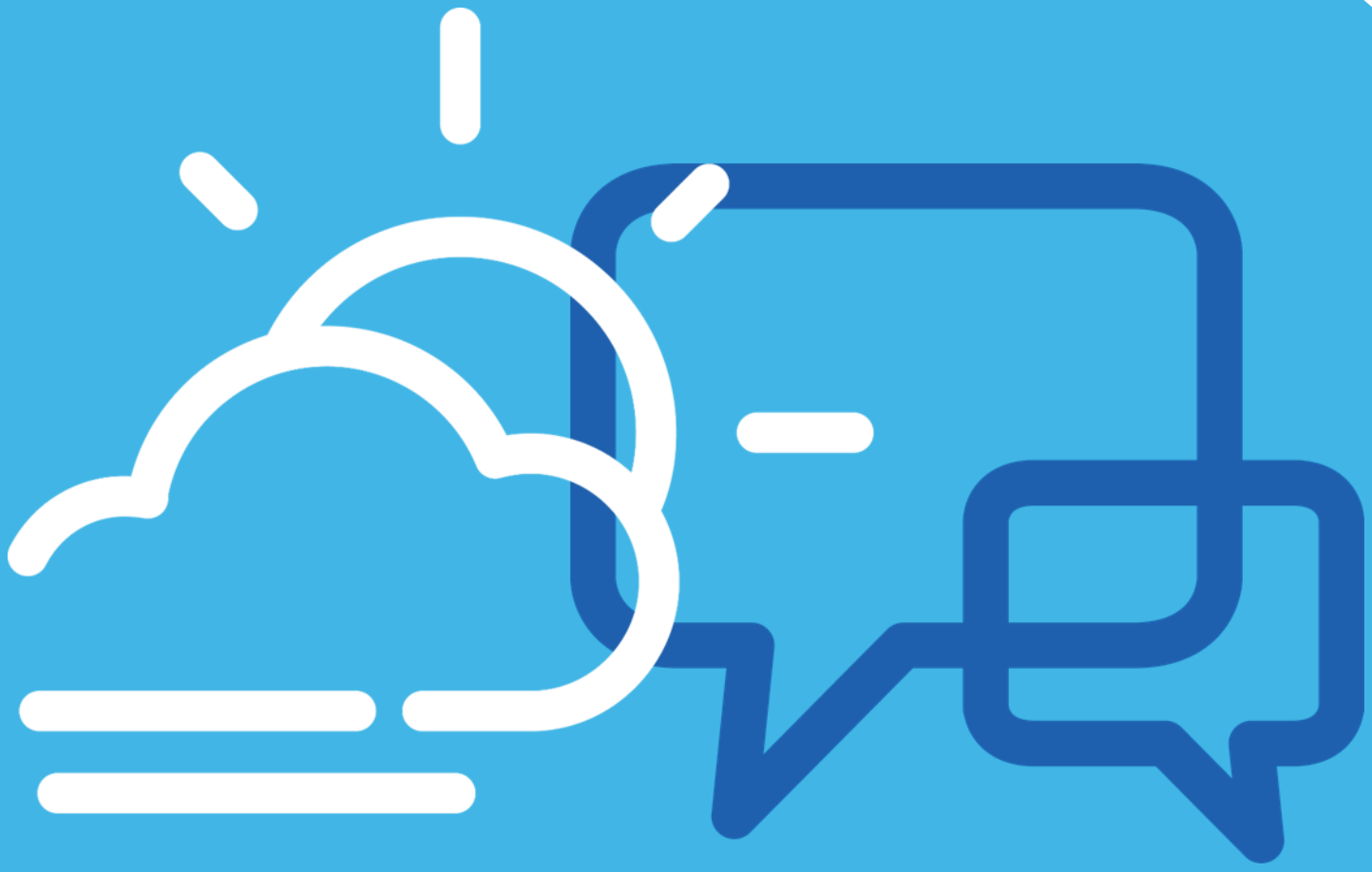
NHS
Greater Manchester Mental Health
NHS Foundation Trust

Information Security Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	Information Security Policy
Executive Summary:	To ensure that Trust information assets are protected to a high standard in line with all necessary legal frameworks and appropriate NHS policies and procedures, against potentially damaging threats.
Executive Lead:	Director of Finance, Capital and IM&T
Document Author:	Deborah Tonkin, Information Governance Manager
Document Purpose:	Policy
Target Audience:	All staff, contractors and third parties
Additional Circulation List:	All employees via the Trust Intranet
Date Ratified:	15/01/19
Ratified by:	Information Governance Steering Group
Consultation:	Representatives from all directorates via membership of the IGSG.
Cross Reference:	Related trust policies including the Information Governance Policy (IG006) and the Incident, Accident and Near Miss Policy and Procedure Information Security Management Code of Practice for NHS organisations and the Data Security and Protection Toolkit.
Superseded Docs	Information Security Policy IG08 V1.0
Date of Equality Impact Assessment:	02/07/2017
Board Objective Reference:	Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes Objective 3 – To engage in effective partnership working Objective 6 – To achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Care Quality Commission objectives:- • Consistency of advice • Clear service standards • Clarity of roles / relationships • Feedback mechanisms • Website and online services • Joined up communication • Internal communications
Risk Register Reference:	N/A
Contact Details for further information	Deborah Tonkin, (Information Governance Manager) deborah.tonkin@gmmh.nhs.uk Tel: 0161 3581573
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 top level Information Security Policy is a key component of the Trust's overall Information Security Management System and should be considered alongside more detailed information security documentation and controls including policies, protocols, practices, procedures, organisational structures and technical measures. These controls need to be established and continually reviewed to ensure that the specific security objectives of the organisation are met.

1.1. Purpose

The purpose of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks used by Greater Manchester Mental Health NHS Foundation Trust. This policy takes into account the NHS Information Governance aims and expectations set out within the Information Security Management Code of Practice for NHS organisations and the Information Governance Data Security and Protection standards.

Information is an asset and like any other important business asset, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments.

1.2. Scope

This policy applies to all those having access to information such as staff employed by the Trust to those engaged in duties for the Trust under a Letter of Authority, Honorary Contract or Work Experience, volunteers and any other third parties such as contractors, students or visitors. This document will be available on the Trust's website and intranet.

2. Definitions

Information Security is defined as the preservation of:

- **Confidentiality**: ensuring information is accessible only to those authorised to have access;
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods;
- **Availability**: ensuring that only authorised users have access to information and associated assets when required**.**

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

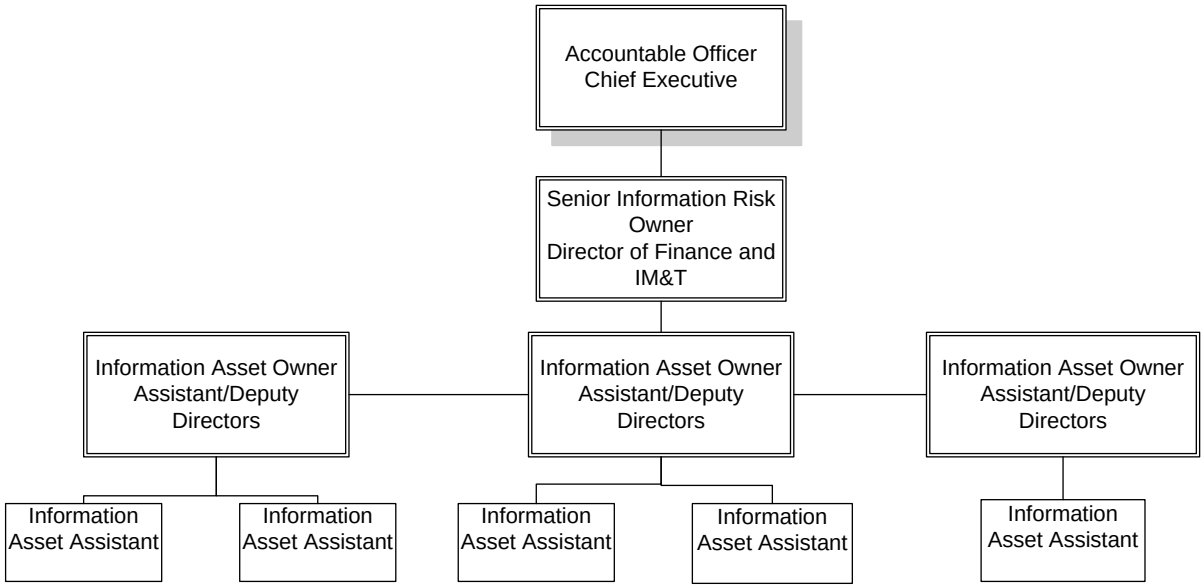
collected and processed, and places a range of new obligations on organisations to be more accountable for data protection.

Data Protection Act 2018
The Data Protection Act 2018 supersedes the Data Protection Act 1998.

3. Duties

3.1. Accountability Hierarchy

Information Security Accountability Hierarchy



3.2. Board/Lead Committee

At board level, responsibility for information security shall reside with the Director of Finance, Information Management and Technology.

3.3. Chief Executive

The Chief Executive is ultimately responsible for all Information Security and associated risks.

3.4. Senior Information Risk Owner

At Greater Manchester Mental Health NHS Foundation Trust the Director of Finance and Information Management & Technology is the Senior Information Risk Owner (SIRO).

In fulfilling this role they will:

- Act as an advocate for Information Security and Information Risks on the Board and to the Chief Executive.
- Own the Information Asset Policy and Risk Assessments.

- Take ownership of and ensure that there is an Information Asset Policy in place and will have responsibility for the risk assessment process of information risks.
- Provide written advice to the CEO on the content the Statement of Internal Control in regards to information risk.
- Lead cultural change to ensure that staff value, protect and use information for the public benefit.

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 security.

3.6. Information Asset Owner

Are accountable to the SIRO and responsible for ensuring information is managed in accordance with the law and trust policies.

- They will provide assurance to the SIRO that information risks are being managed effectively for those information assets that they have been assigned ownership.
- The IAO is responsible for completing, reviewing and monitoring the Information Asset Register and Data Flow Mapping Register within their directorate.
- Each Information Asset Owner will be responsible for the maintenance of all information assets within their directorate.
- Each IAO shall appoint an Information Asset Assistant(s) to assist them.

3.7. Information Asset Assistant

The Information Asset Assistant(s) will be designated by the IAO; it is recommended that these are Heads of Service or Administration Managers. They will assist the Information Asset Owner and have day to day responsibility for the management and accurate recording of information risks associated with information assets.

3.8. Information Governance Manager

The Trust's Information Governance Manager will be responsible for implementing, monitoring, documenting and communicating information security requirements to the Trust.

3.9. Managers

Managers are responsible for ensuring that all permanent, temporary and contract members of staff are aware of:

- The Information Security Policy and associated policies.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

3.10. Staff

Staff and users of information assets must ensure that they have read, understood and comply with the Trust's relevant policies and procedures. Each member of staff shall be responsible for the operational security of the information asset they use.

Each asset user shall comply with the security requirements that are currently in force and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity.

Failure to do so may result in disciplinary action from the Trust and a financial penalty being imposed by the Information Commissioners Office.

3.11. Contractors and Third Parties

Before any contractual agreements which allows a 3rd party access to the Trust's information assets have been finalised, a Data Protection Impact Assessment must be completed and authorised by the Information Governance Manager.

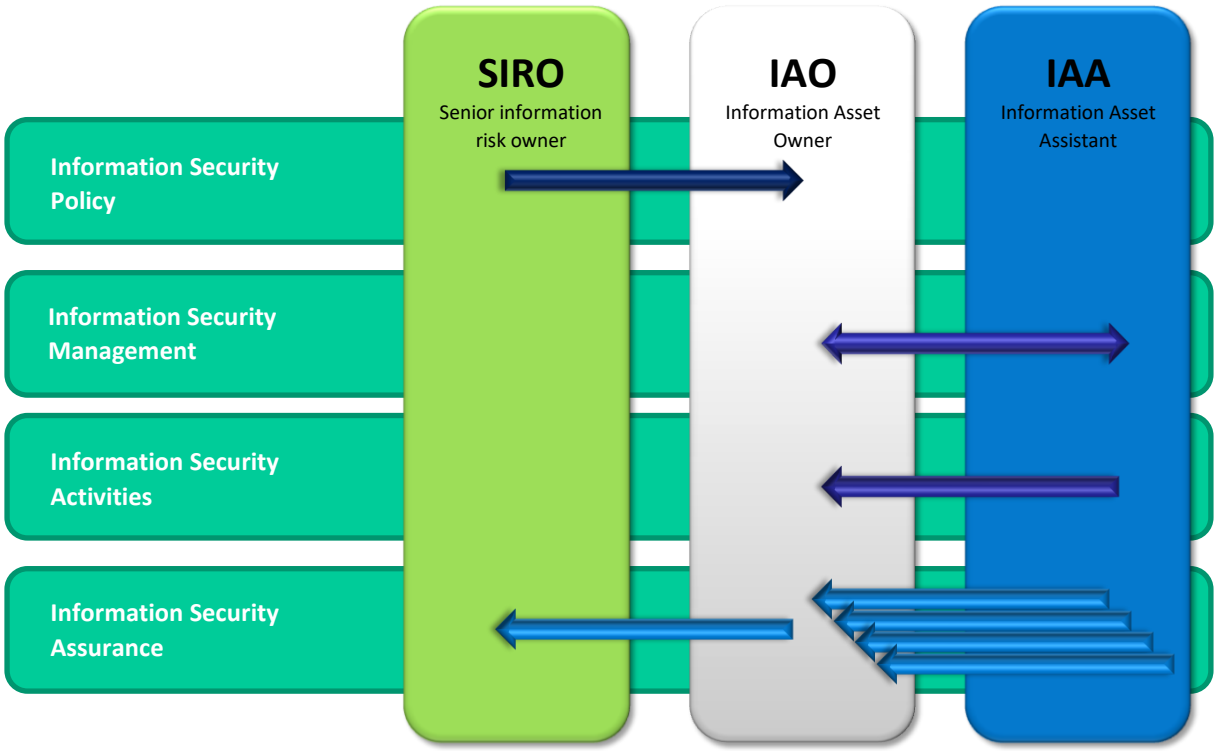
Contractors or 3rd parties who do not have direct access to the Trust's Information Assets, e.g. Grounds Maintenance Workers, must sign a Confidentiality Agreement. All Confidentiality Agreements must be approved by the Information Governance Manager as fit for purpose before contractors are asked to sign them.

Contracts with external contractors that allow access to the organisation's information assets shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies and that the 3rd parties have an up to date approved Data Security and Protection Toolkit which is maintained annually and, where appropriate, an up to date Data Protection Certificate.

Where access to the Trust's Information Asset for third parties is required, an Information Sharing Agreement must be in place and staff must have completed the required Information Governance training before access is granted or any information is shared. Please refer to the Trust's Information Sharing Protocol for further information.

4. Processes and Procedures

4.1. Information Security Assurance Flow diagram



4.2. Information Security Assurance Flow diagram

This policy aims to establish and maintain the confidentiality, integrity and availability of information assets by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Protect information assets under the control of the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Create and maintain within the organisation a level of awareness of the need for Information Security as an integral part of day to day business.

4.3. Management of Information Security

At board level the responsibility for Information Security shall reside with the Senior Information Risk Owner, (Director of Finance & IM&T).

Information Asset Owners shall support the SIRO and are responsible for managing

risks for the information assets which they have been assigned ownership and reporting associated risks via the Trust's risk management procedure, (please refer to the Incident, Accident and Near Miss policy) to the SIRO so there is a clear understanding of all information risks.

Day to day management of information assets shall reside with the Information Asset Assistant.

The Trust's Information Governance Manager shall be responsible for implementing, monitoring, documenting and communicating information security requirements for the organisation.

4.4. Information Security Awareness Training

Please see GMMH Training needs analysis, (Education Commissioning Document) for details of the types of training required by staff group by location and the competencies required.

Managers are encouraged to identify suitable training modules for staff to complete via the online Training via the Learning Hub. Training may be recommended following an incident or where a training need is identified.

4.5. Contracts of Employment

Staff security requirements such as Disclosure and Barring Service check or extra references etc. shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

It is a requirement for all new employees to the Trust to read and understand the Code of Confidentiality before commencing in post. Please refer to the Code of Confidentiality Policy.

Information security expectations of staff shall be included within appropriate job descriptions.

4.6. Security Control of Assets

Each individual assigned with an information asset, (hardware, software, application or data), shall be responsible for the information security of that asset. All information assets will be owned by the relevant Information Asset Owner.

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data. The sharing of passwords to gain access to information, systems or computer devices is strictly forbidden and any such breach could lead to disciplinary proceedings or prosecution.

4.7. User Access Controls

Access to information shall be restricted to authorised users who have a legitimate

business need and a justified reason to access the information.

4.8. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have a business need to use the facilities.

4.9. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need, e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

4.10. Equipment Security

In order to minimise loss of or damage all assets and equipment shall be physically protected from threats and environmental hazard.

4.11. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Trust's IM&T Operational Group.

4.12. Environmental Controls

All staff are required to ensure that information held by the Trust is protected from any and all threats as far as is possible. Where confidential information/data is evident staff have a responsibility to:

- Keep doors and windows locked at all times.
- Limit the number of staff with knowledge of keypad numbers, sharing only where necessary and changing numbers regularly and whenever there is a perceived risk.
- Never allow anyone else to access their ID badge, which provides access to Net2 locked areas within the Trust.
- Ensure that information held on the ground floor cannot be observed via any internally or externally facing windows.
- Ensure that written documentation is stored securely in locked cupboards etc. when not in actual use.
- Always adhere to the trust guidance on clear desk working practices – as outlined in the staff Information Governance handbook.

4.13. Information Risk Assessment

All information assets shall be risk assessed by the IAO annually as a minimum or when there is a significant change to the asset or process the asset undertakes. The

risk assessments shall be recorded on Datix. The outcome of the risk assessments will be collated by the Information Governance Manager and presented at the IGSG. The Senior Information Risk Owner who will communicate any risks to the Board.

Information Security risks need to be identified and quantified in terms of the assets' perceived value, the severity of impact and the likelihood of occurrence. Once identified, information security risks shall be managed on a formal basis in accordance with the Trust's Risk Management Strategy.

They shall be recorded within the departmental risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed and a standing feature of the Trust's risk management programme.

These reviews shall help identify areas of continuing best practice and possible weakness as well as potential risks that may have arisen since the last review was completed.

4.14. Information Security and Cyber Security Events and Weaknesses

All information security and cyber security events and suspected weaknesses are to be reported to the appropriate manager via the Datix incident reporting system in accordance with the Trust's Incident, Accident and Near Miss Policy. The Information Governance Manager must be informed of all IG events, the Head of ICT must be informed of all cyber security events. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

4.15. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Information Governance Manager. Users breaching this requirement may be subject to disciplinary action.

4.16. User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Information Governance Manager or Head of ICT before they may be used on the Trust's systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action. Examples of removable media include items such as USB hard drives, SIM cards, Digital Camera cards, portable hard disks; this is not an exhaustive list and if in doubt must be approved by the Information Governance Manager or Head of ICT. Please see Mobile Media Policy.

4.17. Monitoring System Access and Use

An audit trail of system access and data used by staff shall be maintained and reviewed on a regular basis. The Trust has in place routines to regularly audit compliance with this and other policies. All Trust systems will have a System Level Security Policy in place.

In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy.

The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications including telephone communications, emails and internet usage for the following reasons:

- establishing the existence of facts;
- investigating or detecting unauthorised use of the system;
- preventing or detecting crime;
- ascertaining or demonstrating standards which are achieved or thought to be achieved by persons using the system (quality control and training);
- in the interests of national security;
- ascertaining compliance with regulatory or self-regulatory practices or Trust procedures or polices;
- ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

Misuses of Trust systems and/or unauthorised access could result in a criminal record.

Any misuse of the trusts systems will be regarded as gross misconduct and dealt with under the appropriate HR policies. It will be reported to the ICO and may attract a personal fine and/or criminal prosecution.

4.18. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks are approved by the Head of ICT and/or Information Governance Manager before they commence operation. Where possible, role based access will be implemented in this way so specific responsibilities may be assigned and obligations communicated directly to those who use the system.

4.19. Data Protection Impact Assessment

It is a **legal** requirement under GDPR to complete a DPIA prior to the introduction of any new software, systems or services. Any high risks identified must be reported to the ICO by the DPO who will advise what action should be taken.

All new or significantly changed processes or projects that involve Person Identifiable Data that are planned to be introduced must comply with confidentiality, privacy, data protection, GDPR and information security requirements.

A Data Protection Impact Assessment (DPIA) must be completed by the Project Lead/Service Manager prior to commencing any new projects, processes or systems or when there is a planned change to a project, system or process which involves Personal Identifiable Data. The DPIA shall be updated to reflect all the changes throughout the project implementation.

DPIAs should be reviewed by the appropriate Project Board or Project Lead. The Information Governance Manager and the DPO will approve all DPIA's and keep a register of completed and approved DPIA's.

The Information Governance Manager will provide a report to the Information Governance Steering Group about all new DPIA's.

Please refer to the Trust's DPIA guidance on the intranet for further information about when and how to complete a DPIA along with the Trust's DPIA pro-forma.

The DPIA is designed to assess all possible data security risks and rights to individuals prior to a project/system or database being introduced.

4.20. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Trust's Head of ICT via the DPIA process.

4.21. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Head of ICT. Users shall not install or arrange to have any software installed on the organisation's property without the express permission from the Head of ICT and/or Information Governance Manager. Users breaching this requirement may be subject to disciplinary action.

4.22. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that a business impact analysis, business continuity and disaster recovery plans are produced for critical information, applications, systems and networks within its direct control. All third parties shall ensure they have their own Business Continuity and Disaster Recovery Plans in place to minimise the impact of such events. It is the responsibility of the IAO to ensure local business continuity plans are in place and tested regularly.

4.23. Reporting

The Information Governance Manager shall keep the SIRO informed of the information security status of the organisation by means of regular reports and presentations at the IG Steering Group.

The SIRO will also be made aware of all information risks via the Trust's Risk Management Strategy and escalation process.

5. Training Requirements

Please see GMMH Training needs analysis for details of type of training required by staff group by location and the competencies required.

The online Information Governance Training via the learning hub provides modules to assist managers and staff to be trained in relevant issues.

The Information Governance Manager will provide ad hoc training where the need has been highlighted from a 3 day review or reportable incident.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
The trusts practices for Data security and handling of personal information will be monitored	Annual	Self-assessment using the NHS Digital Data Security & Protection (DS&P) Toolkit	DS&P Toolkit submission & GDPR	IG Manager	IGSG

7. Resource/Implementation Issues

It is the responsibility for all line managers to ensure that all staff under their immediate control, temporary or otherwise complies with this policy.

8. Risk Issues

N/A

9. Requirements, Supporting Documents and References

9.1. Requirements

This Policy has been written to meet the requirements of:

- The General Data Protection Regulation Link
- The Data Protection (Processing of Sensitive Personal Data) Order 2000 Link
- The Computer Misuse Act 1990 Link
- The Access to Health Records Act 1990 Link
- The Human Rights Act 1998 Link
- The Access to Medical Reports Act 1988 Link
- The Data Protection Act 2018 Link
- The Copyright, Designs and Patents Act 1988 Link
- The Electronic Commerce (EC Directive) Regulations 2002 Link
- The Electronic Communications Act 2000 Link
- The Environmental Information Regulations (EIR) 2004 Link

- The Freedom of Information (FOI) Act 2000 Link
- The National Health Service Act 2006 Link
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 Link
- The Public Interest Disclosure Act 1998 Link
- The Regulation of Investigatory Powers Act 2000 Link
- The Department of Health Data Security and Protection Toolkit
- Sir David Nicholson's letter to NHS CEO's
- Other obligations placed on NHS CEO's

9.2. Supporting Documents

- Information Governance Policy
- Information Asset Management Policy
- Mobile Media Policy
- Data Protection Impact Assessment Guidance
- Incident, Accident and Near Miss Policy
- Risk Management Strategy
- Information Sharing Protocol

10. Subject Expert and Feedback

Advice and support queries in relation to this document should be sent 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.