Greater Manchester Shared Services

Information Security Policy

Greater Manchester Shared Services
Hosted by NHS Oldham CCG
on behalf of the Greater Manchester CCGs

Best Care • Best Health • Best Value

Document Change History

Date	Ver.	Status	Author	Details of Change
November 2016	0.1	Reviewed from Oldham CCG to fit GMSS	IG Team	Amendments to fit with GMSS

Document Tracking History

Date	Ver.	Person Presenting	Area Receiving	Comments
November 2016	0.1	IG Team	GMSS IG Group	Recommend Approval by the IG Group
January 2017	0.1	G Coxon	FPG	Recommend Approval after some amendments
January 2017	0.1	K Rigden	SMT	Amendments needed
February 2017	1.0	K Rigden	SMT	Approved

Contents

1. **Assurance Statement....4**
2. **Introduction 4**
3. **Aims & Objectives....5**
4. **Definition of Terms....6**
5. **Duties and Responsibilities....7**
6. **Main Policy....7**
7. **Other Policies and Procedures 10**
8. **Monitoring Arrangements....11**

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.

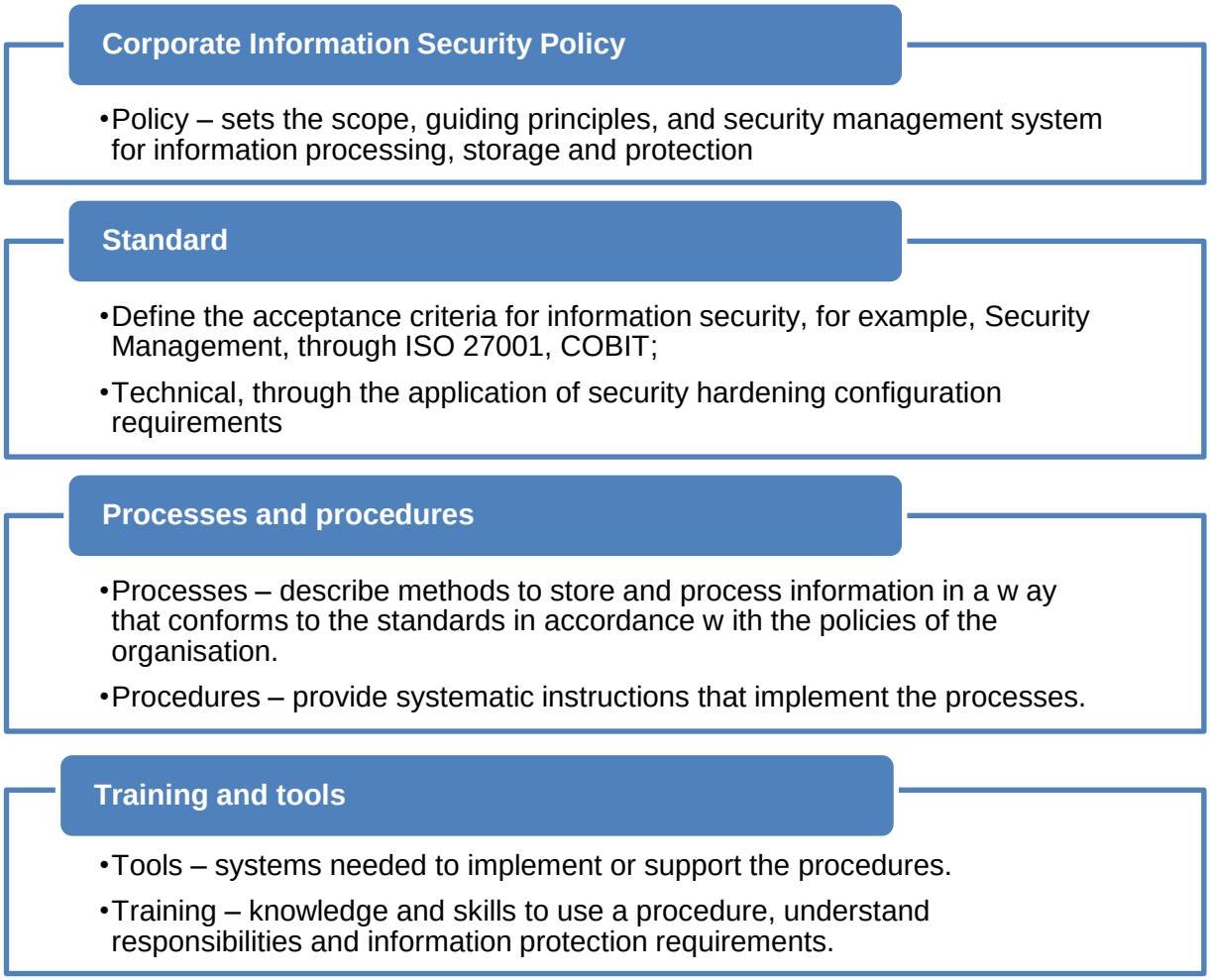
2. Introduction

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 the GMSS functioning in an efficient manner.

The aims and objectives of the 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 a 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.

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.



3. Aims & Objectives

This policy applies to those members of staff that are directly employed by the 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 the GMSS. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the 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 the GMSS information systems and information

- transmission of or passing information to third parties or others that are external to the GMSS.

4. Definition of Terms

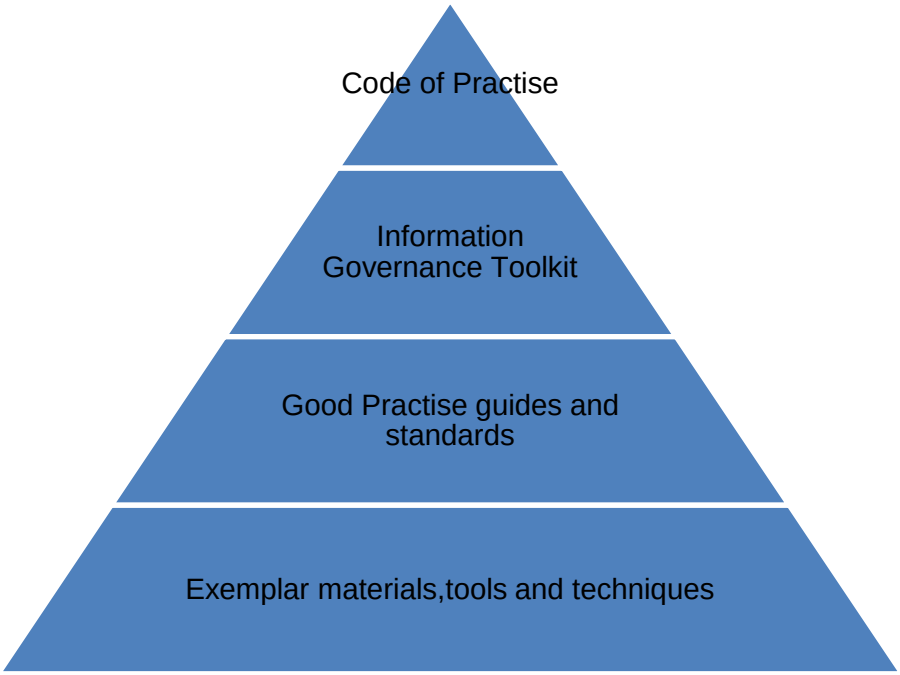
Information Security Management

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.



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

Overall accountability for procedural documents across the organisation lies with the Chief Operating Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

Overall responsibility for the Information Security Policy lies with the GMSS Information Security Manager or equivalent who has delegated responsibility for managing the development and implementation of technical and operational procedural documents to IT Services and Line Managers.

Staff will receive training regarding the policy from a number sources

- Policy and Strategy Manuals
- line manager
- specific training course
- other communication method (e.g. team briefing and intranet)
- Information Governance Toolkit training

6. Main Policy

Risks

The GMSS will undertake risk assessments to identify, quantify and prioritise information security risks. Controls will be selected and implemented to mitigate the risks identified.

Risk assessments will be undertaken using the Governance Risk Assessment methodology to identify and estimate the magnitude of risks and in accordance with the GMSS Information Risk Policy.

Information Security Policy

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

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

The Information Security Policy will be reviewed, at least annually, and approved by the GMSS Integrated Governance Committee. Changes or amendments will be made and approved accordingly.

Information 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

Information security – Requirements

The GMSS will implement technical and operational standards, policies and processes that align with prevailing standards such as 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 the GMSS will be appropriate to business requirements and no information will be stored or processed unnecessarily.

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.

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 the 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.

Information security responsibilities

The Information Security Manager or equivalent, is the designated owner of the Information Security Policy, responsible for the maintenance and update, ensuring timely review and approval and ensuring supporting policies, standards, processes and procedures are in place.

The GMSS auditors will attest to the adequacy and effectiveness of controls to protect the GMSS information and make recommendations where deficiencies are found.

Heads of departments and line managers are responsible for ensuring all staff, contracted third parties (whether individual or an entity) are made aware of and comply with the Information Security Policy including supporting policies, standards, processes and procedures.

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.

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

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

Human resource security

Responsibilities for compliance to information security will be included in job descriptions and 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.

Suppliers will be responsible for conducting appropriate background checks on contractors and third parties who will have access to the GMSS information and information systems.

Physical and environmental security

Restricted information will be physically protected from unauthorised access, damage, interference and/or alteration.

Information processing facilities will be housed in secure areas. These areas must be protected by defined and approved security perimeters with appropriate security barriers and entry controls.

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 the 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 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

The GMSS will develop and implement 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.

IT service community management

A business continuity management process will be implemented to minimise the impact of a disruption of service and to recover from the loss of information assets.

A business impact analysis will be 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.

The 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

The 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. Other Policies and Procedures

The GMSS shall maintain policies and procedures for the effective management of all records. Other policies and relevant procedures that affect this policy but not limited to are:

- Information Governance Strategy & Policy

- Data Protection & Confidentiality Policy
- Record Management Policy
- Business Continuity Plan
- Business Continuity Policy

Other relevant practises are:

- 'Confidentiality : NHS Code of Practice'
- 'Information Security Management: NHS Code of Practice'
- 'Records Management: NHS Code of Practice'

8. Monitoring Arrangements

Performance against Key Performance Indicators will be reviewed on an annual basis and used to inform the development of future procedural documents.

This policy will be reviewed at least on an annual basis and in accordance with the following as and when required:

- Legislative changes
- good practice guidance
- case law
- significant incidents reported
- new vulnerabilities changes to organisational changes.

Equality Analysis

The 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 has identified impact or potential impact as "no impact.