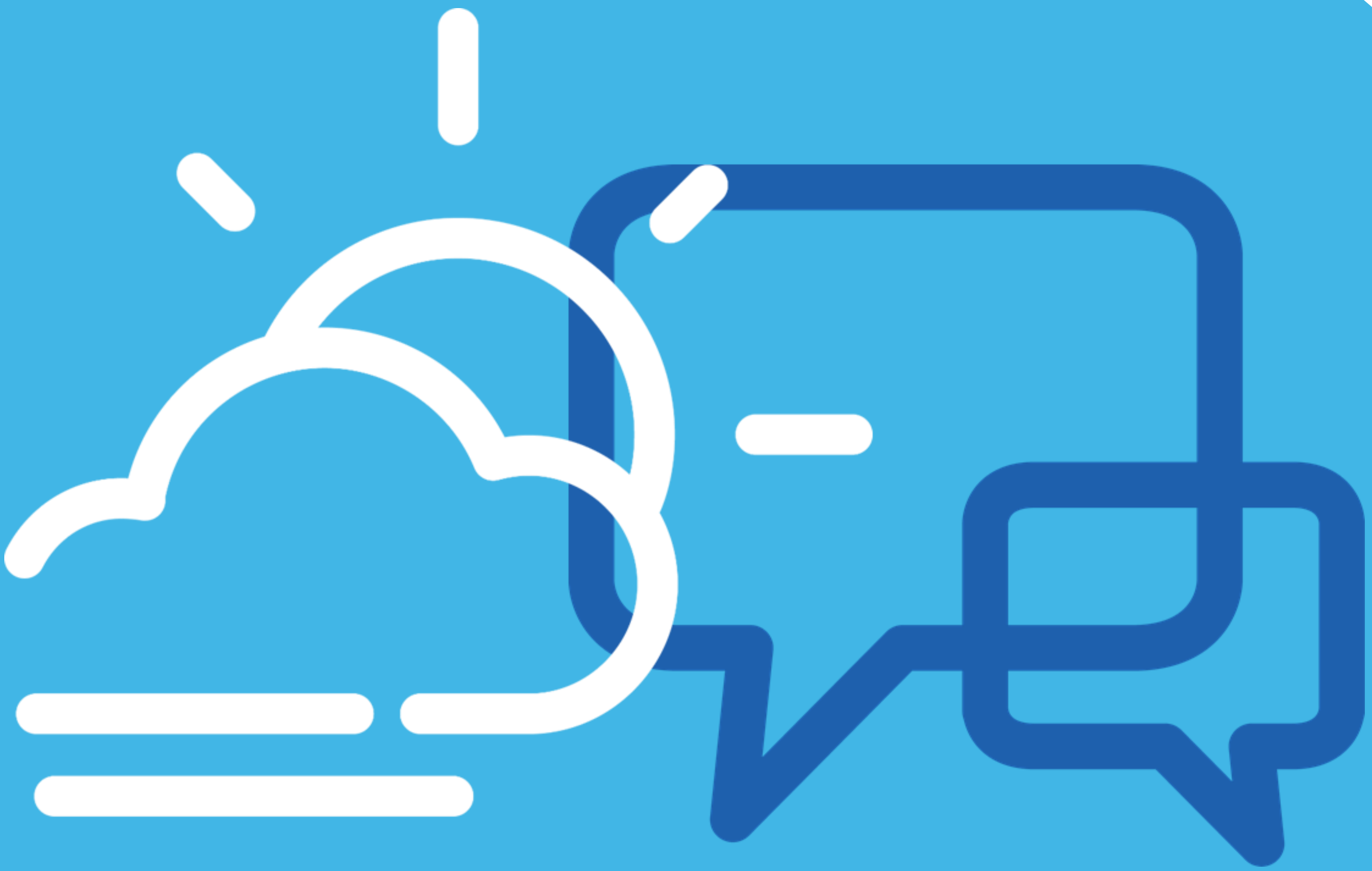
NHS
Greater Manchester
Mental Health
NHS Foundation Trust

Information Governance Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Information Governance Policy**
Executive Summary:	Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. This policy sets out the arrangements that Greater Manchester Mental Health has in place to deliver the Information Governance and Data security and protection agenda.
Executive Lead:	Director of Finance, Capital & IM&T
Document Author:	Deborah Tonkin (Information Governance Manager)
Document Purpose:	Policy
Target Audience:	All staff and contractors, permanent, temporary, seconded, (including volunteers), in all staff groups and all contract types, including bank workers.
Additional Circulation List:	All staff via SharePoint
Date Ratified:	15/01/19
Ratified by:	Information Governance Steering Group (IGSG)
Consultation:	Representatives from all directorates via membership of the IGSG.
Cross Reference:	All Information Governance policies
Superseded Docs:	GMMH Information Governance Policy (IG06) V1
Date of Equality Impact Assessment:	Pending
Board Objective Reference:	3 – to engage in effective partnership working 6 – to achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Regulation 17 : Good governance
Risk Register Reference:	N/A
Contact Details for further information	Deborah Tonkin (Information Governance Manager) Deborah.tonkin@gmmh.nhs.uk Tel: 0161 358 1573
Document Status	This is a controlled document. Whilst this document may be printed, the electronic version posted on the Trust intranet is the controlled copy.

Contents

1. Introduction

This Information Governance Policy provides is the overarching policy for the trusts Data Security and Protection framework. The framework brings together all the legal rules, guidance and best practice that apply to the handling of information, allowing:

- implementation of central advice and guidance;
- compliance with the law;
- year on year improvement plans.

1.1. Purpose

This policy aims to provide a clear Data Security and Protection Management Framework which has effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

At its heart, Information Governance along with Data Protection and Security is about setting a high standard for the handling of information. The ultimate purpose is to demonstrate that Greater Manchester Mental Health NHS Trust, (referred to hereafter as the Trust or Greater Manchester Mental Health), can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good Information Governance and to be consistent in the way they handle personal and corporate information. Greater Manchester Mental Health recognises information is a vital asset and without it the Trust would not be able to:

- manage individual service users and staff;
- plan day to day activities;
- manage budgets;
- contract with commissioners;
- develop services;
- monitor performance;
- provide assurance to regulators and stakeholders, (e.g. Monitor, CQC, NHS Resolution).

1.2. Scope

This policy sets out the arrangements that Greater Manchester Mental Health has in place to deliver the Information Governance and Data security and protection agenda across the trust and is therefore relevant to all staff and contractors, permanent, temporary, seconded, (including volunteers), in all staff groups and all contract types, including bank workers.

2. Definitions

- **DS&PT** – Data Security and Protection Toolkit which replaces the previous Information Governance Toolkit.

- **ICO** - Information Commissioner’s Office
- **Information** - Service User, Staff and Corporate information in all media
- **Trusted Organisation** -
  1. Demonstrating up to date compliance with DS&PT Standards and maintaining these standards each year.
  2. Maintaining registration with the ICO for the processing of personal information.

3. Duties

3.1. Board/Lead Committee

The Information Governance Steering Group (IGSG) will be responsible for the approval and monitoring of this Policy. A full list of responsibilities is documented under the Information Governance Management Framework at 3.7.1 of this Policy.

The IGSG is accountable to the Digital Strategy Board who has responsibility for ensuring that sufficient resources are provided to support the requirements of this Policy.

3.2. Chief Executive

The Chief Executive has overall accountability and responsibility for the Trusts compliance with Information Governance standards. They will provide assurance through the Statement of Internal Control that all information risks are effectively managed and mitigated.

3.3. All Directors, Heads of Service and Managers

All Directors, Heads of Service and Managers will be responsible for ensuring that this Policy is communicated and implemented within their area of responsibility and that the principles and standards which constitute good Data Security and Protection and Information Governance are adopted and are followed on a day to day basis.

3.4. All staff and Contractors

All staff should be aware of their own personal responsibilities for Information Governance and compliance with the law. Contractors are responsible for ensuring they are aware of the requirements incumbent upon them and for ensuring they comply with these.

3.5. Senior Roles

3.5.1 Information Governance Lead

The Information Governance Lead is the Director of Finance, Capital & IM&T, on a day-to-day basis this responsibility has been delegated to the Information Governance Manager. They are accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Data Security and

Protection and IG. Key tasks will include:

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities.
- Ensuring that there is top level awareness and support for IG along with DS&P resourcing and implementation of improvements.
- Providing direction in formulating, establishing and promoting IG policies.
- Establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives.
- Ensuring annual assessments and audits of the Data Security and protection policies and arrangements are carried out, documented and reported.
- Ensuring that the annual DS&P assessment and improvement plans are prepared for approval by the senior level of management, i.e. Information Governance Steering Group.
- Ensuring that the approach to information handling is communicated to all staff and made available to the public.
- Ensuring that appropriate training is made available to staff and completed as necessary to support their duties.
- Liaising with other committees, working groups and programme boards in order to promote and integrate IG standards.
- Monitoring information handling activities to ensure compliance with law and guidance.
- Providing a focal point for the resolution and/or discussion of IG issues.

3.5.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is the Director of Finance & IM&T. The SIRO will act as an advocate for information risk on the Board and in internal discussions. Key tasks will include:

- Implement information risk via the Information Asset Management and wider Trust Risk Management Policy.
- Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- Ensure that the Trust’s approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Approve Pseudonymisation and Restricted Document requests in clinical information system.

3.5.3 Caldicott Guardian

The Caldicott Guardian will act as an advocate for information sharing on the Board and in internal discussions. Key tasks will include:

- Ensuring that the Trust and its partner organisations satisfy the highest practical standards for handling patient identifiable information.
- Acts as the 'conscience' of the Trust in relation to information sharing.
- Supports work to enable information sharing where it is appropriate to share.
- Advises on options for lawful and ethical processing of information.

3.5.4 Data Protection Officer

The GDPR introduces a legal duty to appoint a Data Protection Officer (DPO) for all public authorities and in organisations that carry out certain types of processing activities.

DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments, (DPIAs) and act as a contact point for data subjects and the supervisory authority (ICO).

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The Trust’s DPO will help demonstrate compliance and is part of the enhanced focus on accountability within the Trust.

3.6. Information Governance Team and Other Key Roles

3.6.1 Associate Director of IM&T

The Associate Director of IM&T is responsible for the quality assurance of FOI and subject access responses, reviewing and signing off all DS&P toolkit submissions and action plans as well as delivering IG service improvement priorities.

3.6.2 Head of IT Service Delivery/Deputy SIRO

The Head of IT Service Delivery is responsible for reviewing IG evidence and requirement owner progress throughout the year whilst sitting on the IG requirement panel and acting as the Deputy SIRO.

3.6.3 Information Governance Manager

The Director of Finance & IM&T has delegated the day to day responsibilities as Information Governance Lead to the Information Governance Manager (IGM). A full list of responsibilities is documented under the Information Governance Management Framework, Senior Roles at 3.5 of this Policy.

The Information Governance Manager acts as the Operational Information Governance Lead and the Information Security Officer for the Trust and as such occupies a key role in the delivery of Information Governance activities, with providing advice on all aspects of information security and risk management.

The key responsibilities of the Information Security Officer are to:

a. Draft and/or maintain the currency of the organisation's Information Security Policy.

b. Ensure all arrangements for managing Information are effective and aligned with the organisation's Information Security and Risk Policies.

c. Provide advice for the completion of Data Protection Impact Assessments and escalate any risks to the DPO where appropriate.

d. Provide reports to the senior member of management (e.g. a SIRO/IAO or equivalent) who has responsibility for Information Governance.

e. Provide regular information security risk assurance reports to the information risk lead (SIRO) and, depending upon the supporting structure established, to IAOs and the Information Governance Steering Group

f. Co-ordinate the work of other staff with information security responsibilities.

g. Co-ordinate the necessary response and resolution activities following a suspected or actual security incident or breach. Keeping the SIRO, DPO and information asset owners (IAO's) informed of security incidents, impacts and causes, resulting actions and learning outcomes.

h. Assist in the drafting of System Level Security Policies.

i. Assist in the development of Business Continuity Management arrangements for key information assets.

j. Advise in the development of a Network Security policy and controls for the secure operation of ICT networks, including remote/teleworking facilities.

k. Assist in developing the organisation's Information Asset Register.

l. Develop and document an action plan for the delivery of all specific activities involving the ISM.

3.6.4 Head of ICT – Cyber security

The key responsibilities of the Head of ICT in respect of DS&P and Cyber security are:

a. Ensure security accreditation of information systems in line with the organisation's approved definitions of risk and relevant NHS standards.

b. Ensure compliance with the information security and cyber security components of the DS&P toolkit, contributing to the annual IG assessment.

c. Advise in the development of a Network Security policy and controls for the secure operation of ICT networks, including remote/teleworking facilities.

d. Provide advice and guidance regarding the implementation of IG security standards and controls to mitigate against malicious or unauthorised mobile code.

e. Assist in designing and configuring access controls for key systems.

3.6.5 Senior Information Governance Officer

The Senior Information Governance Officer is responsible for establishing and maintaining policies in relation to DS&P and information governance, security, confidentiality, data protection and information risk. They will put in place effective arrangements to ensure the security and manage the risks associated with Trust information assets and resources. Key tasks will include:

- Providing operational support to the IGM and SIRO.
- Ensuring that all Trust information assets are recorded and risk assessed by the respective Information Asset Owner.
- Investigate Information Governance incidents in relation to data loss and confidentiality breach incidents and feedback to the IGM and DPO.
- Conduct or co-ordinate audits of Information Governance standards which are aligned with the Trust Audit Programme.
- To oversee and advise on the Information Sharing Agreement process.
- Support the Information Governance Manager in embedding an Information Governance culture.
- Ensuring that information sharing agreements are in place with partner organisations.
- Embed the requirement for Data Protection Impact Assessments and assist in the completion and escalating all identified risks to the IG Manager.
- Investigate Information Governance incidents in relation to breaches of confidentiality.
- Provide reports where required to the IGSG and act upon recommendations to improve IG across the trust.
- Discharging the FOI process.

3.6.6 Information Governance Officer

The Information Governance Officer is responsible for establishing and maintaining policies in relation to the Freedom of Information Act. They will put in place effective arrangements to ensure the process meets with current legislation requirements.

Key tasks will include:

- Delivering Information Governance induction sessions to new starters and other training as appropriate.
- To oversee and advise on the Data Protection Impact Assessment process.
- Updating the publication scheme.
- Collating Information Governance Requirement evidence.
- Support the Information Governance Team in embedding an Information Governance culture across the organisation.
- Dealing with Information Governance queries.
- Implementing Pseudonymisation across the Trust so that when information is used for a secondary purpose it will be effectively de-identified.

3.6.7 Registration Authority Manager

The Registration Authority Manager supports the Information Governance agenda and is responsible for establishing and maintaining the Registration Authority Policy. They will put in place effective arrangements to ensure the confidentiality of personal and other sensitive information with the administration of Smartcards.

3.6.8 Information Quality Assurance Team

The Information Quality Assurance Team is responsible for establishing and maintaining policies in relation to Information Quality, Records Management, Subject Access Requests and Access to Health Records. They will put in place effective arrangements to ensure information within the Trust is of the highest quality in terms of completeness, accuracy, relevance and timeliness.

Key tasks will include:

- Ensuring the standards in the Data Quality Policy are adhered to.
- Leading on and delivering appropriate training for clinical services to improve the data quality of information in all clinical systems.
- Ensuring that robust processes are in place for Subject Access Requests.
- To oversee and advise on the records management process.
- Investigate Information Governance incidents in relation to loss of records or poor records management practice.
- Conduct or co-ordinate audits of records management standards which are aligned with the Trust Audit Programme.

3.7. Key Governance Bodies

3.7.1 Information Governance Steering Group

The Information Governance (IG) Steering Group is accountable to the Greater Manchester Mental Health NHS Foundation Trust IM&T Digital Strategy Board. Its purpose is to support and drive the broader Information Governance and Data Protection and Security agenda through the development of best practices which are acceptable, practicable, ‘owned’ and therefore better supported across the whole organisation. It will also influence the integration and inclusion of IG standards with other governance, strategies, work programmes and projects.

Key responsibilities of the Information Governance Steering Group:

- Provide assurance to the Digital Strategy Board that an appropriate comprehensive and effective Information Governance and Data Protection and Security framework and systems are in place throughout the Trust in line with national standards.
- Have delegated responsibility from the Digital Strategy Board to ratify Information Governance strategies, policies and procedures.
- Direct the work of the Information Governance Operational Group.
- Receive decision making requests from the Information Governance Operational Group.
- Ensure that the Trust’s approach to information handling is communicated to all

staff and that they are made aware of individual responsibilities through policy, procedure and training.

- Inform the review of the management and accountability arrangements for Information Governance.
- Ensure that all requirements of the Data Security and Protection Toolkit are implemented and that work plans are developed to track actions and monitor progress.
- Ensure that all requirements of NHS Resolution and CQC related to Information Governance are met.
- Approve and sign off the annual Information Governance assessment.
- Report final DS&P Toolkit scores to the Digital Strategy Board.
- Receive reports from each of the work areas and act on them if necessary.

3.7.2 Information Governance Operational Group

The Information Governance (IG) Operational Group is accountable to the Information Governance (IG) Steering Group. Its purpose is to implement Information Governance best practice across the whole organisation.

Key responsibilities of the Information Governance Operational Group:

- To ensure that an appropriate comprehensive Data Security and Protection and Information Governance framework and systems are in place throughout the Trust in line with national standards.
- To ensure that the Trust has effective policies and procedures in place that cover all aspects of Data Security and Protection including an Information Governance policy and associated implementation strategy.
- To ensure that the Trust undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.
- To develop the Data Security and Protection work programme and improvement plan on an annual basis and to monitor the implementation of that plan.
- To provide a focal point for the resolution and/or discussion of Information Governance operational issues.
- To liaise with other Trust committees, working groups and programme boards in order to promote Information Governance issues.
- To prepare the annual DS&P assessment for sign off by the IG Steering Group.
- Cascade the Trust’s approach to information handling to all staff.
- To ensure that training made available by the Trust is taken up as necessary to support their role.
- To receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action. The group will share any learning experience towards an improved and effective service.
- To ensure that all relevant risks are recorded on the Trust Risk Management

System (DATIX).

- To ensure that Data Flow Mapping has been reviewed and updated on a yearly basis.

4. Processes and Procedures

4.1. Policy Statement

The Trust will ensure robust Information Governance by demonstrating compliance with the standards set out in the Data Security and Protection Toolkit through maintaining a satisfactory score.

The Trust will create and maintain its ‘plan’ through the DH NHS Digital online system which enables:

- Owners to be assigned to assertions.
- Evidence to be collated.
- Reports to be created of the above.

4.2. Confidentiality and Data Protection

The Trust will ensure that:

- The Data Security and Protection for the Information Governance agenda is supported by adequate resources with suitable confidentiality and data protection, GDPR skills, knowledge and experience.
- Policies in relation to Data Security and Protection are established and maintained.
- Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users.
- Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected in line with legislation.
- Individuals are informed about the proposed uses of their personal information via Privacy Notices.
- There are appropriate procedures for recognising and responding to individuals requests for access to their personal data.
- There are appropriate confidentiality and audit procedures to monitor access to confidential personal information.
- It proactively uses information with its partner organisations to support care as determined by law, statute and best practice. Where information is shared with partner organisations an information sharing agreement or contract will be established or alternatively partners should be a ‘trusted organisation’.
- All person identifiable data processed outside of the UK complies with the

General Data Protection Regulation, Data Protection Act (2018) and Department of Health guidelines.

- All new (and changes to) processes, services, information systems and other relevant assets are developed and implemented in a secure and structured manner to comply with IG security accreditation, information quality and confidentiality and data protection requirements via the Data Protection Impact Assessment.

4.3. Information Security and Risk

The Trust will ensure that:

- The Information Governance agenda is supported by adequate resources with suitable information security skills, knowledge and experience.
- Policies in relation to information security and information risk are established and maintained.
- A formal information risk assessment and management programme for the appropriate management of key information assets is in place.
- Documented information security incident / event reporting and management procedures are accessible to all staff.
- There are established business processes and procedures that satisfy the Trust’s obligation as a Registration Authority.
- Monitoring and enforcement processes are in place to ensure that NHS national application Smartcard users comply with the terms and conditions of use. Operating and application information systems, under the Organisation’s control, support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.
- An organisational structure to include IAO’s and IAA’s support the Senior Information Risk Owner (SIRO) is in place.
- All transfers of hard copy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers.
- Business Continuity Plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service-specific measures are in place.
- Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.
- Information assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code.
- Have policy and procedures in place to ensure that Information Communication Technology (ICT) Networks operate securely.
- Policy and procedures are in place to ensure that mobile computing and teleworking are secure.

- All information assets that hold or are personal data, are protected by appropriate organisational and technical measures.
- The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate.
- Adherence to confidentiality is audited daily through FairWarning reports.
- It adopts safe haven practices that include the concept of 'new safe haven'.

4.4. Clinical Information

The Trust will ensure that:

- The Information Governance agenda is supported by adequate resources with suitable information quality and records management skills, knowledge and experience.
- Policies in relation to records management and information quality are established and maintained.
- There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements.
- Procedures are in place to ensure the accuracy of service user information on all systems and/or records that support the provision of care.
- A multi-professional audit of clinical records across all specialties is undertaken.
- Procedures for monitoring the availability of paper healthcare records and tracing missing records are in place.

4.5. Secondary Uses

The Trust will ensure that:

- National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop.
- External data quality reports are used for monitoring and improving data quality.
- Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained.
- A documented procedure and a regular audit cycle for accuracy checks on service user data is in place.
- Clinical staff are involved in validating information derived from the recording of clinical activity.
- The Completeness and Validity check for data has been completed and passed.
- An audit of clinical coding, based on national standards, will be undertaken by an NHS Classifications Service approved clinical coding auditor every 12 months.
- Training programmes for clinical coding staff entering coded clinical data are

comprehensive and conform to national standards.

4.6. Corporate Information

The Trust will ensure that:

- Documented and implemented procedures are in place for the effective management of corporate records.
- Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act (2000).
- As part of the information lifecycle management strategy, an audit of corporate records will be undertaken annually.

4.7. Key Policies

All policies are created in line with the Trust Policy for the Development & Management of Trust Wide Documents and are distributed for consultation before being ratified by the Information Governance Steering Group. Once approved, staff will be made aware of new policies through the staff newsletter and dissemination from the IGSG. Policies are made available to staff electronically via the intranet and all Data Security and Protection polices will be published on the trust internet site.

The Data Security and Protection framework consists of the following policies:

- Information Governance Policy
- Information Governance Staff Handbook
- Confidentiality Policy
- Information Sharing Policy
- Information Security Policy
- Mobile Media Security Policy
- Information Asset Management Policy
- Registration Authority Policy
- Safe Haven Policy
- Records Management Policy
- Corporate Records Management Procedure
- Health Records Management Procedure
- Freedom of Information Policy
- Data Quality Policy.

4.8. Governance Framework

Responsibility and accountability for Information Governance is cascaded through the Trust in the following ways:

4.8.1 Staff Contracts and Contracts with Third Parties

All staff and those undertaking work on behalf of the Trust need to be aware that they must meet Information Governance requirements and it should be made clear to them that breaching these requirements, e.g. service user confidentiality, is a serious disciplinary offence. It is therefore important that all staff have a contract of employment which sets out responsibilities with regard to data protection, confidentiality, and information security.

In addition, any third party with whom the Trust carries out business either as an agent or supplier, where the work involves access to information about identifiable individuals or access to locations where this information is available must have terms specified in contracts relating to expectations and compliance with Information Governance standards. The Information Governance Team can be contacted for advice if required.

4.8.2 Information Asset Owner (IAOs) Arrangements

Information Asset Owner have been appointed in each Directorate across the Trust. They are senior individuals who have responsibility for one or more information assets. For information risk, IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets. The process is described in detail in the Information Asset Management Policy.

In addition, IAOs will appoint one or more Information Asset Assistants who will support them on a day to day basis.

The Information Governance Manager will provide on-going day to day advice and support to Information Asset Owners and coordinate the IAO work plan on behalf of the SIRO.

IAOs are members of the Information Governance Steering Group.

4.8.3 Information Governance contacts/Information Asset Assistants

IAA’s have been appointed in each Directorate across the Trust. They are operational managers who have additional responsibilities for supporting the Information Governance agenda. They will cascade and communicate best practices applying to the handling of information.

All IAA’s are members of the Information Governance Operational Group.

4.8.4 Work stream Leads and Assertion Owners

Work stream Leads and assertion Owners are identified annually and standards are allocated based on area of expertise or role within the Trust. They support the DS&P Toolkit assessment process by working through requirements to ensure the Trust has the necessary policies, procedures and processes in place to comply with the Information Governance standards and meet all Data Security and Protection requirements.

All assertion owner are members of the Information Governance Steering Group.

4.9. Training and Guidance

4.9.1 Training

The Education Commissioning Document sets out the Trust approach to training in Information Governance, confidentiality, data protection and data security. In summary, this document mandates that all staff are required to complete basic Information Governance training appropriate to their role through the Trust learning hub.

All new staff must complete online IG training prior to starting their new post.

Additional requirements have been placed on specific staff in key roles. These are reviewed on an annual basis by the IGSG and relevant staff are informed by the Information Governance Team.

Training for specialist staff will be identified through the appraisal process and will be arranged in line with development needs and the individual’s personal development plan. Specialist training needs analysis can be found in Appendices.

4.9.2 Guidance

Staff need clear guidelines on expected working practices. In addition to Trust policies and procedures the Information Governance Department will provide:

- Regular communications to staff on new Information Governance policies and procedures.
- Access to policies and procedures through intranet.
- Contact details for staff who can provide specialist support in Information Governance.
- Regular communications in the Trust staff newsletter relating to up to date advice and guidance on relevant issues.
- Further development of the Information Governance section on intranet so that it becomes a comprehensive knowledge base resource for staff and the first point of call for advice and assistance.

4.10. Incident Management

All staff have responsibility to immediately report any incident involving the known or suspected loss of information or breach of confidentiality. Clear guidance on this process is available through the Trust Incident, Accident and Near Miss Policy and Procedure which have been aligned with the “Checklist for Reporting, Managing and Investigating IG Serious Incidents (SI)”.

Information Governance related breaches must also be reported through the DS&P Toolkit. This will then automatically inform the ICO if the breach is of a significant level.

5. Training Requirements

Refer to the Induction and Training Policy and the specialist training needs analysis in the appendices and see also section 4.9.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
IG Work Programme Progress	Monthly/ Quarterly	DS&P Toolkit	Minutes	IG Manager	Information Governance Steering Group / Information Governance Operational Group / IM&T Strategy Group
Incident Analysis	Monthly/ Quarterly	DATIX	Minutes	Senior IG Officer	Information Governance Steering Group / Information Governance Operational Group
Uptake of DS&P Toolkit	Monthly	DS&P Toolkit	Report	IG Officer	Information Governance Steering Group / Information Governance Operational Group
DS&P Toolkit Annual Assessment	Annually for sign-off	DS&P Toolkit	Assessment	IG Manager	Information Governance Steering Group

7. Resource/Implementation Issues

The Information Governance Framework has been reviewed and no resource issues have been identified.

8. Risk Issues

None have been identified by the Author.

9. Requirements, Supporting Documents and References

9.1. Requirements

Board Objective Reference:	3 – to engage in effective partnership working 6 – to achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Regulation 17 : Good governance

Other requirements	Legislation including the General Data Protection Regulation and the Data Protection Act

9.2. Supporting Documents

- Common Law Duty of Confidentiality
- Access to Health Records Act (1990)
- Data Protection Act (2018)
- General Data Protection Regulation
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- NHS Data Security and Protection Toolkit
- Information Security Management: NHS Code of Practice
- Records Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- Caldicott reviews 1, 2 and 3.

9.3. References

- Information Governance Education Commissioning Document.

10. Subject Expert and Feedback

All queries should be directed to the author.

11. Review

Trust policy for review is every five years, however this policy will be reviewed annually in line with the Data Security and Protection Toolkit, or sooner in the light of organisational, legislative or other changes.

12. Appendices

See following pages.

Appendix 1 – Training Needs Analysis for Specialist IG Training

All Information Governance training is to be completed on an annual basis in line with the Data Security and Protection Toolkit. Completion of specialist training is required for specific job roles within the Trust. The required training has been detailed below:-

Names	Mandatory Training	Specialist Training	Access to Records Management	Additional training compliance
SIRO	✓	✓		
Deputy SIRO	✓	✓		
Caldicott Guardian	✓	✓		
Data Protection Officer	✓	✓		
Information Asset Owners	✓	✓		✓
Information Asset Assistants	✓	✓		
Information Quality Manager	✓	✓		
Information Governance Manager	✓	✓		✓
Information Quality Assurance –	✓	✓		
Information Governance Team	✓	✓		✓
SAR Co-ordinators	✓	✓	✓	
All staff	✓			