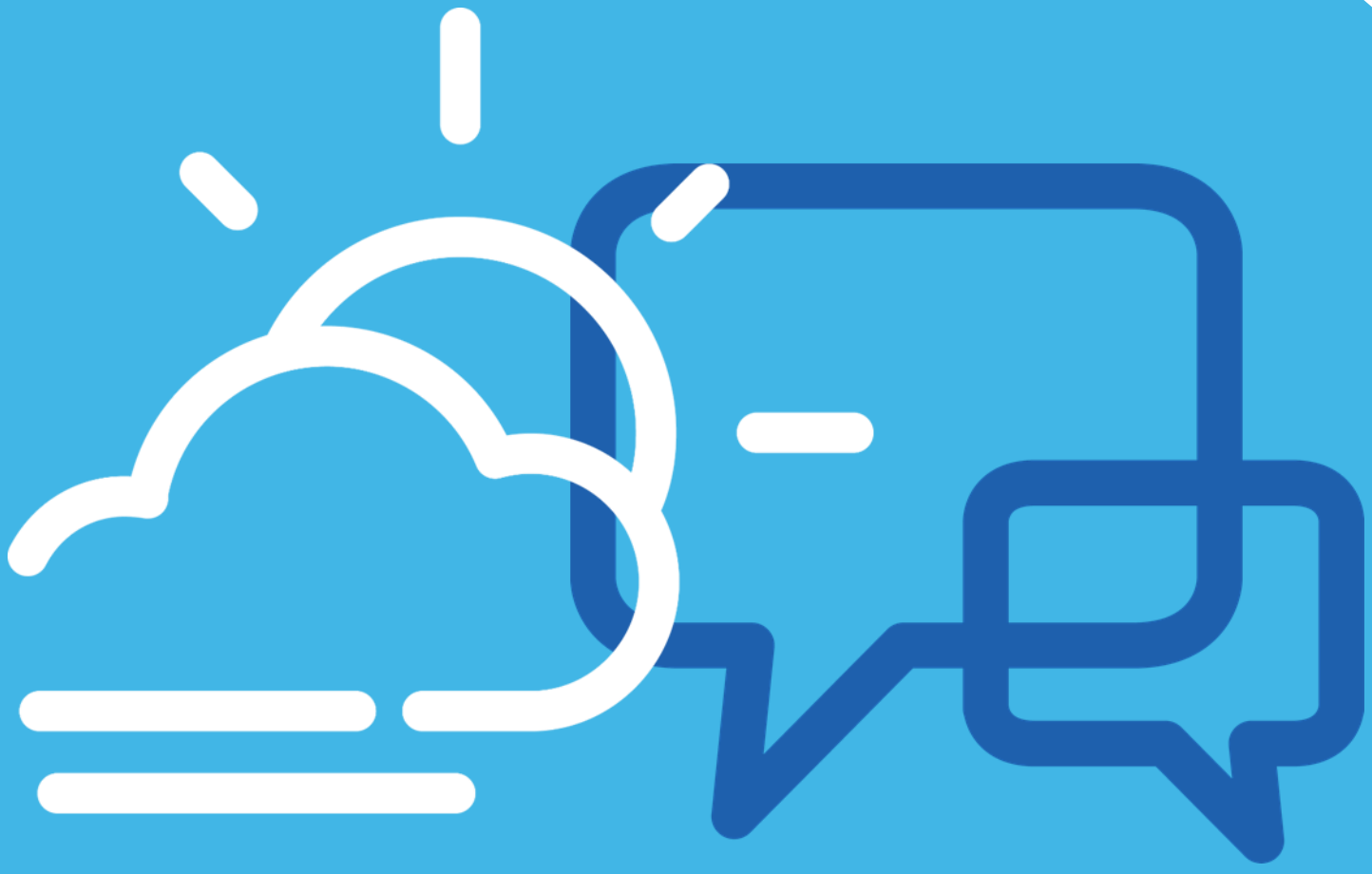
NHS
Greater Manchester Mental Health
NHS Foundation Trust

Information Asset Management Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Information Asset Management Policy**
Executive Summary:	This policy forms part of Greater Manchester Mental Health Trust's Information Security Management System and outlines the approach to information risk and information asset management in order to protect GMMH, its staff and patients from such risks.
Executive Lead:	Director of Finance and IM&T
Document Author:	Deborah Tonkin, Information Governance Manager
Document Purpose:	Policy
Target Audience:	All staff of GMMH Mental Health Trust including clinical, contractors and students.
Additional Circulation List:	N/A
Date Ratified:	15/01/2019
Ratified by:	Information Governance Steering Group
Consultation:	All staff via SharePoint Sept/Oct 2017; followed by consultation with representatives from all directorates via membership of the IGSG.
Cross Reference:	Related trust policies & guidelines including the Information Governance Policy
Superseded Docs:	GMW Information Asset Management Policy
Date of Equality Impact Assessment:	11/09/2017
Board Objective Reference:	2 – to work with service users & carers to achieve their goals; 4 – to invest in our environments; & 6 – to achieve sustainable financial strength & be well-governed.
CQC Regulation Reference:	CQC Quality & Risk Profile (QRP)
Risk Register Reference:	All risks to be assessed locally and on an individual basis as outlined within the body of this document.
Contact Details for further information:	Information Governance Team Tel: 0161 2710744/0161 3581573 mailto:InformationGovernance@gmmh.nhs.uk
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 4
1.1. Purpose 4
1.2. Scope 4
2. Definitions 5
3. Duties 7
3.1. Board/Lead Committee 7
3.2. Chief Executive 7
3.3. Information Governance Steering Group 7
3.4. Senior Information Risk Owner (Director of Finance and IM&T) 7
3.5. Data Protection Officer (DPO) 8
3.6. Information Governance Manager 8
3.7. Information Asset Managers (IAO) 10
3.8. Information Asset Assistants 12
3.9. All Staff 12
4. Information Asset Management Process 12
4.1. Protection of Assets 12
4.2. Information Asset Register 13
4.3. Information Risk Assessments 13
4.4. Information Risk Management Strategy Group 14
4.5. Data Flow Mapping 14
4.6. Incident Reporting 14
4.7. Incident Categories 15
4.8. Data Protection Impact Assessments (DPIA) 15
4.9. Third Party Contractual Obligations 16
4.10. Privacy Notices 16
5. Training Requirements 16
6. Monitoring 16
7. Resource/Implementation Issues 17
8. Risk Issues 17
9. Requirements, Supporting Documents and References 17
9.1. Requirements 17
9.2. Supporting Documents 17
10. Subject Expert and Feedback 18
11. Review 18
Appendix 1 – Examples of Risks for Information Assets 19
Appendix 2 – Data protection by Design 22

1. Introduction

1.1. Purpose

Greater Manchester Mental Health Foundation Trust (GMMH) aims to provide the highest quality services that achieve economy, efficiency and effectiveness. Information asset management is an integral part of continuous quality improvement and GMMH is therefore committed to mitigating risk associated with information assets in all parts of the organisation.

Information handling can represent a significant corporate risk in the sense that failure to protect information properly or use it appropriately can have a damaging impact on the Trust's reputation with patients, customers, the public and other public sector bodies. It also opens up the possibility of legal action against the Trust and its board under its duty of care to handle patient information appropriately.

The risks associated with information assets are inherent in all administrative and business activities and everyone working for or on behalf of GMMH must continuously manage information assets. The Board recognises that the aim of information asset management is not to eliminate risks, but rather to provide the structural means to identify, prioritise and manage the risks involved in all GMMH activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that would be derived.

The key requirement is for information assets to be managed in a robust way within work areas and not be seen as something that is the sole responsibility of Information Management and Technology or Information Governance staff. Assurances need to be provided in a consistent manner. To achieve this, a structured approach is needed, building upon the existing information governance framework within which GMMH is already working. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

The Board acknowledges that information asset management is an integral part of good management practice. The intent is to embed information assets management in a very practical way into business processes and functions. This is achieved through key approval and review processes/controls, and not to impose assets management as an extra requirement.

This document is based on NHS Digital – NHS Information Risk Management (Digital Information Policy) January 2009.

1.2. Scope

To provide a clear Information Asset Management Framework that has 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 secure its information assets.

2. Definitions

Information Asset – Information assets come in many shapes and forms. Therefore, the following list can only be illustrative.

Typical information assets include:

- Personal Information Content
- Databases and data files
- Back-up and archive data
- Audit data
- Paper records (patient case notes and staff records)
- Paper reports
- Other Information Content
- CCTV
- System/Process Documentation
- System information and documentation
- Operations and support procedures
- Manuals and training materials
- Contracts and agreements
- Business continuity plans
- Computer Software
- Applications and System Software
- Data encryption utilities
- Development and Maintenance tools
- Computer Hardware
- Servers
- PCs
- Laptops
- PDAs
- Communication Devices (including Mobile Phones, Blackberrys etc.)
- Removable Media (USB drives, Memory Sticks, CDs, DVDs etc.)

- Environmental services e.g. power and air-conditioning
- People skills and experience
- Shared service including Networks and Printers
- Computer rooms and equipment
- Records libraries

The below definitions are in line with the Trust's Asset Management Policy

- **Threat** – any event or situation which has the potential to cause the loss of, unauthorised access to, unauthorised changes or destruction of, information assets held or controlled by GMMH.
- **Event –** a threat which materialises.
- **Risk** – the likelihood and severity of an event occurring. Other words, such as probability, consequence or impact are sometimes used instead, but GMMH uses likelihood and severity in all documents to avoid confusion.
- **Severity** – The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Likelihood** – A qualitative description or synonym for probability or frequency.
- **Information Assets Assessment –** the systematic process for prioritising information assets on the basis of a combination of the severity of consequence and likelihood of occurrence.
- **Information Assets Management** - the systematic process for identifying, assessing, mitigating and reviewing information asset risks.
- **Controls** – documents, systems, processes, devices and equipment intended to mitigate the likelihood and/or severity of a risk.
- **Incident** – any event which results, or might have resulted, in the loss of, unauthorised access to, or unauthorised changes or destruction of, any information assets held or controlled by GMMH. Further guidance can be found in the Incident, Accident and Near Miss Policy.
- **Reportable incident** - An incident that is 'likely' to have caused 'minor harm' is reportable to the ICO.
- **General Data Protection Regulation –** The General Data Protection Regulation (GDPR) applies across Europe from 25th May 2018. GDPR supersedes the previous UK Data Protection Act 1998 (DPA). GDPR brings significant and wide-reaching changes in the way we deal with data protection. It expands the rights of individuals to control how their personal

data is collected and processed, and places a range of new obligations on organisations to be more accountable for data protection.

- **Data Protection Act 2018 –** supersedes the DPA 1998.

3. Duties

3.1. Board/Lead Committee

The Board ultimately owns, and is accountable for ensuring that GMMH has, an Information Asset Management Policy. On a day to day basis the GMMH Information Governance Steering Group, on behalf of the Board, has taken ownership of this Policy.

3.2. Chief Executive

The CEO has overall responsibility and will delegate responsibility for the oversight and implementation of information asset management to a Director on the Board of GMMH. This Board member will be appointed as the Senior Information Risk Owner.

3.3. Information Governance Steering Group

The IGSG will on behalf of the GMMH Board be the committee responsible for the oversight and assurance of the processes for the management of information assets.

3.4. Senior Information Risk Owner (Director of Finance and IM&T)

The SIRO will be responsible for leading and fostering a culture that values, protects and uses information for the success of GMMH and the benefit of all its customers. This will include:

- ensuring GMMH has a plan to achieve and monitor the right NHS IG culture, across the Organisation and with its business partners;
- taking visible steps to support and participate in that plan (including completing own training);
- maintaining sufficient knowledge and experience of GMMH's business goals with particular emphasis on the use of and dependency upon internal and external information risk;
- ensuring GMMH has Information Asset Owners (IAOs) who understand their roles and are supported by the information Assets management specialists that they need;
- initiating and overseeing an information risk awareness / training programme of work to communicate importance and maintain impetus;
- ensuring that good information governance assurance practice is shared within GMMH and to learn from good practice developed and practiced within other NHS organisations locally and nationally.

- The SIRO will undertake strategic information assets management training.
- The SIRO will be directly accountable to the Board and will own the development and maintenance of information assets management policies, procedures and standards, act as an advocate for information assets on the board and in internal discussions, and provide written advice to the Chief Executive on the content of the Statement of Internal Control (SIC) relating to information Assets.
- The SIRO will nominate information asset owners to be ascribed to Information assets. The IAOs will usually be the senior individuals involved with running the relevant business unit, department and/or system.
- The SIRO will ensure that a line of communication is established with GMMH's Chief Executive to brief, discuss and/or report upon matters on information asset assurance and information asset culture affecting GMMH, including input to the annual NHS IG reporting processes, (Data Security and Protection Toolkit).
- The SIRO will sign off an annual assessment of performance, including material from the IAOs and specialists, covering NHS Data Security and Protection reporting requirements.

3.5. Data Protection Officer (DPO)

A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). The data protection officer is responsible for overseeing data protection and Information Governance strategy and implementation to ensure compliance with GDPR requirements. The DPO will 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 all data subjects including information asset management.

3.6. Information Governance Manager

The Information Governance Manager will act in support of the SIRO. The Information Governance Manager is responsible for the on-going development and day-to-day management of the Trust's Asset Management Programme for information privacy and security. This will include:

- acting as the focal point for information asset management in GMMH including resolution of any pan-organisation or other escalated asset issues raised by Information Asset Owners, Auditors, etc.;
- developing and implementing an IG Information Asset Management Policy that is appropriate to all departments of GMMH and their uses of information setting out how compliance will be monitored;
- initiating and overseeing a comprehensive programme of work that identifies, prioritises and addresses IG (including information asset) and system

accreditation for all parts of GMMH, with particular regard to information systems that process personal data;

- ensuring that Privacy Impact Assessments are carried out on all new projects/system when required in accordance with the guidance provided by the Information Commissioner;
- ensuring all risks of key information asset of GMMH are assessed monthly in line with the Trust's Risk Management Strategy via the Risk Assurance Statement to ensure that mitigation plans are robust;
- ensuring that the information asset management methods and standards are documented, applied and maintained consistently throughout GMMH
- ensuring that information asset assessment is completed on an annual basis taking account of NHS Information Governance guidance;
- understanding the information assets risks faced by GMMH and its business partners, ensuring that they are addressed, and that they include investment decisions including outsourcing;
- ensuring that information asset assessment and mitigating actions taken benefit from an adequate level of independent scrutiny by outside bodies when required, i.e. the Information Commissioner and Auditors.

The Information Governance Manager will ensure routine meetings are established with the SIRO and/or the Deputy SIRO, (Head of IM&T Service Delivery), to brief, discuss or report upon matters on information asset assurance and information asset culture affecting GMMH, including input to the annual NHS Data Security and Protection toolkit.

The Information Governance Manager will ensure that GMMH has implemented an effective information incident management and response capability that supports the sharing of lessons learned and integrates with the existing GMMH asset management framework managed by the Information Governance Team.

The Information Governance Manager will ensure that IG incidents are part of the Trusts incident response and communications plan, including the reporting of 'perceived' or 'actual' Information Governance Serious Untoward Incidents, (IG SUIs). This will be captured by the Trust's Datix system in line with the Trust's Incident, Accident and Near Miss Policy

The Information Governance Manager will ensure that GMMH's management, investigation and reporting of IG SUIs conforms to national guidance and Trust policies and procedures for non-IG SUIs, (e.g. clinical incidents).

The Information Governance Manager will advise the SIRO on the appointing of information asset owners in relation to the assets they 'own'.

3.7. Information Asset Managers (IAO)

IAOs are directly accountable to the SIRO and Information Governance Steering Group and must provide assurance that information assets are being managed effectively in respect of the information risks that they are responsible for.

IAOs are responsible for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers. This will include:

- understanding GMMH's plans to achieve and monitor the right IG culture, across Trust and with its business partners;
- taking visible steps to support and participate in that plan, (including completing own training);
- ensuring that staff understand the importance of effective information governance and receive appropriate education and training;
- considering whether better use of any information held is possible, within applicable information governance rules, or where information is no longer required.

IAOs are responsible for knowing what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset. This will include:

- maintaining an understanding of 'owned' assets and how they are used;
- approving and minimise information transfers while achieving business purposes;
- approving arrangements where it is necessary for information to be put onto portable or removable media such as laptops and USB pens and ensure information is effectively protected to NHS information governance standards and comply with Trust policies;
- approving the information disposal mechanisms for the asset in line with Trust Policy;
- ensuring that all new data (information) flows are recorded on spreadsheets and risk assessed via Datix when a new flow is established/identified,
- ensuring data (information) flow mapping exercise is carried out for all assets at least annually, and that such data maps are provided to the Information Governance Manager and IG Steering Group when required.

IAOs are responsible for knowing who has access to the asset and why, whether it be system or information to ensure access is monitored and compliant with policy.

This will include:

- understanding GMMH's policies on the use of information and the management of information assets;
- ensuring decisions on access to information assets are taken in accordance with NHS information governance good practice and the policies of GMMH;
- ensuring that access provided to an asset is the minimum necessary to satisfy business objectives;
- ensuring that the use of the asset is checked regularly and that use remains in line with policy;
- ensuring that all new assets are subject to a Privacy Impact Assessment (PIA) (where appropriate), recorded on the Information Asset Register and risk assessed via Datix when a new asset is acquired/identified;
- ensuring that an Information asset register is maintained and made available to the Information Governance Manager and IG Steering Group whenever requested.

IAOs are responsible for understanding and addressing risks to the asset, and providing assurance to the SIRO. This will include:

- seeking advice from information governance subject matter experts when reviewing information assets;
- conducting Data Protection Impact Assessments for all new projects that meet the criteria specified by the Information Commissioner; this is a legal requirement under GDPR;
- undertaking quarterly asset assessment reviews for all 'owned' information assets in accordance with NHS Information Governance guidance and report to the Information Governance Manager, ensuring that information assets are identified, documented and addressed, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks;
- escalating risks to the Information Governance Manager and/or SIRO where appropriate and to make the case where necessary for new investment to secure 'owned' assets;
- providing an annual written assessment to the Information Governance Manager for all assets 'owned' by them, following guidance from the Information Governance Manager on assessment method, format, content, and frequency.

IAOs will ensure the confidentiality, integrity, and availability of all information that their system creates, receives, maintains, or transmits and take action to mitigate against any reasonably anticipated threats or hazards to the security or integrity of such information. IAOs may nominate Information Asset Assistants

3.8. Information Asset Assistants

IAAs are directly accountable to the IAO of the asset and must provide assurance that information assets are being managed effectively in respect of the information asset that they 'administer'.

IAAs will:

- ensure that policies and procedures are followed in respect of information governance and information asset management;
- recognise actual or potential security incidents and consult their IAO on incident management;
- ensure the confidentiality, integrity, and availability of all information that their asset creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- ensure Information Asset Registers are accurate and up to date;
- ensure the Data Flow Mapping information is accurate and up to date;
- support the completion of the Data Security and Protection toolkit and any such associated work

3.9. All Staff

Managing assets and complying with this policy is the responsibility of all staff.

Each department/team in GMMH has responsibility for identifying, assessing, controlling and managing assets within their department and for communicating assets management and other relevant policies and procedures to their staff.

4. Information Asset Management Process

4.1. Protection of Assets

GMMH will be particularly careful to protect all data the release or loss of which could cause:

- harm or distress to patients or staff;
- damage of GMMH's reputation;
- financial loss or exposure to GMMH;
- major breakdown in information systems, information security or information integrity;
- significant incidents of regulatory non-compliance.

4.2. Information Asset Register

GMMH will establish and maintain a corporate Information Asset Register by Directorate. This register will:

- be kept by each directorate, which is then drawn together into one 'corporate' register. There is no intention of replicating information already on other asset registers, so references can be made where appropriate to other key registers; e.g. Staff list and skill sets held within ESR, IT asset register of equipment etc;
- be maintained by IAOs and IAAs using the existing 'Guidance Notes for the Completion of Information Asset Templates' (these will be supplied to IAO by the Information Governance Manager);
- be managed by the Information Governance Manager, who will:
    - define the asset register format and methodology, which will be based on the HSCIC guidance and example asset register;
    - ensure that all IAOs regularly update their asset registers;
    - ensure the corporate asset register mirrors all individual directorate asset registers.

4.3. Information Risk Assessments

Risk assessments will be performed for all the Trust's information assets and systems including critical information assets.

Information risk assessments will:

- be carried out by IAOs for their information assets and the availability, confidentiality and integrity of information in their possession and the IAOs will plan and implement appropriate mitigation action where a risk has been identified;
- be carried out using the information risk assessment forms on the Datix risk management system;
- be recorded on Directorate risk registers via Datix in line with the Trust's Risk Management Strategy;
- be reviewed bi-monthly via the Risk Strategy Group and when any new information asset is identified.

Information risk assessments will occur at the following times:

- annually, (managed by the Information Governance Manager), for the SIRO to support the SIRO's written advice on the Statement of Internal Control to the Chief Executive;

- at the inception/acquisition of new systems, applications, facilities, information flow etc., that may impact the assurance of GMMH Information or Information Systems; where appropriate this risk assessment may be in the form of a PIA;
- before enhancements, upgrades, and conversions associated with critical systems or applications; Where appropriate this assessment maybe made in the form of a PIA;
- whenever NHS policy or legislation requires Asset determination;
- whenever the GMMH management team or board require it.

Information risk assessments must take the risks and possible controls listed in Appendix 1 into consideration.

4.4. Information Risk Management Strategy Group

Information risks form part of the Trust's Risk Management Strategy Group which occurs bi-monthly. All current risks scored over 12 and all closed risks, key action points and any new risks are brought to this meeting for review. For further information on risks please refer to the Risk Management Strategy.

4.5. Data Flow Mapping

GMMH will undertake a bi-annual data, (information), flow mapping exercise and from this exercise determine the information risk regarding its information flows within the organisation and or with it partners. This exercise will be:

- managed by the Information Governance Manager;
- undertaken by the IAO's;
- reported to the IGSG.

4.6. Incident Reporting

Staff should compete incident reporting as soon as possible via Datix, in line with the Trust's Incident, Accident and Near Miss Policy. See the policy for detailed requirements, processes.

The key points from the Incident Reporting and Investigation procedure are summarised below:

- all incidents must be reported immediately by the member of staff involved, using DATIX, which must be checked, graded and signed off by their line manager before being input via DATIX WEB or sent to the Risk Management Team within 24 hours for recording in the DATIX system;
- the DPO and IG Manager will ensure that external bodies are notified in accordance with their individual requirements;

- all incidents will be investigated to an extent commensurate with their potential severity; (please refer to the Incident, Accident and Near Miss policy);
- as a minimum, the line manager should consider whether appropriate action has been taken, whether any lessons can be learned from identification of root or contributory causes, and whether any further action is necessary. This should be recorded on DATIX;
- for more serious incidents (level 4 and 5) , a 3 day review and Root Cause Analysis must be carried out and shared with the IG team;

All suspected or actual breaches which are a level 4 or 5 must be reported to the IG team immediately by telephone: the Trust has a legal responsibility to report all data breaches that are likely to impact the data subject to the ICO within 72 hours.

4.7. Incident Categories

Please refer to the Trust's Incident, Accident and Near Miss policy for incident categories and levels.

- All reported incidents will be notified via the Datix notification process to the Information Governance Manager, and the Information Quality Assurance Manager for investigation.
- If person identifiable data is involved, the impact of the loss will be assessed and where appropriate reported to the SIRO and Data Protection Officer. If necessary, based on its severity, the incident will be escalated and reported to the Information Commissioners Office.

4.8. Data Protection Impact Assessments (DPIA)

It is a legal requirement under GDPR that 'Data Protection by design' is established; this means that all Data Protection requirements are to be considered prior to implementation of any new system/service. As such, it is a legal requirement that a Data Protection Impact Assessment (DPIA) is conducted for all new projects and for any changes to existing systems/processes, (for example new systems, new services, change in how the service is run, change in how information is collected and/or recorded, a request to share information, a request to send a questionnaire to patients, etc.), within an IAO's area of responsibility.

- This will be undertaken in accordance with guidance available on the Information Governance intranet (this guidance is in line with the Information Commissioner's Office Guidance).
- Using the DPIA pro-forma and guidance documents available from the Information Governance team.
- Approval for DPIA's in the first instance will be from the Information Governance Manager and the appropriate IAO. Where a risk that is deemed 'high' or 'unmitigated' this will be escalated to the SIRO and DPO for consultation and review. Where a risk continues to be high the DPO will

review for reporting to the ICO*.

*This will occur if the Information Governance Manager feels there is still a risk to the organisation or data subjects that has not been mitigated or taken in to consideration during the DPIA process.

Please refer to the Trust's DPIA guidance and procedure (see also Appendix 2) which can be found on the Information Governance intranet pages and policy pages. Where possible the Trust will publish completed and approved DPIAs where there is not a risk to the organisation to do so.

4.9. Third Party Contractual Obligations

GMMH will use the data handling clauses from the Office of Government Commerce's model ICT contract for services, as its generic IG model for contracts with third parties.

4.10. Privacy Notices

Under GDPR all services/department must have a privacy notice published which informs data subjects of the reason their data is being processed, the legal basis for processing, and to inform data subjects of their rights. It is recommended that the Privacy notice be completed using the information from the DPIA.

5. Training Requirements

Please refer to the Trust Mandatory Training Matrix for full details.

The SIRO, IAO's and IAA's must undertaken and pass strategic Information Risk training annually. Training requirements will be communicated via the Information Governance Manager.

The Information Governance Manager shall provide ad hoc training and awareness session to the SIRO, IAO and IAA's when required or requested to ensure all roles can be carried out effectively.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
Information risk reports	Quarterly	Minutes	Minutes	Information Governance Manager	IGSG
Review of Information Asset Register and Data Flow Mapping	Annually	Minutes	Minutes	SIRO and IAOS	IGSG

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
Review of all incidents	Ad-hoc	Datix	Datix	IAO's	IGSG and Risk management
Dara Security and Protection Toolkit	Annually	Report	Assessment	CEO, SIRO, IAOs	IGSG and Trust Board
SIRO report to Board on Information Risks	Annually	Minutes	Minutes	SIRO	Trust Board
SIRO annual report	Annually	Minutes	Minutes	SIRO	Trust Board

7. Resource/Implementation Issues

None identified.

8. Risk Issues

All risks to be assessed locally and on an individual basis as outlined within the body of this document.

9. Requirements, Supporting Documents and References

9.1. Requirements

Board Objectives	2 – to work with service users & carers to achieve their goals; 4 – to invest in our environments; & 6 – to achieve sustainable financial strength & be well-governed.
CQC Regulations	CQC Quality & Risk Profile (QRP)
Other requirements	• Data Security and Protection Toolkit • General Data Protection Regulation • Data Protection Act 2018

9.2. Supporting Documents

- Information Governance Policy
- Induction and Mandatory Training Policy (Including Organisation Wide TNA)
- Information Security Policy
- Data Security and Protection Toolkit
- Mobile Media Policy
- Disciplinary Policy

- Subject Access Policy
- Incident, Accident and Near Miss Policy
- Risk Management Strategy
- NHS Information Risk Framework

10. Subject Expert and Feedback

Deborah Tonkin – Information Governance Manager

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.

Appendix 1 – Examples of Risks for Information Assets

Examples of Risks for Information Assets

1. **Information Asset not available:**
   a) Theft of information
   b) Loss of information
   c) Information corrupted/unreadable/virus
   d) Information incorrectly disposed
   e) System/network failure Backup of information not in place
   f) Information unusable – contaminated, e.g. water, smoke, fire, asbestos dust
   g) Wilful damage by employee/public

2. **Information accessed by unauthorised person**
   a) Passwords shared
   b) No password protection
   c) Mobile media not encrypted
   d) Information disclosed by accident
   e) Physical security not in place, e.g. Locks on doors, cabinets, drawers
   f) Eavesdropping
   g) Information available on a public drive/shared drive
   h) Insecure disposal of information
   i) System misused/hacked
   j) Contractors, temps, students not authorised users

3. **Other risks**
   a) Information used for other purposes than originally collected, no consent given. (secondary uses of personal information)
   b) Information out of date
   c) Information kept longer than retention period
   d) No licence for software therefore using illegally, may have illegally downloaded

e) Loss of expertise for a specific information asset if only one member of staff trained in use for example

f) Procedures not in place for use of information asset

g) Staff not trained in use of Information Asset, include contractors, temps students etc.

h) Booking out system not in place for paper documentation/files/records

i) Uncontrolled copying of information

j) Version control not in place

k) Duplicated information

Examples of Controls that may Reduce Risk

1. Relevant policies are in place and are being followed e.g. security policy, safe haven, mobile media.
2. Confidentiality and other IG policies such as Email and Internet Policy are read and understood by staff.
3. Job descriptions include Information Security and IG responsibilities where necessary e.g. for IG Manager, SIRO, Information Asset Owners.
4. HR screening undertaken as per HR policy in particular where access to sensitive data is required.
5. Staff are made aware of the confidentiality/IG clause in their contract of employment.
6. Procedures and protocols in place and being followed by staff who are regularly trained.
7. Ensure all staff undertake annual IG Training.
8. Ensure security weaknesses and software malfunctions reported.
9. Ensure actions taken following reported incidents to learn from mistakes made.
10. Undertake regular risk assessments of buildings/areas where information is held to ensure area is secure including key management for access to building.
11. Clear desk policy for personal/confidential information.
12. Ensure workstations locked/turned off by user when not in use. Laptops must be removed from desk/docking station by user at end of working day and locked away securely.
13. Password protected screensaver should be in use by all staff.

14. Prohibit working in public areas if possible, assign secure working areas that cannot be accessed by public if possible to prevent tampering with equipment or viewing of information.
15. Site workstations/laptops where they cannot be overlooked by unauthorised personnel. Obtain privacy screens if necessary.
16. Equipment taken off site – ensure staff aware of procedures in Mobile Media Security Policy to ensure laptops etc. are kept secure at all times and not left in cars/unattended for example.
17. All mobile media must be encrypted as per Mobile Media Security Policy.
18. Ensure confidential waste, IT equipment, fax rolls and records are destroyed in accordance with Trust Policy (e.g. Records Management Policy and the Mobile Media Security Policy)
19. Business Continuity plans in place and tested to protect information assets.
20. Data Protection Impact Assessments completed for new/changed processes/systems where information may be used in a different way than was originally collected for.
21. Ensure information sharing agreements in place where information needs to be shared with other organisations.
22. Specialist Security Information Advice provided by IG Team.
23. Third party assurances obtained regarding information security e.g. completion of DS&P Toolkit, clause in contracts.
24. Up to date Inventory of information assets. An inventory is a detailed list of what information is held. E.g. a filing cabinet may hold ‘Payroll Records’ as reported on the Information Asset Register, the inventory will list the actual record held in the filing cabinet.
25. Correct classification and marking of information as to whether it is personal, sensitive, corporate or confidential etc. So it is clear to users what type of information is held.
26. Information should be held on network drives, no personal information should be ‘stored’ indefinitely on mobile media such as pen drives, cd’s, laptop hard drives (these can be used for transfer of information only)
27. Secure backups and audit trails in place for system.
28. Keep track of who has access to restricted drives. Users should be deleted when they leave or transfer to another department
29. Exit strategies for staff leaving, suspended or made redundant to ensure access to systems prohibited, IT equipment and keys handed back to manager.

Appendix 2 – Data protection by Design