NHS
Greater Manchester Shared Services

GMSS
Data Security & Protection Framework

Review Date: November 2020

Document Control

Title / Reference:	Data Security & Protection Framework (formerly IG Framework)
Status:	Final
Version:	V1.2
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
Split the IG Strategy & Policy into the IG Framework & IG Policy documents	IG Team	Sep 17	0.1
Reviewed in line with GDPR and staff changes	IG Team	Feb 19	1.1
Reviewed in line with GDPR and DSPT – annual review	IG Team	Nov 19	1.2
Formatting amendments for consistency	Gov Comm	Jan 20	1.2

Review

Name	Role	Date	Version
IG Group	IG Group	Nov 19	1.2
Governance Committee	Governance Committee	Jan 20	1.2
Senior Management Team	Senior Management Team	Feb 20	1.2

Approval

Name	Role	Date	Version
IG Group	IG Group	Nov 19	1.2
Governance Committee	Governance Committee	Jan 20	1.2
Senior Management Team	Senior Management Team	Feb 20	1.2

Distribution

Name	Role	Date	Version
Saved in policy folder		Nov 19	1.2
Updated policy tracker		Nov 19	1.2
GMSS Publication scheme		Apr 20	1.2
The Bulletin		Apr 20	1.2
People Matters		Apr 20	1.2

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. Introduction

The Data Security & Protection Framework (formerly Information Governance) document aims to capture GMSS's approach to Data Security & Protection (DS&P).

Robust DS&P requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that GMSS will deliver this is documented within this Data Security & Protection Framework. This will be reviewed annually by GMSS SMT or by GMSS IG Group.

The Data Security & Protection Framework must be read in conjunction with other GMSS Data Security & Protection Documents.

The framework provides a summary / overview of how GMSS is addressing the Data Security & Protection agenda and adapted appropriately to the capacity and capability of the organisation.

There are many different standards and legislation that apply to DS&P and information handling, including, but not limited to:

General Data Protection Regulation (GDPR)	Health and Social Care Act 2012	Freedom of Information Act 2000
Common Law Duty of Confidentiality	Confidentiality: NHS Code of Practice	Human Rights Act 1998
International Information Security standard: ISO/IEC 27002: 2005	Access to Health Records Act 1990	Information Security NHS Code of Practice
Caldicott Guidance	Computer Misuse Act 1990	Mental Capacity Act 2005
Public Records Act 1958	Records Management Code of Practice for Health and Social Care 2016	Data Protection Act 2018

DS&P is required to be adequately resourced with effective organisational and managerial structures and processes underpinned by documented policies and procedures, and regular and updated staff training

GMSS recognises the role Data Security & Protection plays in ensuring the organisation processes and handles its personal, sensitive and business information in accordance with UK laws and Department of Health Policy, thus protecting GMSS, its employees and most importantly, patients.

It is of paramount importance to ensure that information is efficiently and legally managed, and that the appropriate policies, procedures, guidance and management accountability and structures provide a robust governance framework for information management.

2. Strategic Aims

The aim of this Framework is to set out how GMSS will effectively manage DS&P. The organisation will achieve compliance by:

- Establishing, implementing and maintaining local GMSS policies for the effective management of DS&P;
- Establishing robust DS&P processes that conforms to Department of Health standards and comply with all relevant legislation;
- Ensuring information is provided accordingly to service users, stakeholders and shareholders about how information is recorded, handled, stored and shared and managed;
- Providing clear advice, guidance and training to all staff to ensure that they understand and apply the principles of DS&P to their working practice;
- Sustaining and DS&P culture through increasing awareness and promoting DS&P, thus minimising the risk of breaches of personal data;
- Assessing GMSS performance using the DS&P Toolkit and Internal Audits, developing and implementing action plans to ensure continued improvement.

3. Key Roles 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 Data Security & Protection 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.

Caldicott Guardian

The Caldicott Guardian is the conscience of the organisation and is responsible for ensuring that GMSS process satisfies the highest practical standards for handling patient and service user information. This includes ensuring any sharing of patient and service user data is justified and lawful.

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 Team.

Information Security Role

Provides the following Information Security support:

- Information Security (IS) qualifications as a qualified lead auditor for Information Security;
- Undertake or commission IS Audits of a key information asset process and generate a report for GMSS SIRO.

Information Governance Team

GMSS Data Security & Protection responsibilities will be supported by the GMSS Information Governance Team and will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Data Security & Protection.

All staff

All staff, whether permanent, temporary or contracted, working in a clinical or non-clinical environment are responsible for ensuring that they are aware of the Data Security & Protection requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All staff have a responsibility to ensure they complete the mandatory training requirements of the organisation, Data Security & Protection forms part of these mandatory training requirements.

4. Governance Framework

Responsibility and accountability for DS&P is cascaded through GMSS and is co-ordinated by GMSS Head of Policy and Corporate Operations & GMSS IG Team via the following:

- IG Group;
- Staff contracts of employment;
- Information Sharing Agreement / Data Processor Agreement;
- Data Protection Impact Assessment Pro forma;
- Information Asset Ownership – documented within the Information Asset Register;
- DS&P / IG Training (via Virtual College);
- DS&P / IG Training Needs Analysis;
- DS&P / IG Updates in GMSS staff bulletins;
- DS&P / IG Policies and Procedures.

5. Training and Guidance

Staff receive clear guidelines on expected working practices and the consequences of failing to follow policies and procedures via the methods as outlined above in the Governance Framework section.

Data Security & Protection training and the required software package for completion is outlined in the Training Needs Analysis.

All staff are mandated to undertake DS&P / IG training on an annual basis.

Where relevant further training and education will be required of staff, staff will be informed via the Data Security & Protection Training Needs Analysis.

All agency / temporary staff must have evidence of adequate Data Security & Protection training and / or undertake the mandatory DS&P training programme via Virtual College. This must be evidenced by managers.

GMSS Information Governance Staff are officially trained in Data Protection and Freedom of Information (ISEB qualification).

Training and advice is provided to staff on request and can be provided in other formats as appropriate.

6. Data Security & Protection Toolkit & Annual Performance

NHS Digital has developed standards of assertions and compliance is measured by the Data Security & Protection Toolkit (DSPT) formerly the Information Governance Toolkit. GMSS will complete this annual self-assessment tool. The assertions of the DSPT Toolkit cover all aspects of DS&P including:

- People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles;
- Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses;
- Technology: ensure technology is secure and up-to-date.

An assessment of compliance of Assertions, within the Data Security & Protection Toolkit will be undertaken each year. A proposed action/work programme will be maintained and annual assessments will be presented to SMT / Governance Committee / IG Group for approval.

7. Data Security & Protection (IG) Incident Management

GMSS IG Officers will score and classify IG / data security incidents in accordance with the NHS Digital "Guide to the Notification of Data Security and Protection Incidents" (May 2018).

Incidents will be assessed following the ‘Breach Assessment Grid’ which can be found in the above Guide.

Any breaches other than "green breaches" are reportable using the Data Security and Protection Toolkit.

Where an IG / data security incident / breach relates to a vulnerable group in society as defined in the guidance, the minimum score will be a 2 in either significance and likelihood unless incident contained.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, full details will automatically be reported to the Information Commissioners Office and the NHS Digital Data Security Centre.

The Department for Health and Social Care will also be notified where it is (at least) likely that harm has occurred and the impact is at least serious.

Incidents must be reported within 72 hours. This 72 hours starts when GMSS becomes aware of the breach which may not necessarily be when it occurred. Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

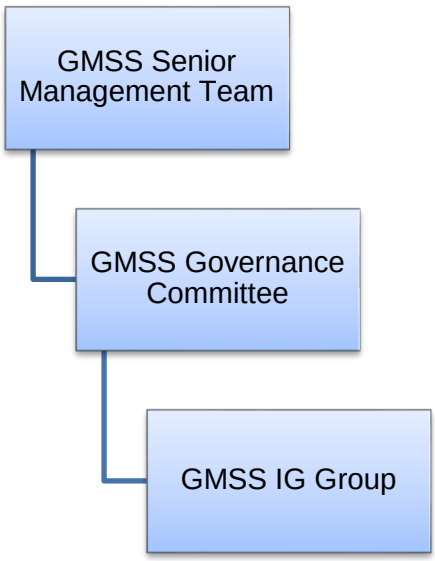
8. Reporting Structure

GMSS Information Governance Group chaired by the Caldicott Guardian, reports to GMSS Governance Committee who then report to GMSS Senior Management Team. The group focuses on the implementation and compliance of Data Security & Protection principles. The responsibilities of the group include, but are not limited to:

- Recommending for approval and adoption all related polices, protocols, strategies and procedures within the Data Security arena, having due regard to legislation and NHS requirements;
- Recommending for approval the annual submission of compliance with the requirements in the NHS Data Security & Protection Toolkit and related action plans;
- To co-ordinate and monitor the Data Security & Protection Policy across the organisation;
- Make recommendations on the necessary resourcing to support requirements;
- Deliver the implantation of GDPR & Data Protection Act 2018;
- To address all issues surrounding information management and information security issues that may affect GMSS;
- To identify and approve all necessary staff information and training as outlined in the NHS Data Security & Protection Toolkit;
- Ensure that risks are included on the corporate risk register;
- Scan the horizon for key emerging risks within the DS&P / IG environment.

GMSS will monitor and co-ordinate with service suppliers the implementation and on-going management of the Data Security & Protection / Data Security & Protection Framework and DS&P Toolkit requirements via the IG Group.

9. Information Governance Organisational Structure



10. Training and Awareness

This framework 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 framework 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.

11. 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.

12. 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.

13. Equality Statement

GMSS aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this framework 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.

14. Monitoring and Review

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

This framework 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 2020.