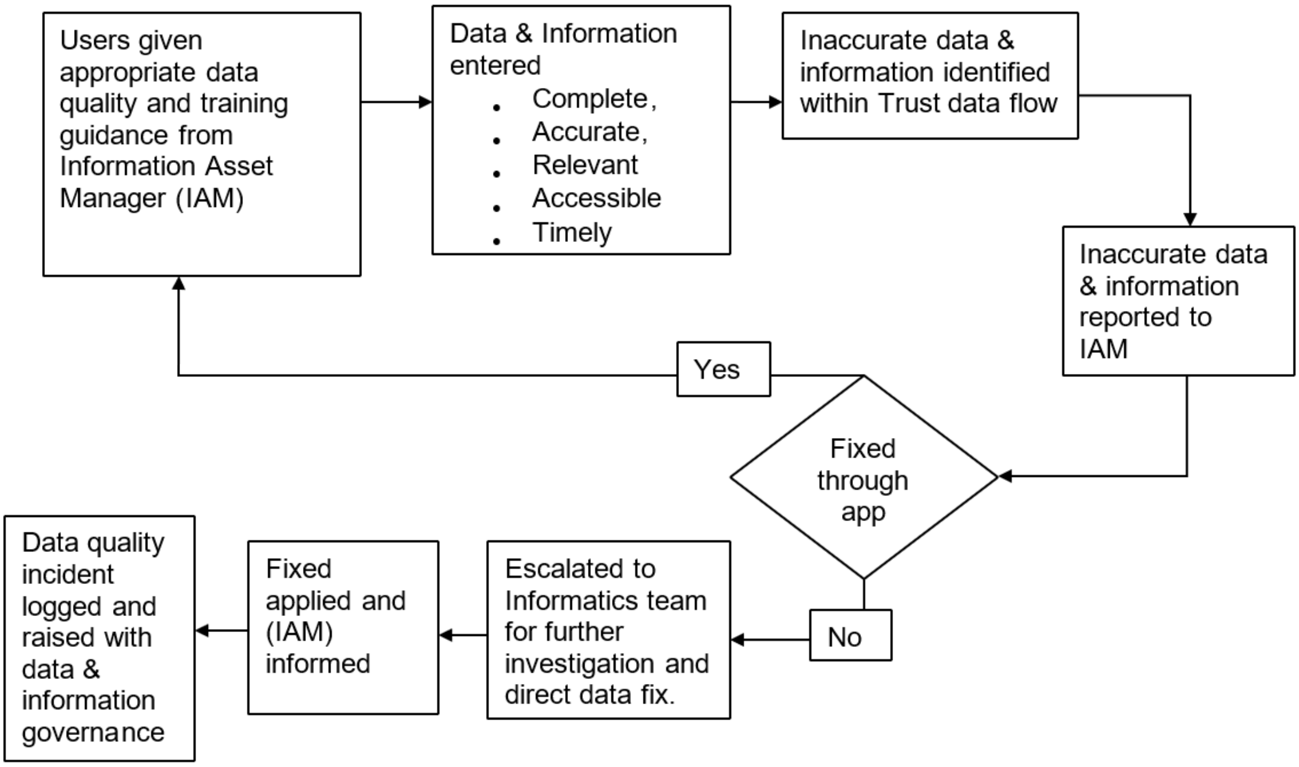
Version 1.7 of this policy is stored and available through the SHSC intranet/internet.. This version of the policy supersedes the previous version (V1.6 11/2019). Any copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

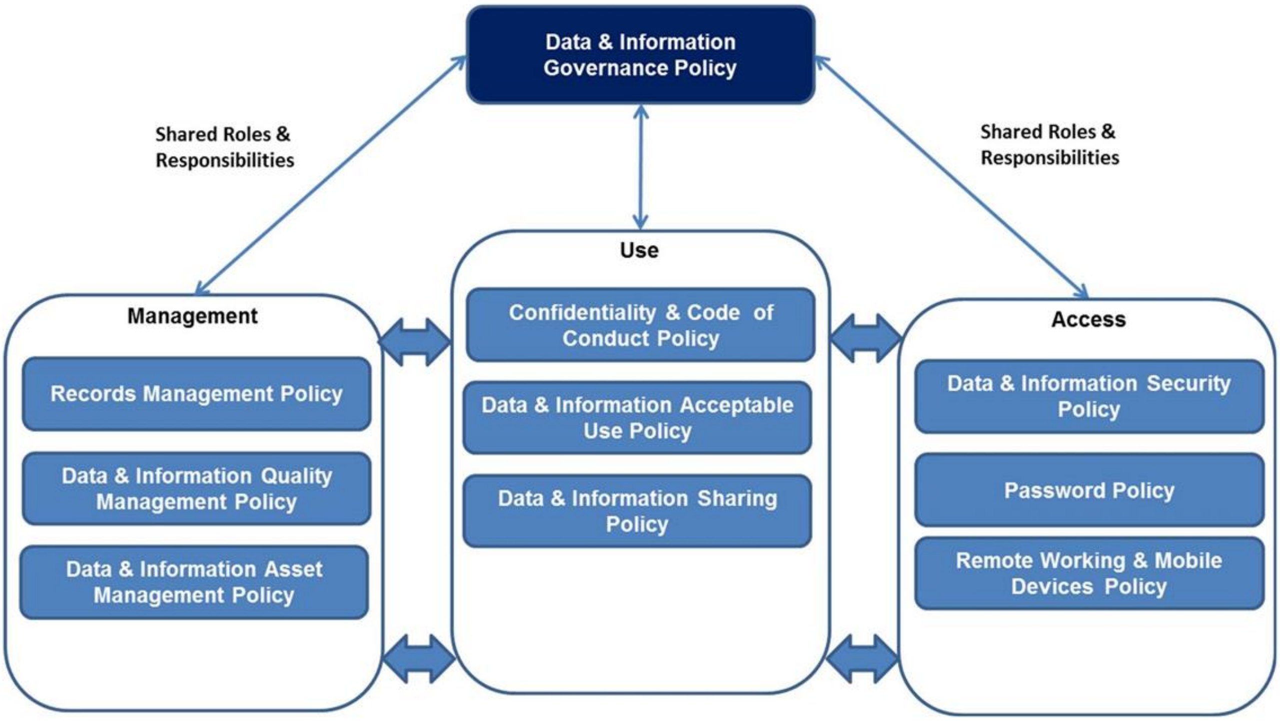
Version No.	Type of Change	Date	Description of change(s)
0.1	Draft policy created	03/2018	New policy created replacing the previous Information Quality Assurance policy and aligning to Data & Information Governance Strategy & Policy.
1.5	Amended and approved	05/2018	Minor amendments and approval by Data & Information Governance Board (DIGB)
1.6	Review	10/2019	Updates for legislative and monitoring changes and contact details.
1.7	Review	08/2022	Update for organisational change, simplification of specified roles, removal of process for updating GP details.

Contents

Flowchart


Users given appropriate data quality and training guidance from Information Asset Manager (IAM)
Data & Information entered
Complete,
Accurate,
Relevant
Accessible
Timely
Inaccurate data & information identified within Trust data flow
Inaccurate data & information reported to IAM
Fixed through app
Yes
No
Escalated to Informatics team for further investigation and direct data fix.
Fixed applied and (IAM) informed
Data quality incident logged and raised with data & information governance

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

1 Introduction

The NHS has long recognised the need for information to be collected on the population that it serves. Information on the care provided by hospitals and trusts is required at a local and national level to enable more effective treatment of patients and provide continuity of care, monitor and manage service level agreements, monitor health improvement programmes, support clinical governance and to understand the health needs of the population.

NHS information systems have grown over recent years and now accommodate increasing levels of data which is required to be collected on patients and staff. This growth has, however, come with an increased concern for the quality of the data.

The Trust recognises that all of their decisions, whether health care, managerial or financial, need to be based on information which is of the highest quality. Data quality is crucial and the availability of complete, accurate, relevant and timely data is important in supporting patient/service user care, governance, management and service agreements for health care planning and accountability.

2 Scope

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

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 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

This policy is intended to emphasise the importance of good data quality to all staff in the Trust and to explain how good data enhances care of service users.

4 Definitions

Data
Data is a collection of facts from which information is constructed via processing or interpretation.

Information
Information is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

Data Quality
Data quality is a measure of the degree of usefulness of data for a specific purpose.

5 Detail of the policy

This policy provides details of the key processes and principles which support good data quality within the Trust

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, data & Information products to help improve the provision of healthcare.
Senior Information Risk Owner	SIRO	Director Finance	Owns the Trusts 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 Trustwide 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 Measuring and Improving Data Quality Indicators

Data quality can be measured using a wide spectrum of indicators which ensure that data is meaningful and fit for purpose.   Data that is fit for purpose should be:

- Complete
- Accurate
- Relevant
- Accessible
- Timely

Key information assets have Information Asset Owners and Managers assigned to them. Each Information Asset Manager should measure and seek to improve the completeness and validity of key data items on their system. They are also responsible for keeping reference tables used by their systems up to date.

7.2 Service User Details

Services are responsible for checking that service user information is accurate and kept up to date – this includes the name, dates of birth, address and postcode and registered GP of the service user. These items should be checked when a service user is referred into a service (including when a previous service user is re-referred to services as well as new referrals), and routinely when service users are seen during the course of their treatment.

Other data items are required for monitoring and service provision including ethnic group, gender, disabilities and sexual orientation although service users have the right to decline to provide this information. Gender and ethnic group are as reported by the service user.

Information about carers, next of kin and children involved with the service user, where recorded, should be kept up to date.

7.3 NHS Numbers

The NHS number is a key element of data quality which serves to uniquely identify service users and therefore to avoid the creation of duplicate records. The Trust will record and verify the NHS number for service users recorded on its systems wherever possible. Other key data items, which must be collected and recorded, include clients' ethnicity, registered GP details and address and postcode.

The NHS number must be used in all internal and external service user/patient related Trust correspondence.

NHS numbers should be recorded where known by the service when they create a new client record on patient information systems. This will alert the service if the person already exists on the system under another name – if the person already exists then that record should be used and updated where necessary (systems linked to the National Spine such as SystmOne are able to import client details from the Spine and these will be updated automatically as details on the Spine change).

Individual NHS numbers can be identified by staff who have access to Summary Care Record/Personal Demographics Service (PDS) via SmartCards. SmartCards with this role will be issued to appropriate members of staff who have a justified work need to access Summary Care Record/PDS – the HR department are responsible for issuing SmartCards.

Existing NHS numbers for service users recorded on the Insight system will be verified and new numbers identified via batch-tracing processes which will be managed centrally by IMST.

7.4 GP Details

Systems should record the current registered GP practice for the service user. Systems are set up to record individual GPs at a practice but the important detail is that service users are linked to a specific practice rather than an individual GP – a service user may specify a particular GP to be recorded on the system but any active GP at the correct practice is sufficient.

The Insight system will record partner GPs at a practice. Locum and salaried GPs will not be recorded as they do not have their own caseloads.

Temporary GP registrations will not be recorded on Insight.

7.5 Deaths

Once service users have been successfully matched by batch tracing or individually via Summary Care Record the Trust is able to run reports to identify when any of them are recorded as having died on the National Spine.

The Information Department will run regular reports to identify service users recorded on Insight who have died. Where there are no open services the client records will be archived. Where there are current services recorded they will be notified by the Information Department so that they can update records and remove any future appointments and then the service will be responsible for archiving the client record in a timely manner.

In most cases deaths are recorded on the National Spine very quickly but in some cases, for instance when a death has been referred to the coroner, the death may not be recorded on the National Spine for some time so that services may be aware of the death well before it is identified by reports. Whenever a service becomes aware of a death before they are notified of it by the Information Department they should still update their records and archive the client on the system rather than leaving the client as active on the system. Most records can still be amended even when the service user is recorded as having died but if the system does not allow an action for an archived client a request can be made to IMST to temporarily unarchive the client record.

7.6 Service Details

Referrals to services should be recorded promptly on the relevant patient information system rather than waiting until the person is seen before recording them.

Activity and notes should be recorded as soon as practically possible, ideally on the same day whilst information is fresh in the worker’s mind, so that colleagues can access the most up to date information if they need to provide treatment and so that activity is available for management and contracting reports.

Caseloads and care co-ordinator or named worker details should be kept up to date on the system and appointments should be outcomed on the day rather than left as ‘to be attended’.

7.7 System Warnings/Alerts

The Insight system has the facility to record short alerts or warnings against service user records. These must not be used to record detailed clinical information because they can be seen by casual browsers – where necessary they can be used to direct workers to a particular note or assessment which can be accessed when needed and which will be subject to an audit trail. Similarly, the warnings should not be used to record keysafe codes which allow entry to a service user’s home – again the details should be recorded in a separate document attached to the record.

Warnings/alerts should be reviewed regularly and removed when no longer relevant. This process will also prevent system users accessing the record from being presented with irrelevant warnings which obscure important information. The system user who created the warning is responsible for removing it when no longer relevant. Care co-ordinators should also review warnings attached to their service users and remove those that are no longer needed.

7.8 Notes and Forms

Where necessary, system users can update notes and documents on the Insight system. Previous versions will be stored automatically so that they can be accessed should we need to refer to the version that was current at the time a decision was made.

If an Insight document that has been finalised needs to be changed, an electronic request form can be submitted to IMST. If a document needs to be changed without maintaining the previous version, or removed completely this can also be requested by electronic form which will need management approval in order to deviate from Trust policy that document history should be maintained.

Some forms can be created in draft for later revision and finalisation. Services must not leave forms as draft for significant lengths of time – this may prevent the continuation of the care pathway or may mean that colleagues treating the service user are not provided with comprehensive information.

7.9 Inpatients

Inpatient stays are recorded via the bedstate module of Insight. For e-prescribing wards it is important to record admissions promptly so that information is available to the JAC system to allow medication to be prescribed.

Wards are required to complete electronic ward reports to verify that information for the day is complete and accurate. These should be completed promptly but should not be marked as complete when information – such as discharges awaiting a discharge summary – is still outstanding.

7.10 Worker and Service Details

Service managers are responsible for ensuring that recorded details about their staff are kept up to date on patient information systems. This includes requesting keyworker codes for new starters in sufficient time for accounts to be set up and notifying IMST when workers are no longer members of their teams.

7.11 Clinical Audit

The Trust has a programme of regular audits which involve clinical staff in verifying information recorded. The results of audits are reported to Trust committees and any identified data quality issues will be acted upon.

7.12 Data Quality Metrics and Benchmarking

The Trust compiles and submits a number of mandatory datasets and regular returns such as the Mental Health Services Dataset (MHSDS), the IAPT dataset, NDTMS for Substance Misuse and Strategic Data Collection Service returns.

Services including clinicians are involved in the collation and approval of data for central returns – they are responsible for identifying and rectifying and data quality problems with source data.

Where the submission process for mandatory datasets involves data quality checks the automated reports will be used to identify any missing, incomplete or inaccurate data. Any such problems will be rectified before submission if possible or promptly thereafter.

Reports provided on dataset submissions by external bodies such as NHS Digital for MHSDS will be summarised and reported to the appropriate SHSC committee.

The Trust takes part in a number of benchmarking exercises as part of the NHS Benchmarking Network. The results of these exercises will be used to compare performance against other participating Trusts and any differences will be investigated to identify whether they are genuine differences in performance or as a result of data quality issues.

7.13 Clinical Coding Audit

As part of the requirements of the Data Security & Protection Toolkit the Trust commissions an annual audit of diagnosis coding for inpatient discharges. Any issues raised are passed to the responsible clinician.

The final audit report is forwarded to the Medical Director and the relevant clinical directors for action.

7.14 Reporting Security Incidents and Weaknesses

An Information Security 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 security 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 room or filing cabinet containing sensitive information left unlocked in an accessible area.
- Leaving 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 to the wrong address 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 NHS applications.
- Any unauthorised alteration of patient data.

The Trust handles considerable amounts of patient data, much of which is sensitive. An information security incident involving sensitive data, especially patient

[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)

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 Management Policy and Procedure).

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 (DIGG)
The Data Protection Officer will keep SIRO & DIGG informed of the information security status of the Trust 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 the Information Governance Toolkit to the Data Security & Protection Toolkit which takes account of the National Data Guardian’s data security standards.

It replaces the previous Information Quality Assurance policy.

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 reviewed 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 ensuring the quality of data processed within the Trust	Review in light of any incidents, staff requests and suggestions. Work programme of the Data Quality Group.	Information Manager, Assistant Deputy Director of IMS&T (Informatics and Architecture), IT Dept.	Annual	Data Quality Group reporting to Data & Information Governance Group	Information Manager, Assistant Deputy Director of IMS&T (Informatics and Architecture), IT Dept. Data Quality Group	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. 09/2023 (short review date in light of the introduction of the new EPR).

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	Data Quality Group	TBC	

11 Dissemination, Storage and Archiving (Control)

This section should describe how the new policy will be disseminated. It says where the policy will be made available and to whom. This will normally be that the policy is available on the Trust's intranet and available to all staff.

It makes it plain that any previous versions must be deleted and describes the archiving and storage arrangements for the current and previous versions of the policy.

It says who is responsible for archiving and version control, and what they should do.

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1.5	08/2018	08/2018		
1.6	11/2019	11/2019		
1.7	November 2022	November 2022	November 2022	N/A

12 Training and Other Resource Implications

Departmental managers are responsible for ensuring that their staff are aware of and comply with this policy.

Information Asset Owners and Information Asset Managers are responsible for the quality of the data within the systems they are responsible for.

Training and awareness to be provided through regular Digital communication and training.

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/UK GDPR
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Confidentiality Code of Practice
- NHSx 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?	✓