Policy:

IMST 002 Data & Information Governance

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	V1.2
Date of Approval By PGG	28/11/2022
Date of Ratification	January 2023
Ratified By	ARC
Date of Issue	November 2022
Date for Review	30/11/2025

Summary of policy
This policy sets out the overall governance framework for the use, processing and storage of confidential personal information within the Trust as part of a suite of information governance policies.

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

Keywords	Data Governance, ITIL, GDPR, Data Quality, Information Governance, DSPT

Storage & Version Control

Version 1.2 of this policy is stored and available through the SHSC intranet/internet. This version of the policy supersedes the previous version (V1.1 11/2019). Any copies of the previous policy held separately should be destroyed and replaced with this version.

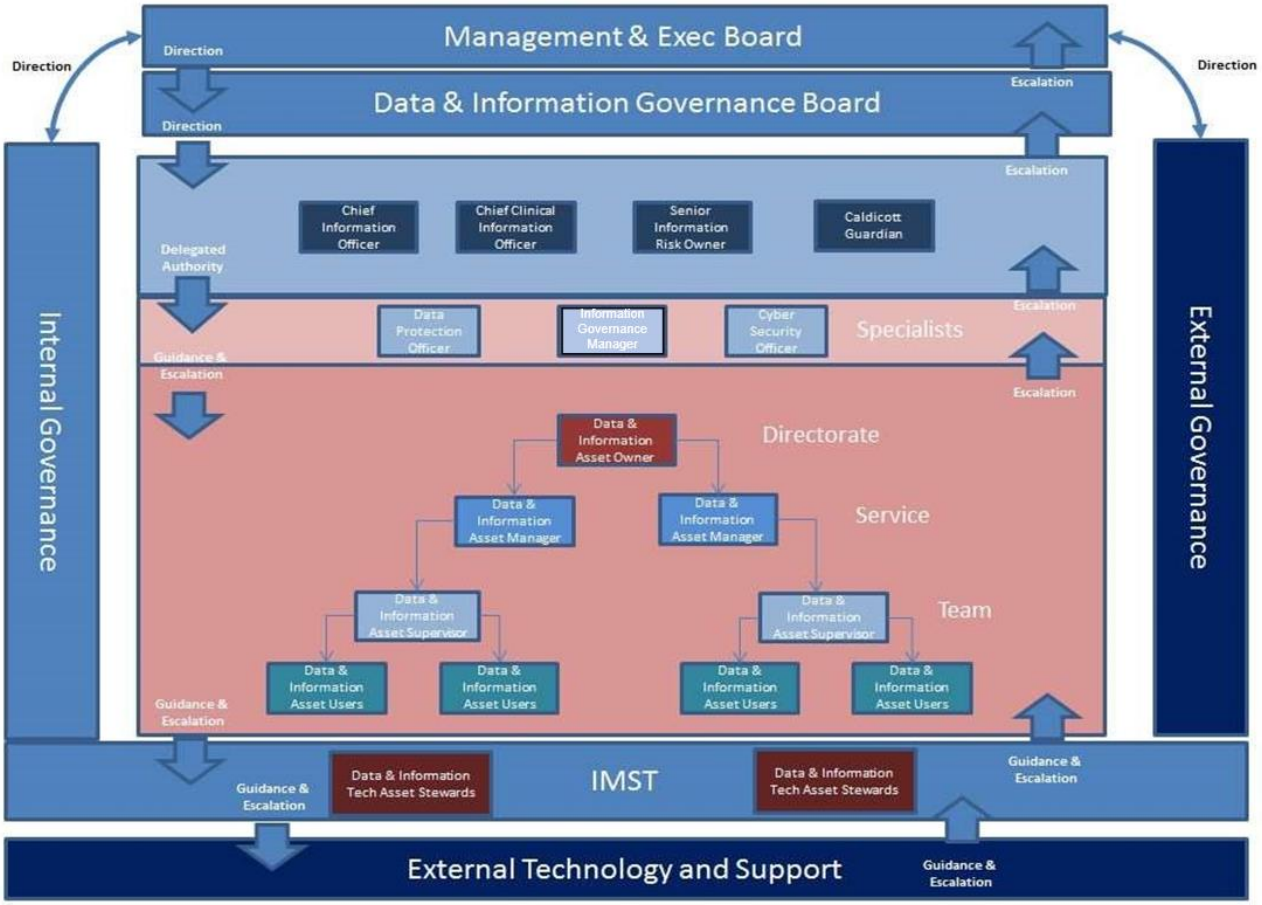
Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
1	New policy created as comprehensive review of IG policies.	03/2018	
1.1	Review	10/2019	Updates for legislative and monitoring changes and contact details.
1.2	Review	08/2022	Update for organisational change, simplification of specified roles.

Contents

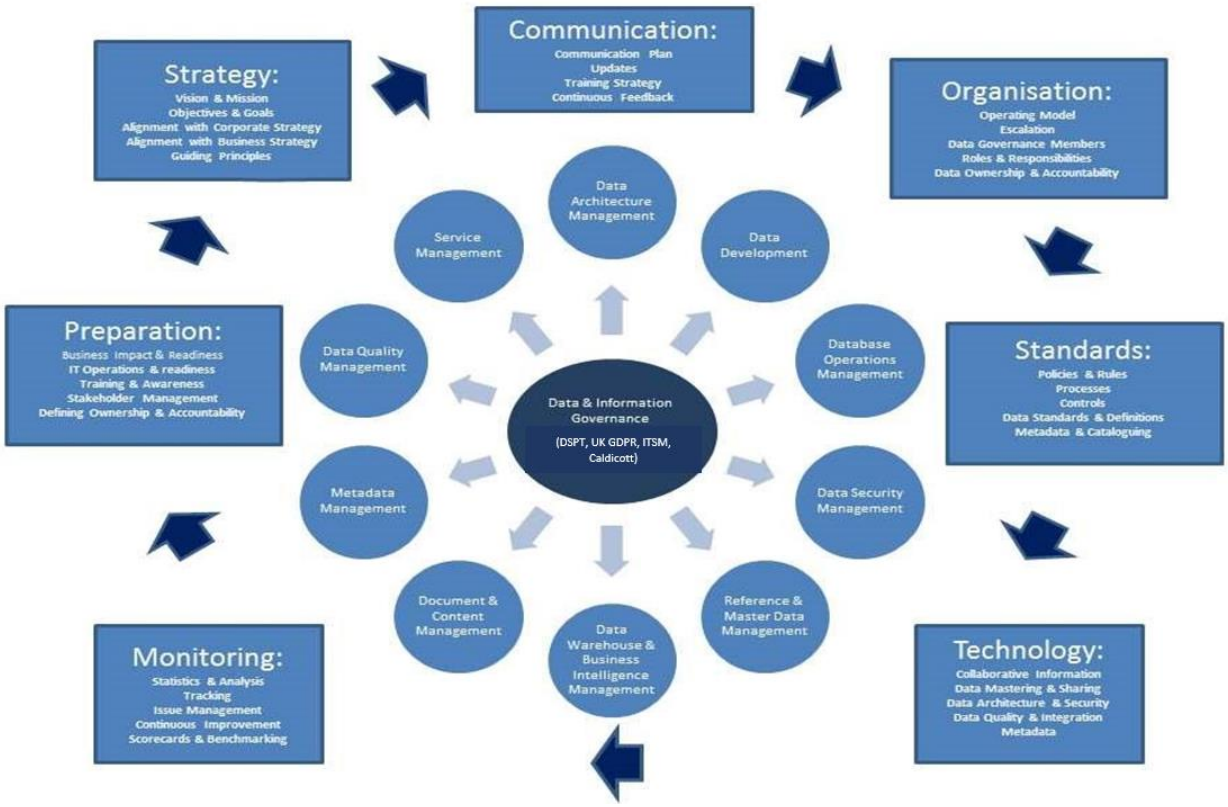
Section		Page
	Version Control and Amendment Log	
	Flow Chart	1
1	Introduction	2
2	Scope	2
3	Purpose	4
4	Definitions	4
5	Details of the Policy	6
6	Duties	6
7	Procedure	7
8	Development, Consultation and Approval	14
9	Audit, Monitoring and Review	15
10	Implementation Plan	16
11	Dissemination, Storage and Archiving (Control)	16
12	Training and Other Resource Implications	17
13	Links to Other Policies, Standards, References, Legislation and National Guidance	17
14	Contact details	17
	APPENDICES	
	Appendix A – Equality Impact Assessment Process and Record for Written Policies	18
	Appendix B – New/Reviewed Policy Checklist	20

Flowchart


Management & Exec Board
Direction
Escalation
Data & Information Governance Board
Chief Information Officer
Chief Clinical Information Officer
Senior Information Risk Owner
Caldicott Guardian
Delegated Authority
Data Protection Officer
Information Governance Manager
Cyber Security Officer
Specialists
Guidance & Escalation
Data & Information Asset Owner
Directorate
Data & Information Asset Manager
Service
Data & Information Asset Supervisor
Team
Data & Information Asset Users
Internal Governance
External Governance
Data & Information Tech Asset Stewards
IMST
External Technology and Support

1 Introduction

The Data & Information Governance policy provides methodology for a Trust-wide shared data and information management framework in accordance NHS & industry business Information management best practice and statutory & legal obligations.



The governance of data & information assets is crucial in achieving a secure data & information handling and management structure within the organisation. Data & Information is an invaluable resource to Sheffield Health & Social Care FT (SHSC) and its loss can damage the organisation's reputation and service delivery. The misuse of data and information can also damage the organisation and individuals.

SHSC has a legal obligation to comply with all appropriate legislation in respect of data, information and IT security.

This document should be read in conjunction with all Trust data & information governance policies which are available on the SHSC intranet.

The data and information governance policy provides the overarching policy for all data and information governance shared roles and responsibilities for the below policies.

2 Scope

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

This strategy 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.

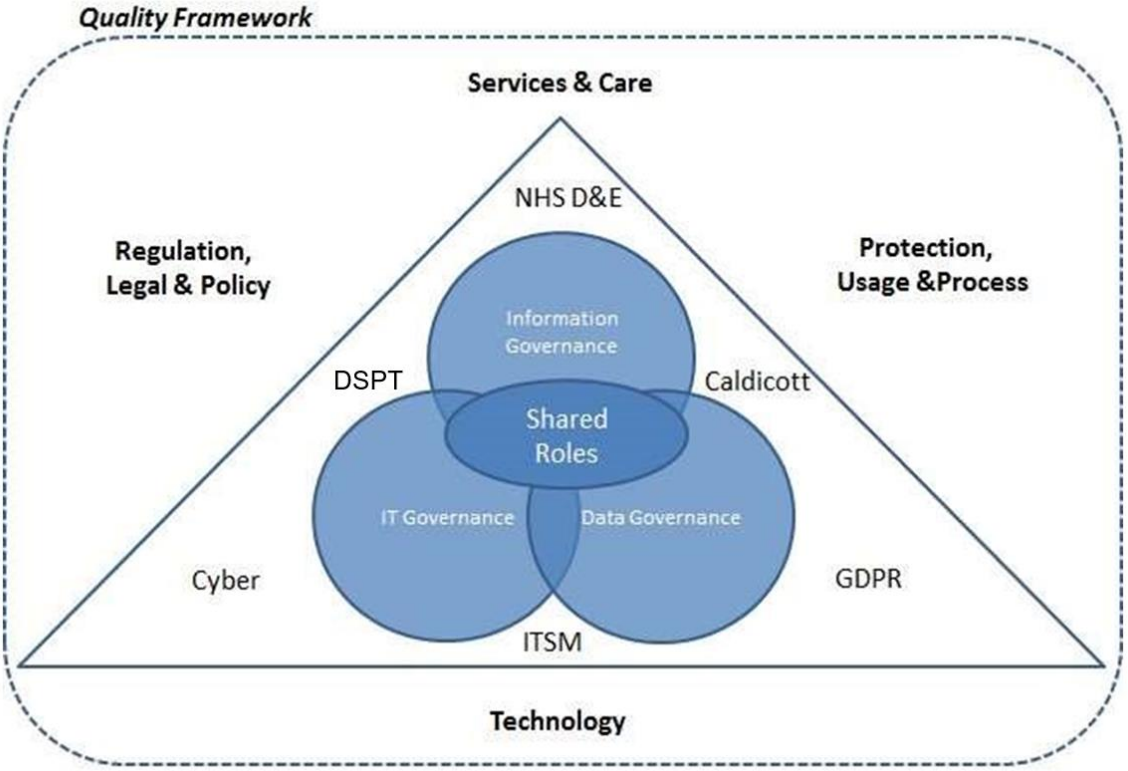
Other systems brought onto Trust premises including, but not limited to, those of contractors and third party suppliers, which are used for Trust business.

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

The Trust has a commitment to ensure that data & information assets are managed in accordance with all relevant regulations and guidance. This strategy supports the implementation, identification and management for all data, information & systems assets within the Trust using a technical and business collaborative approach for management, responsibility and accountability. The strategy aligns and synchronises responsibilities for Data Governance, Information Governance & System Governance as a means of increasing wider ownership and distributed data and information responsibility.

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.

Data & Information Asset
An information asset can be defined as a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

The Data Security & Protection Toolkit categorises an information asset as:

- Information: Databases, system documents and procedures, archive media/data, paper records etc.

- Software: Application programs, system, development tools and utilities.
- Physical: Infrastructure, equipment, furniture and accommodation used for data processing.
- Services: Computing and communications, heating, lighting, power, air conditioning used for data processing.
- People: Their qualifications, skills and experience in use of information systems.
- Intangibles: For example, public confidence in the organisation's ability to ensure the Confidentiality, Integrity and Availability of personal data.

An asset can be a single significant document or a set of related data, documents or files. It can be shared or be confined to a specified purpose or organisational unit. It will have recognisable and manageable value, risk, content and lifecycle. The Trust has hundreds of such systems, both electronic and paper-based, that hold information relating to service users and staff.

Critical Information Asset
A critical information asset is one which the organisation is reliant on and cannot operate without. The result of the information asset being unavailable for up to 24 hours will disrupt and affect patient care, quality of service and the operations of the organisation.

All critical assets must have a System Level Security Policy (SLSP) and business continuity plan in place.

General Data Protection Regulation (GDPR) / UK GDPR
An EU regulation for increased data protection and privacy for individuals, giving regulatory authority greater powers to take action against businesses that breach the new laws. The GDPR is now replaced by the UK GDPR with similar requirements. 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 UK GDPR & DSPT compliance.

Data Security & Protection Toolkit (DSPT)
The Data Security & Protection Toolkit is a performance tool produced by NHS Digital. It draws together the legal rules and central guidance set out above and presents them in one place as a set of information governance requirements. Organisations are required to carry out self-assessments of their compliance against the IG requirements.

Caldicott
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Information Technology Service Management (ITSM)
IT service management (ITSM) refers to the entirety of activities – directed by policies, organised and structured in processes and supporting procedures – that are performed by an organisation to design, plan, deliver, operate and control information technology (IT) services offered to customers.

5 Detail of the policy

This policy sits at the head of a suite of information governance policies. It sets out the overall governance framework for the use, processing and storage of confidential personal information within the Trust.

6 Duties

The policy 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 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 that 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 Accountable Officer

The Trust's Accountable Officer is the Chief Executive who has overall accountability and responsibility for Data & Information Governance. This responsibility is delegated through Trust data and information senior governance roles and framework.

7.2 Data & Information Governance Group (Strategic)

The role of the Group is to have a strategic overview and final responsibility for data & information governance within corporate and service areas across the Trust, in accordance with its Assurance Framework and strategic priorities.

The Data and Information Governance Group will ensure processes and procedures are in place with appropriate levels of capacity and capability to assure;

- Data and information quality
- Data and information security
- Education and awareness of staff in regard Freedom of Information, Data Protection and Caldicott Principles and other information governance requirements and their compliance
- Appropriate responses to data security breaches and a robust review of any incidents
- Good practice for both care and corporate records
- Compliance with the Data Security & Protection Toolkit
- Statutory reporting requirements are met

The Data and Information Governance Group will oversee;

- All policy in relation to data and information; quality, management, storage, security, access and use
- Support its members in regard to their accountabilities of Caldicott Guardian, SIRO, CCIO, and CDIO
- Trust compliance with Freedom of Information, Data Protection and Caldicott Principles
- Processes for, reports to ICO and QAC and lessons learnt arising from Information Risk Incidents

The Data and Information Governance Group will ensure "one version of the truth" overseeing Information Standards and Assets, the Data Dictionary (data definitions)

- Governance of data and information, its source location and ownership
- Definition and derivation of KPIs and Trust MI.
- Projects and service activities that involve the management, storage and migration of data
- Projects and service activities that produce KPIs, MI, BI, reports and dashboards using Trust data

7.3 Chief Digital Information Officer

The Chief Digital Information Officer is the title given to the most senior individual within the Trust who is responsible for the Information Technology that supports the overarching strategies of the Trust. Some of the responsibilities of the CDIO are:

- To lead Business Transformation
- To head decision making regarding purchasing of IT equipment and creation of new IT systems
- To lay out the IT strategy for the Trust
- To produce the IT policy for the Trust
- To make sure that the Trust follows the guidelines and policies in place for data and information and meets recognised standards

7.4 Chief Clinical Information Officer

The Chief Clinical Information Officer works with the CDIO in the implementation of digital technology within the Trust providing a vital voice for clinical strategy, allowing new IT products to help improve the provision of healthcare. Some of the responsibilities of the CCIO are:

- Work with the CDIO from a clinical perspective, adding a real time view on the development of new IT equipment and systems
- Support and help to implement IT strategies through clinical engagement
- Aid in the delivery of a cost-effective digital service whilst ensuring the safety of service users

7.5 Senior Information Risk Owner

The Senior Information Risk Owner owns the Trusts information risk policy and risk assessment process. This ensures that the Trust has a robust incident reporting process in regard to information risks which does not see this as just an IMST problem but as a Trust-wide problem that must be taken seriously and addressed in the appropriate manner.

The SIRO is also responsible for creating a Trust information risk strategy which allows the organisation to exploit assets whilst managing risks effectively.

7.6 Caldicott Guardian

The Caldicott Guardian is a senior member of the Trust who is responsible for protecting the confidentiality of patient and service user information and enabling the appropriate level of information sharing.

The Caldicott Guardian plays a key role in making sure that partner organisations of the Trust meet the highest practicable standards for handling patient identifiable information. These partnered organisations could be other NHS organisations or could be other public organisations such as the council.

The Caldicott Guardian can give advice regarding the transfer of service user information relating to justification, necessity, level of scope of information to be transferred and compliance.

7.7 Data Protection Officer

Supporting Trust-wide data & information governance in accordance with GDPR, NHS Digital & England guidance and the Data Security & Protection Toolkit.

- Educating the Trust and employees on important data & information compliance requirements
- Training staff involved in data & Information processing

- Conducting audits to ensure compliance and address potential issues proactively Serving as the point of contact between the Trust and GDPR Supervisory Authorities
- Monitoring performance and providing advice on the impact of data & information protection efforts
- Maintaining comprehensive records of all data processing activities conducted by the Trust, including the purpose of all processing activities, which must be made public on request
- Interfacing with data & Information service users to inform them about how their data is being used, their rights, and what measures the Trust has put in place to protect their personal information

7.9 Cyber Security Officer

Supporting the Trust to continuously assess, implement and manage Trust-wide cybersecurity, and removing identified vulnerabilities with support from all technical and business managers and users.

- Investigate new security risks and identifying appropriate solutions to mitigate those risks.
- Respond to real life security incidents that exist in our external environment whether we have been affected directly or not.
- Attend security events and forums to keep abreast of current threats and counter measures.
- Implement new security products/tools to perform specific security roles on our Infrastructure; including the daily operation of these products/tools to ensure they remain effective in preventing and detecting security issues.
- Maintain the existing ICT infrastructure at a pace of change and technical level that hasn't been necessary before but which is explicitly needed now to ensure that any vulnerabilities are addressed before they are exploited.
- Attend specialist training courses to give staff the skills and expertise to be able to:
    - identify security risks;
    - resolve security incidents;
    - utilise security products/tools effectively
- Develop clear security procedures for frontline staff on how to react to Cyber Threats e.g. Cyber Incident Process and business continuity
- Transfer knowledge to other members of IMST to improve our all-round security awareness and capability.
- Support third party penetration testing identifying physical and virtual threats and taking appropriate remedial actions.
- Manage risks arising from shared infrastructure/services with third party organisations, ensuring the Trust remains protected.

7.10 Information Asset Owners

Information Asset Owners will be senior representatives of the directorates closely aligned to major stores of organisational data, information and systems. They will be supported by Trust specialists in data protection, freedom of information and IT security.

Some responsibilities of are:

- Overseeing administration and management of all organisational data & information through the use of Information Asset Managers.
- Ensuring standardisation of data & information procedures Trust-wide including handling and access.
- Establishing policies that manage Trust data & information.

- Creating guidelines regarding definitions of data & information attributes, policy, access and data & information elements that cross data & information manager boundaries.
- Control the implementation of data & information related policies and monitor the progress of their implementation.
- Controlling the management of organisational data & information including setting priorities for different data elements.
- Overseeing the establishment and maintenance of the enterprise data & information model.
- Incorporating and delivering data quality requirements within annual service plans;
- Monitoring and addressing data quality issues within their clinical services (via Service Line and Divisional performance and governance meetings);
- Ensuring that staff attend data quality training and adhere to policies and procedures;
- Contributing to the development of the training programme and audit programme.
- The owners will be supported in discharging these responsibilities through the direct support of IMST Staff.

All levels of Data & Information control are covered by this document including but not limited to:

- Shared commercially
- Shared between Trusts
- Shared academically
- Shared for FOI purposes

7.11 Information Asset Managers

Information Managers have the primary administrative and management responsibilities for segments of data primarily associated with their functional area. The Information Manager for a particular area of the Trust must be associated with that area, i.e. the Information Asset Manager for the HR department data would be a senior member of the HR directorate.

Data Responsibilities:

- Interpreting policy and defining procedures pertaining to the use and release of the data for which they are responsible.
- Ensuring proper use of organisational data in accordance with Trust and UK policy.
- Ensure accuracy and quality of data.
- Implement programs for data quality improvement.
- Help to ensure the standardisation of data elements through regulation of code values and look-up tables by developing Trust-wide procedures for use in association with other Information Asset Managers. This includes how data is stored and that standardised documentation regarding the data exists.
- Ensuring compliance with applicable Trust and UK policies and regulatory requirements,and take appropriate action if incidents violating these requirements occur.
- Approving requests for access to organisational data and making sure that the appropriate levels of access and permission are granted dependant on the classification of the data.
- Promoting information handling procedures to staff that may be required to handle the data for which they are responsible.
- Assisting staff in the interpretation and use of the data elements as required.

- Identifying the most reliable source for data and the update precedence when more than one source exists.
- Identifying any NPD within the data element and that suitable procedure is in place to protect this data.
- Managing the lifecycle of the data element including generation, use, retention and disposal.
- Ensuring that education is provided to data users in the control and handling of data.

Information Responsibilities:

- Be directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets.
- Ensure their team and those interacting with the asset understand information security and are confident in their handling of information.
- Lead and foster a culture that values, protects and uses information for public good.
- Know who has access and why, and ensure that their use of the asset is monitored.
- Understand and address risks to the asset, provide assurance to the SIRO and ensure any data loss incidents are reported and appropriately managed.
- Ensure any new information assets have a completed Data Protection Impact Assessment and are entered on the Information Asset Register.
- Any changes to an information asset are documented on the Information Asset Register and follow the correct change control process.
- Put procedures and controls in place to ensure the integrity and availability of their information assets.
- Put in place a business continuity plan for any key information assets.
- Are aware of what information is held, and the nature of and justification for information flows to and from the assets for which they are responsible.
- Ensure there is good understanding of the hardware and software composition of their assigned assets to ensure their continuing operational effectiveness. This includes establishing and maintaining asset records that will help predict when asset configuration changes may be necessary.
- Review their information assets on an annual basis as a minimum.
- To provide a report on the status of the asset to the DIGG on a yearly basis.

System Responsibilities:

- Work closely with IMST & third parties to ensure continuous system and technical data and information compliance, business continuity, Service Level Agreements & Operational Level Agreements are in place.
- Communicate a system roadmap and delivery plan to the technical service lead and appropriate governance board.
- Manage major issues and governance exception & incidents in accordance with Trust policy.
- Sign off and agree system change and agreed maintenance

7.12 Information Manager

- Overseeing and managing Informatics team towards critical Trust data, information and reporting needs and regulatory requirements
- Managing national data set delivery and introduction of new national data and information technical standards and implementation.
- Reporting to Head of Informatics & Information Systems

7.13 Data & Information Quality

Data & Information Quality is crucial and the availability of complete, accurate, relevant, accessible and timely data is important in supporting patient care, clinical governance, management and service agreements for healthcare planning and accountability. A data quality policy and regular monitoring of data standards are a requirement of the Data Security & Protection Toolkit.

Quality information is essential for:

- The delivery of effective, relevant and timely care, and to minimise risks to patients
- Efficient administrative and health care processes, such as communication with patients, their families and other carers and professionals involved in their treatment/care
- Management and strategic planning, requiring accurate information about the volume and type of health care activity to provide appropriate allocation of resources and future service delivery
- Establishing acceptable service agreements for health care provision
- Health care governance, which depends on detailed, accurate patient data for the identification of areas where health care could be improved
- Providing information for other NHS and non-NHS organisations – these organisations depend on the information we send them and need to have confidence in its quality
- Being able to allow local and national benchmarking
- Budget Monitoring, including Payment by Results, and financial planning to support service delivery
- It is also important to ensure that the data quality is of a high standard in order to comply with the UK GDPR, in particular principle 4 - 'accurate and up-to-date', and to satisfy the national NHS data quality requirements.

Good quality data is SMART

- Specific - valid
- Measurable – consistently understood across the organisation
- Accurate and held securely and confidentially
- Realistic – comprehensive in coverage
- Timely – delivered to a timescale that fits the purpose for which it is used.

Good quality data will be used by the Trust to support:

- Effective patient care
- Risk minimisation
- Information for patients
- Clinical governance
- Corporate governance
- Efficient clinical and administrative processes
- Effective communication and engagement with service users, their families and carers
- Appropriate allocation of resources
- Operational management
- Strategic planning
- Information for other NHS organisations such as service level agreements with commissioners
- Future projects
- Complying with statutory duties, including Public Sector Equality Duty (Equality Act 2010)

A high level of data quality will be maintained by the Trust through:

- Setting and meeting standards
- Collecting and processing data according to nationally and locally defined standards
- Setting local standards where national standards are not appropriate or do not meet the requirements of a specialist hospital
- Ensuring staff are aware of policies and receive ongoing training
- In working with partnerships the Trust expects the organisations with whom it works to meet the same data quality expectations as those of the Trust

Standards are necessary to ensure that data is:

Accurate – Data should be sufficiently accurate for its intended purposes, representing clearly and in sufficient detail the interaction provided at the point of activity. Data should be captured only once, although it may have multiple uses. Accuracy is most likely to be secured if data is captured as close to the point of activity as possible. Reported information that is based on accurate data provides a fair picture of performance and should enable decision making at all levels. The need for accuracy must be balanced with the importance of the uses of the data, and the costs and efforts of collection. For example, it may be appropriate to accept some degree of inaccuracy where timeliness is important. Where compromises have to be made on accuracy, the resulting limitations of the data should be clear to its users.

Valid – Data should be recorded and used in compliance with relevant requirements, including correct application of any rules or definitions. This will ensure consistency between periods and with similar organisations. Where proxy data is used for an absence of actual data, organisations must consider how well this data is able to satisfy the intended purpose.

Reliable - Data should reflect stable and consistent data collection processes across collection points and over time, whether manual or computer based systems or a combination. Managers and stakeholders should be confident that progress toward performance targets reflects real change, rather than variations in data collection approaches or methods.

Relevant - Data captured should be relevant to the purposes for which it is used. This entails periodic review of requirements to reflect changing needs. It may be necessary to capture data at the point of activity which will be relevant only for other purposes, rather than current intervention. Quality assurance and feedback processes are intended to ensure the quality of such data.

Complete – Data requirements should be clearly specified based on the information needs of the organisation and data collection processes matched to those requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in recording of certain data items.

Timely – Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available quickly and frequently enough to support information needs and to influence the appropriate level of service or management decisions.

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.

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 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 confidential, person-identifiable data and Trust systems	Review in light of any incidents, staff requests and suggestions	Information Governance Manager; Assistant Deputy Directors of IMS&T; Data Protection Officer; IT Dept.	Annual	Data & Information Governance Group	Information Governance Manager; Assistant Deputy Directors of IMS&T; Data Protection Officer; IT Dept.	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 – 11/2025

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	DIGG	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	08/2018	08/2018		
1.1	11/2019	11/2019		
1.2	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 an annual basis.

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

The Information Governance team will work the Senior Information Risk Owner, Information Asset 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/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

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, 20 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?	✓