NHS
Greater Manchester Shared Services

GMSS Information Security Policy

Review Date: November 2021

Document Control

Title / Reference:	Information Security Policy
Status:	Approved
Version:	V1.3
Date Issued / Ratified:	February 2020
Originator of Document and Job Role:	IG Team
File Classification:	Official Data
Retention:	Life of the organisation plus 6 years (place of deposit)
Target Audience:	All GMSS staff & 3rd party partners
Links to other strategies, policies, procedures etc:	• Data Security, Protection & Confidentiality Policy • Data Security, Protection & Confidentiality Framework • Confidentiality Audit Procedure • Data Security Breach & Incident Reporting Policy • Secure Transfer of Data Policy • Acceptable Use of IT / Information Systems Policy • Information Classification Policy • Records Management Policy • Risk Management Policy • Information Risk Policy • Subject Access Request Policy • Registration Authority (Smart Card) Procedure • Data Security, Protection & Confidentiality Staff Handbook **This list is not exhaustive**

Change History

Summary of Changes	Name	Date	Version
Reviewed from Oldham CCG to fit with GMSS	IG Team	Nov 16	0.1
Recommend approval by the IG Group	IG Team	Nov 16	0.1
Recommend approval after some amendments	FPG	Jan 17	0.1
Amendments needed	SMT	Jan 17	0.1
Amendments made to accommodate GDPR	IG Team	Aug 17	1.2
Reviewed slight amendments	IG Team	Nov 19	1.3
Formatting amendments for consistency	Gov Comm	Jan 20	1.3

Review

Name	Role	Date	Version
IG Group	IG Group	Nov 19	1.3
Governance Committee	Governance Committee	Jan 20	1.3
Senior Management Team	Senior Management Team	Feb 20	1.3

Approval

Name	Role	Date	Version
IG Group	IG Group	Nov 19	1.3
Governance Committee	Governance Committee	Jan 20	1.3
Senior Management Team	Senior Management Team	Feb 20	1.3

Distribution

Name	Role	Date	Version
Saved in policy folder		Nov 19	1.3
Updated policy tracker		Nov 19	1.3
GMSS Publication scheme		Mar 20	1.3
The Bulletin		Mar 20	1.3
People Matters		Mar 20	1.3

DOCUMENT STATUS:
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled

Contents

1. Assurance Statement

This policy sets out a framework of governance and accountability for Information Security management across the Greater Manchester Shared Services (GMSS). The policy along with the Information Security Management Code aims to provide and develop a positive culture of information security throughout GMSS by maintaining:

- **Confidentiality:** protecting information from unauthorised access and disclosure.
- **Integrity:** safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion.
- **Availability**: ensuring that information and associated services are available to authorised users whenever and wherever required.

2. Introduction

The Information held and managed by the Greater Manchester Shared Services is an asset that all staff have a duty and responsibility to protect. The availability of complete and accurate information is essential to GMSS functioning in an efficient manner.

The aims and objectives of GMSS Information Security Policy is to set out a framework for the protection of the organisation's information and information assets to:

- Protect against threats, whether internal or external, deliberate or accidental;
- Enable information sharing in a secure and consistent manner;
- Encourage consistent and secure use of information;
- Ensure all users of GMSS information systems have an understanding of their roles and responsibilities in the protection and use of information;
- Ensure the continuity of IT Services and minimise disruption to business operations;
- Ensure the GMSS meets its legal and fiduciary responsibilities. Including those defined by the GDPR and DPA.

The GMSS Information Security Policy is a high-level document that utilises a number of controls to protect the organisations information. The controls are delivered through policies, standards, processes, procedures, supported by tools and user training.

Corporate Information Security Policy

- Policy – sets the scope, guiding principles, and security management system for information processing, storage and protection

Standard

- Define the acceptance criteria for information security, for example, Security Management, through ISO 27001, COBIT;
- Technical, through the application of security hardening configuration requirements

Processes and procedures

- Processes – describe methods to store and process information in a way that conforms to the standards in accordance with the policies of the organisation.
- Procedures – provide systematic instructions that implement the processes.

Training and tools

- Tools – systems needed to implement or support the procedures.
- Training – knowledge and skills to use a procedure, understand responsibilities and information protection requirements.

3. Aims & Objectives

This policy applies to those members of staff that are directly employed by GMSS and for whom the GMSS has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience, the organisation’s policies are also applicable whilst undertaking duties for or on behalf of GMSS. Further, this policy applies to all third parties and others authorised to undertake work on behalf of GMSS.

The GMSS Information Security Policy, standards, procedures and processes applies to all forms of information, including but not limited to:

- Verbal communication by telephone and social media;
- Information (printed or written);
- Information stored in manual filing systems;
- Communications, including those sent by post, courier, electronic mail, text messaging and Bluetooth;
- Information that is stored in and/or processed by information systems including servers, personal computers (PCs), laptops, mobile phones, tablet devices, personal digital assistant (PDA) and any other mobile device that is allowed access to GMSS information systems and information;
- Transmission of or passing information to third parties or others that are external to GMSS.

4. Definition of Terms

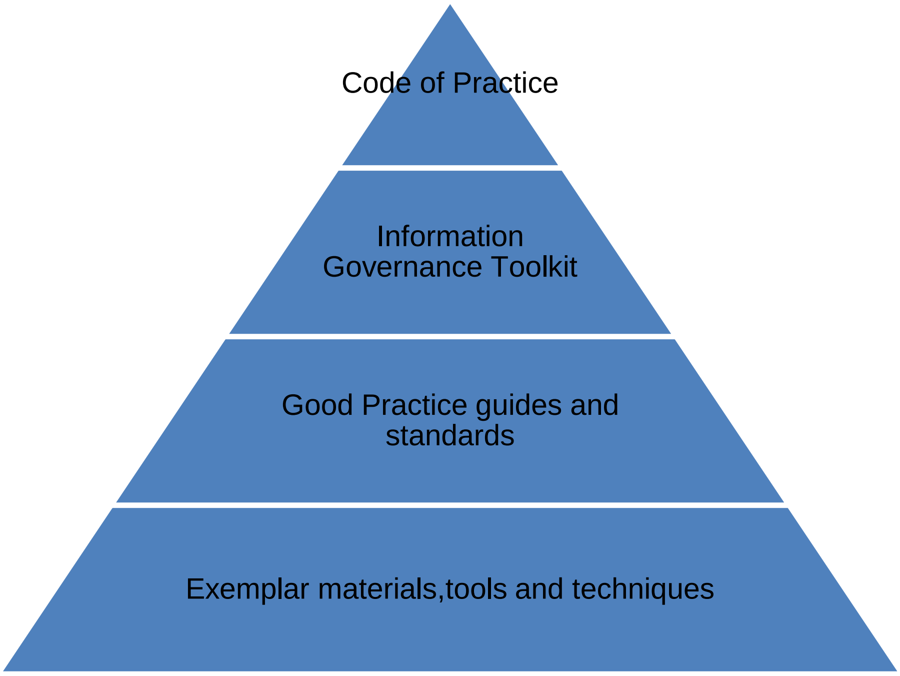
Information Security Management

The 'Information Security Management: NHS Code of Practice is a guide to the methods and required standards of practice in the management of information security, for those who work within or under contract to, or in business partnership with NHS organisations in England.

It is based on current legal requirements, relevant standards and professional best practice.

This Code of Practice replaces HSG 1996/15 – NHS Information Management and Technology Security Manual, and provides a key component of Information Governance arrangements for the NHS.

It is part of an evolving information security management framework because risk factors, standards and practice covered by the Code will change over time. The guidelines contained within the Code of Practice apply to NHS information assets of all types.


Code of Practice
Information Governance Toolkit
Good Practice guides and standards
Exemplar materials,tools and techniques

Confidentiality

The 'Confidentiality: NHS Code of Practice' sets out the required standards of practice concerning confidentiality and patients' consent to use their health records.

It is a guide for those who work within or under contract to NHS organisations and is based on legal requirements and best practice.

5. Duties and Responsibilities

Managing Director

The Managing Director has overall responsibility for Data Security & Protection within GMSS. As Accountable Officer, they are responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Governance provides a framework to ensure information is used appropriately and is held securely.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible for identifying and managing the information risks to GMSS. This includes oversight of the organisation's information security / governance incident reporting and response arrangements and the Registration Authority business process.

The SIRO for the organisation of the Chief Finance Officer

Data Protection Officer (DPO)

The DPO role is required as part of the General Data Protection Regulation.

The DPO's role is to inform and advise GMSS and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to:

- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities;
- Advise on data protection impact assessments;
- Train staff and;
- Conduct internal audits.

In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

The DPO for the organisation is the IG Manager.

Senior Managers

Senior Managers are responsible for the security of their physical environments where information is processed or stored. Furthermore, they are specifically responsible for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and use obligations applicable to their area of work;
- Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security;
- Determining the level of access to be granted to specific individuals;
- Ensuring staff have appropriate training for the systems they are using;
- Ensuring staff know how to access advice on information security matters.

Information Governance Team

The GMSS Information Governance Team are responsible for supporting the organisation and staff to ensure information is processed legally, securely, efficiently and effectively. Providing guidance to staff around the use and process of personal data of information contained within GMSS information assets in line with data protection and information security legislations and regulations.

Head of Corporate IT & IT Security Manager

The Head of Corporate IT and IT Security Manager are responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure GMSS systems and infrastructure remain compliant with the Data Protection Act 2018.

The Head of Corporate IT and IT Security Manager is responsible for ensuring that all GMSS electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

Information Asset Owners

All Information Asset Owners are responsible for ensuring that third party data processors have appropriate ISO and/ or Cyber Essentials accreditation where appropriate for assets stored electronically with third parties. Information Asset Owners are also responsible for ensuring appropriate data protection assurance from all third party suppliers processing GMSS data.

All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should undertake their mandatory annual Data Security Awareness training and understand:

- What information they are using, how it should be protectively handled, stored and transferred;
- What procedures, standards and protocols exist for the sharing of information with others;
- How to report a suspected beach of information security within the organisation;
- Their responsibility for raising any information security concerns with the Head of IT, IT Security Manager or the IG Team.

Contracts with external contractors that allow access to the organisation’s information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

6. Main Policy

Policy Framework

The Information Security Policy document sets out GMSS approach to managing Information Security.

The Information Security Policy is approved by the IG Group, Governance Committee then SMT and is communicated to all staff, constituent businesses, contractual third parties, partners, suppliers, agents and others who will have access to GMSS information and information systems.

The Information Security Policy will be reviewed in line with the suite of IG policies and IT policies. Changes or amendments will be made and approved accordingly.

Contracts of Employment

Responsibilities for compliance to keep information secure will be included in terms and conditions of employment.

Where appropriate, background checks will be carried out on new employees. These background checks will be relative to the level and classification of information employees will access within the GMSS.

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.

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

Security – Protection

It is a statement of management intent that the policy of the GMSS will be to ensure that information will be protected from a loss of:

- Confidentiality - ensuring that information is accessible only to those that are authorised;
- Integrity - safeguarding the accuracy and completeness of information;
- Availability - ensuring that authorised users have access to relevant information when required and in a timely manner.

Security – Requirements

GMSS is implementing technical and operational standards, policies and processes that align with prevailing standards in line with ISO27001 (Information Security Management).

The requirements of policy, processes and procedures will be incorporated into the GMSS operational procedures and contractual agreements.

Information stored and processed by GMSS will be appropriate to business requirements and no information will be stored or processed unnecessarily as laid out in the General Data Protection Regulations (GDPR)

Business continuity plans will be developed, implemented, maintained and tested and such plans will be a contractual obligation of any relevant supplier.

All breaches of information security, actual or suspected will be reported and suitably investigated in line with information incident management procedures which will provide guidance on what constitutes an information incident.

Training and education regarding information security will be given to staff, contractors and third parties as well as any others who will have access to GMSS information and information systems. Training may be provided in different formats as appropriate.

Coordination of Information Security

The security of information will be achieved through assigning information security roles and co-ordinating the implementation of this policy across GMSS, constituent businesses and third parties

Where required, government approved external specialist advice will be drawn on to address new and emerging threats and standards.

Asset Management

All GMSS assets, for example, people, information (electronic and hardcopy), software, computer and communication equipment and service utilities, will be accounted for and have an owner.

GMSS will implement controls that will ensure its assets are appropriately protected.

Owners of such assets will be responsible for the maintenance and protection of assets they are assigned.

Physical and Environmental Security

Controls will be put in place to ensure restricted information will be physically protected from unauthorised access, damage, interference and/or alteration.

Communications and Operations Management

Responsibilities will be assigned and policies, processes and procedures for the management, operation and on-going security and availability of all data and information processing facilities will be implemented.

To reduce the risk of inadvertent, negligent or deliberate misuse of GMSS information systems, separation of duties or responsibilities, will be implemented.

Appropriate controls will be applied to all types of communication, internal and external, to ensure only information required to be communicated is, the communication is secure and reaches the intended recipient.

Access Control

Access to GMSS information systems and GMSS information will be controlled, with access driven by business requirements.

Staff will be granted access to GMSS information systems and GMSS information based on their role and to a level that will enable them to carry out their job responsibilities.

A formal and documented user provisioning process will be implemented which will govern access to GMSS information systems and GMSS information.

Information Systems Acquisition, Development and Maintenance

Information security requirements will be defined and communicated during the development of business requirements for new systems or changes to existing systems.

Failure of the GMSS, constituent businesses to engage with IT, to define these requirements, will result in rejection of new systems or changes to existing systems.

Controls to mitigate risks identified during design, procurement development, testing and deployment will be implemented.

Information Security Incident Management

GMSS has a formal incident reporting and escalation process.

All staff contractors and third parties will be made aware of procedures for reporting security incidents or vulnerabilities that may have an adverse impact on the security, integrity or availability of the GMSS information systems and GMSS information.

Information security incidents and vulnerabilities associated with information systems will be reported within an agreed timeframe and prescribed corrective action taken.

Information Risk Assessment

All information assets are identified and assigned an Information Asset Owner (IAO) and an Information Asset Administrator (IAA).

Information Assets along with Data Flows and associated Risks are reviewed at least twice a year. The IAOs and IAAs follow the guidance from the IG Team which is approved by the SIRO.

The SIRO is made aware of any risk assessments that are reported as high, where action is taken to reduce these risks as soon as possible. Following from these reviews a SIRO Report is produced detailing the reviews and highlighting any risks.

Please see the Information Risk Policy for further information.

Business Continuity Management

A business continuity management process is in place to minimise the impact of a disruption of service and to recover from the loss of information assets.

A business impact analysis has been conducted, by the business, to assist in defining appropriate controls against the consequences of disasters, security failures, loss of service and loss of service availability.

GMSS will ensure arrangements are in place to protect critical business process from the effects of major failures or disasters, of information systems or services, and to ensure timely resumption.

Compliance

GMSS will abide by any law, statute, regulatory and/or contractual obligations affecting its information and information systems.

The design, operation, maintenance, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.

All staff, contractors and third parties and all others that are, or have been, authorised to access are required to comply with the Information Security Policy and its supporting standards, policies, processes and procedures.

Failure to comply could result in disciplinary and/or legal action.

7. Training and Awareness

This policy will be made available to all staff via The Bulletin and published on GMSS Website and on People Matters for GMSS staff.

All staff are responsible for adhering to the General Data Protection Regulations 2016, Caldicott Principles, the National Data Guardian Data Security Standards, the Data Protection Act 2018 and the common law duty of confidentiality.

All staff are mandated to undertake Data Security Awareness training on an annual basis.

Staff will receive guidance regarding this policy from a number of sources:

- Policies and procedure located on People Matters;
- Line manager;
- Other communication methods (e.g. staff briefings, team meetings, IG updates).
- The IG Team and/or IT Security Manager.

8. Classification of Information

GMSS implement appropriate information classifications controls, based upon the data security legislation.

Further details of the classifications controls can be found in the Information Classification Policy and the Records Management Policy.

9. Legislation & Guidelines

A set of procedural documents will be made available via People Matters.

- General Data Protection Regulations 2016
- Data Protection Act 2018
- The National Data Guardian Data Security Standards
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidence
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000
- Guide to the Notification of Data Security and Protection Incidents.

10. Equality Statement

GMSS aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the GMSS legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief.

The Equality Analysis has been completed and any associated policies and procedures will be analysed accordingly.

11. Monitoring and Review

This policy will be monitored through staff awareness and supporting evidence to the Data Security & Protection Toolkit.

This policy will be reviewed on a two yearly basis and in accordance with the following as and when required:

- Legislative changes;
- Good practice guidance;
- Case law;
- Significant incidents reported;
- New vulnerabilities; and
- Changes to organisational infrastructure.

The next review is scheduled for November 2021.