NHS
Greater Manchester Shared Services

GMSS Data Security, Protection and Confidentiality Policy

Review Date: November 2021

Document Control

Title / Reference:	Data Security, Protection & Confidentiality Policy (formerly IG Policy)
Status:	Approved
Version:	V3.0
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 Policy and IG Framework documents	IG Team	Sept 17	1.0
Updated	IG Team	Jan 18	2.0
Reviewed in line with GDPR, DPA 18 and DSPT guidance	IG Team	Nov 19	3.0
Formatting amendments for consistency	Governance Committee	Jan 20	3.0

Review

Name	Role	Date	Version
IG Team	IG Team	Nov 19	3.0
Governance Committee	Governance Committee	Jan 20	3.0
Senior Management Team	Senior Management Team	Feb 20	3.0

Approval

Name	Role	Date	Version
IG Group	IG Group	18/10/17	1.0
SMT	SMT	14/11/17	1.0
IG Group	IG Group	28/02/18	2.0
IG Group	IG Group	Nov 19	3.0
Governance Committee	Governance Committee	Jan 20	3.0
Senior Management Team	Senior Management Team	Feb 20	3.0

Distribution

Name	Role	Date	Version
Saved in policy folder		Oct 17	1.0
Updated policy tracker		Nov 17	1.0
Saved in policy folder		Feb 18	2.0
Saved in policy folder		Nov 19	3.0
GMSS Publication scheme		Mar 20	3.0
The Bulletin		Mar 20	3.0
People Matters		Mar 20	3.0

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 purpose of this policy is to provide guidance to all NHS Greater Manchester Shared Service (henceforth referred to as “GMSS”) employees on Data Protection.

GMSS has a statutory duty to safeguard the personal data, special category of data and other business confidential information it processes whatever format such as paper and electronic. The principle of this policy is to provide guidance regarding the legislation and key standards that GMSS and its staff and any other third party who works for or on behalf of GMSS must comply with to ensure data is confidential, available when needed and is of high integrity.

To support this policy the IG team has produced a portfolio of policies, guidance, bulletins and templates, to help staff comply with key legislation including the General Data Protection Regulation 2016 (henceforth referred to as GDPR) and the Data Protection Act 2018 (henceforth referred to as the DPA). Staff will also receive instruction and direction regarding this policy from a number of other sources including communications, team meetings and line management direction.

All staff working for or on behalf of GMSS are bound by a common law duty of confidentiality to protect personal data they process during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the DPA, GDPR and the National Data Guardian Data Security Standards and for healthcare and other professionals, via their own professional Codes of Conduct.

GMSS is committed to adhering to data protection legislation and national standards. This means ensuring that all personal and special category of personal data is processed fairly, lawfully, securely, efficiently and transparently so that the public can:

- Understand the reasons for processing personal and special category of personal data;
- Gain trust in the way GMSS processes data;
- Understand their information rights regarding the processing of their personal and / or special category of personal data.

This policy provides a guide to Data Security / Information Governance but advice should always be sought from your manager or the GMSS IG Team before disclosing data.

GMSS will continue to maintain and review policies, procedures and guidance to ensure compliance with data protection legislation, the Caldicott principles and the National Data Guardian Data Security Standards.

2. Purpose & Scope

This policy applies to those members of staff that are directly employed by GMSS and for whom GMSS has legal responsibility.

For those staff covered by a letter of authority / honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of GMSS.

Further, this policy also applies to all third parties and others authorised to undertake work on behalf of GMSS.

The purposes of this policy are:

- To ensure personal data processed adheres to confidentiality, availability and integrity;
- To provide guidance for all individuals working within the organisation;
- To ensure a consistent approach to data security and confidentiality across GMSS;
- To ensure all staff are aware of their responsibilities with regards to processing personal data.

This policy applies to all forms of information, including but not limited to:

- Paper and electronic filing systems;
- Communications, including those sent by post, electronic mail, text messaging;
- Information that is stored in and/or processed by information systems including servers, personal computers (PCs), any other mobile device;
- Information that is stored, copied, moved or transferred to any type of removable or portable transmission, both internal or externally to a third party.

All NHS bodies and those carrying out functions on behalf of the NHS have a duty of confidentiality to service users and a duty to support professional ethical standards of confidentiality.

Everyone working for the NHS has a personal duty of confidentiality to the service user and to his / her employer. The duty of confidentiality is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

3. Roles & Responsibilities

Managing Director

The Managing Director has ultimate responsibility for the implementation of the provisions of this policy. As the 'Managing Director" they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

GMSS has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

Responsibilities will be delegated to the:

Caldicott Guardian

The Caldicott Guardian's role:

- Ensures that GMSS satisfies the highest practical standards for handling patient identifiable information / confidential information;
- Acts as the conscience for GMSS;
- Facilitates and enables information sharing and provides advice on the options for lawful and ethical processing of information;
- Ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff;

- Oversees all arrangements, protocols and procedures where confidential patient data may be shared with external bodies both within, and outside, the NHS;
- Attends appropriate annual training to ensure they remain effective in their role and to ensure GMSS comply with assertion 3.4.1 of the Data Security & Protection Toolkit (NDG Data Security Standards).

Senior Information Risk Owner (SIRO)

The SIRO's role:

- Is an Executive Director or Senior Management Team Member;
- Takes overall ownership of the Organisations Information Risk Policy;
- 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;
- Advises the Senior Management Team on the effectiveness of information risk management and data security across GMSS;
- Attends suitable annual training to ensure they remain effective in their role and to ensure GMSS comply with assertion 3.4.1 of the Data Security & Protection Toolkit (NDG Data Security Standards).

Data Protection Officer (DPO)

The Data Protection Officer role:

- Informs and advises employees about their obligations to comply with GDPR, the Data Protection Act and other relevant legislation and monitors compliance with such legislation;
- Monitors compliance with data protection policies and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, the production of a Data Security / IG Framework document supported by relevant policies and procedures;
- Raises awareness of data protection issues with staff and at a senior level;
- Raises awareness and monitors compliance of data security training;
- Monitors compliance of audits;
- Provides advice and guidance on any GMSS Data Protection Impact Assessments (DPIA's) as per Article 38 of the GDPR;
- Maintains expert knowledge in data protection;
- Is the point of contact with the supervisory authorities, including the ICO, and any individual whose data is being processed;
- Attends suitable annual training to ensure they remain effective in their role and to ensure GMSS comply with assertion 3.3.1 of the Data Security & Protection Toolkit (NDG Data Security Standards).

The Data Protection Officer for GMSS is the IG Manager.

Information Asset Owners and Administrators (IAO / IAA's)

The Information Asset Owners and Administrators will:

- Lead and foster a culture that values, protects and uses information for the success of GMSS and benefit of its patient population;

- Know what information comprises or is associated with each asset, and understands the nature and justification of information flows to and from the asset;
- Know who has access to the asset, whether system of information, and why, and ensure access is monitored and compliant with policy;
- Understand and address risks to the asset, and provide assurance to the SIRO.

Information Governance Team

Data Security & Protection responsibilities lies with GMSS Information Governance Team who are accountable for ensuring effective management, accountability, compliance and assurance for all aspects of the Data Security & Protection Framework.

The Information Governance Team will:

- Monitor, co-ordinate and manage the Data Security & Protection Toolkit (DSPT) to ensure compliance with the DSPT (NDG Data Security Standards);
- Monitor GDPR Compliance within GMSS
- Deliver Data Security / Information Governance to GMSS;
- Maintain awareness of Data Security / Information Governance issues within GMSS;
- Review and update Data Security / Information Governance related policies / procedures / templates / guidance in line with local and national requirements

Line Managers

Line Managers will:

- Take responsibility for ensuring that the Data Security, Protection & Confidentiality Policy is communicated and implemented within their group or directorate, including any temporary or contract staff.

Employees

It is the responsibility of all employees (including any temporary or contract employee) covered by the scope of this policy, to adhere to and keep up to date with any changes to this policy.

Employees will receive instruction and direction regarding the policy from a number of sources:

- Policy / strategy and procedure manuals;
- Line Manager;
- Specific training course;
- Other communication methods, for example, team meetings, The Bulletin.

All employees (including any temporary or contract employee) must ensure that they read and follow the user requirements within the GMSS Data Security Handbook which supports GMSS Data Security / Information Governance policies.

All employees (including any temporary or contract employees) are mandated to undertake Data Security / IG Training as per the Data Security / IG Training Needs

Analysis. Training can be provided in other formats as appropriate.

Where relevant further training and education will be required of employees, the employee will be informed via the Data Security / IG Training Needs Analysis.

GMSS will monitor and co-ordinate the implementation and ongoing management of the Data Security / Information Governance framework and Data Security & Protection Toolkit requirements via the IG Group, GMSS Caldicott Guardian and the SIRO.

The IG Group will report to the GMSS Senior Management Team. This will be the route of escalation for issues.

Failure to comply with any part of this policy could result in disciplinary and / or legal action.

4. Definitions

Personal Data

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Information that identifies individuals is confidential, and should not be used unless absolutely necessary.

Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual should be used. It should be noted however that even anonymised information can only be used for justified purposes.

Special Categories of Personal Data

Article 9 of the GDPR refers to sensitive data as “special categories of personal data”. This data is sensitive so needs more protection. These special categories of data are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Health Data;
- Sexual life / sexual orientation;
- Genetic data;
- Biometric data.

Personal Confidential Data

Personal data including any health related information (including where health related information can be derived from context) or health related information in a context from which personal data can be identified, is personal confidential data. This term was introduced via the National Data Guardian Review of Data Security, Consent and Opts

Outs conducted in 2013.

Health Data

This means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Anonymous Data

This is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. GDPR does not apply to anonymised information and where ever possible anonymous data should be used.

Pseudonymisation

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Processing

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller

This means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor

This means a natural or legal person, public authority, agency or other body which processes personal data “on behalf of” the data controller.

Consent

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal Data Breach

This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

5. The General Data Protection Regulation 2016

The General Data Protection Regulation (along with the Data Protection Act 2018) governs how GMSS processes personal data.

Under GDPR, GMSS no longer has to register with the ICO but under the Data Protection (Charges and Information) Regulations 2018 it is a legal requirement for data controllers to pay the ICO a data protection fee. These fees will be used to fund the ICO's data protection work.

GMSS as a Data Controller must comply with the 7 key data protection principles as set out in Article 5 (1) e of the GDPR. These are:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

GMSS must be transparent regarding how personal data is processed. This is normally undertaken by the provision of a privacy notice. GMSS have a Staff Privacy Notice which is made available via People Matters and a Patients & Public Privacy Notice which is available via GMSS website. Both of these Privacy Notices outline GMSS's data processing activities.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a matter that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Only use personal data obtained by GMSS in connection with the business of GMSS and ensure information is not used for any purposes other than originally intended.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes of which they are processed*;*

Only obtain the minimum amount of personal data and do not obtain personal data which is not needed.

(*d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;*

Ensure that all personal data processed manually or electronically is accurate and up to date to ensure high quality data. Where personal data is provided from other sources ensure that there are appropriate procedures in place to continually review and update the different sources to ensure accuracy and version control. Where possible do not hold duplicate copies as this increases the risk of inaccurate data being held.

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interests, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

For further guidance regarding records retention, please see GMSS's Records Management Policy. When disposing of paper personal data, all staff **MUST** use the confidential waste destruction process. For the deletion / destruction of electronic data held on devices / equipment, please contact the IT provider.

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

GMSS and its IT provider have policies and processes in place to ensure the technical security of data. The IG Team has produced a variety of policies and procedures to inform staff regarding how to keep personal data secure and confidential. Please contact the IG Team for more information. Some tips to help to do this are:

- Do not allow unauthorised access to personal data;
- Do not share passwords with anyone;
- Do not leave confidential information on your desk or post trays and ensure all paperwork is tidied away when not in use or at the end of the day;
- Ensure that computer / laptop screens are locked when away from the desk;
- Hold confidential conversations in a private area.

Article 5 (2)

"The controller shall be responsible for, and be able to demonstrate compliance with, the other data protection principles"

GMSS evidences compliance with this with the following:

- Implements and maintains a suite of data security, protection policies / procedures and guidance;
- Adopts a 'data protection by design and default' approach;
- Ensures GDPR compliant contracts are in place with organisations that process personal data on behalf of GMSS;
- Maintains a Records Of Processing Activities (ROPA) – please see the Information Asset Register and / or the Data Flow Mapping Register for more information;
- Implements and maintains appropriate security measures;
- Records and, where necessary, reports personal data breaches to the Information Commissioner's Office (ICO);
- Carries out data protection impact assessments (DPIA's) for uses of personal data that are likely to result in high risk to individuals' interests;
- Has an appointed Data Protection Officer;
- Adheres to relevant codes of conduct and signing up to certification schemes where appropriate.

6. Rights of the Data Subject under GDPR

Individuals have strengthened rights under GDPR. In summary, these are them:

Right to be informed (Articles 13 & 14) – Individuals have the right to be informed about the processing of their personal data, this is explained via GMSS Patients & Public & Staff 'Privacy Notice/s.

Right of access (Article 15) – Individuals can request access to personal data we hold about them. The timeframe for responding and supplying the information is 1 calendar month. No fee can be charged (unless an exemption applies).

Right to rectification (Article 16) – Individuals can request that inaccurate personal data is rectified or completed if it is incomplete. The request can be verbal or in writing and GMSS have one calendar month to respond.

Right to erasure (Article 17) - Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Right to restriction of processing (Article 18) - Where accuracy is contested individuals have right to restrict processing. This is not an absolute right and only applies in certain circumstances. GMSS must respond to a request for restriction within one calendar month.

Notification Obligation regarding rectification or erasure of personal data or restriction of processing (Article 19) – GMSS (as data controller) must communicate rectification or erasure of personal data or restriction of processing to whom anyone whom the personal data has been disclosed (unless this is impossible or involves disproportionate effort).

Right to Data Portability (Article 20) - This right only applies where explicit consent is used as the legal basis for any processing.

Right to object (Article 21) – Individuals have the right to object to processing data. However, GMSS can demonstrate compelling legitimate grounds to continue processing then it can continue.

Right not to be subject to a decision based solely on automated processing including profiling (Article 22) - GMSS do not process data using this method, so this right will not apply to our data processing activities.

Right to withdraw consent (Article 7) – Where consent is used as the legal basis the right to refuse (or withdraw) consent applies to information sharing. However, this right might not apply if the sharing is for a mandatory or legal requirement imposed on GMSS.

Right to complain (Article 77) – If staff / patients feel that personal data processed at GMSS has not been handled correctly or are unhappy with a response to any requests made, a complaint can be made to the IG team (initially) and the if still unhappy the complaint can be lodged with the Information Commissioner's Office (ICO) https://ico.org.uk/

For further information about individual rights under GDPR, please see the Individual Rights Procedure.

7. The Data Protection Act 2018

The Data Protection Act 2018 (DPA) which sits alongside the General Data Protection Regulation (GDPR) plays a part in filling in the gaps that are not covered in the GDPR

and where the GDPR permits member states to make some adaptations to reflect national requirements.

Under GDPR, the organisation no longer has to register with the ICO but under the Data Protection (Charges to Information Regulations) 2018 it will remain a legal requirement for data controllers to pay the ICO a data protection fee. These fees are used to fund the ICO's data protection work the UK.

Schedule 1, Part 4 of the DPA 2018 (and also Article 30 of GDPR) states that the organisation shall maintain a Record of Processing Activities (ROPA) for personal data. Processing for GMSS is recorded on the Information Asset Register and Data Flow Mapping Register. An update on the current status of GMSS's record of processing is presented to the SIRO and IG Group.

Schedule 1, Part 4, Section 38 of the DPA states that an appropriate policy document needs to be in place for the processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of Schedule 1 of the Act. This is documented in GMSS 'Appropriate Use Policy Document' which sets out how we protect personal and special category data. The types of processing undertaken in GMSS where this is required are:

- Employment, social security and social protection - DPA 2018, Schedule 1, Part 1, S1;
- Part 2, S5 of Schedule 1 of the Data Protection Act 2018 where the processing of special category personal data is necessary for reasons of substantial public interest.

The DPA also covers the areas of processing which are not covered in the GDPR relating to:

Law Enforcement Processing

- It provides a bespoke means of processing personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes of, or access to, personal data transmitted, stored or otherwise processed.
- Allows the unhindered flow of data internationally whilst providing safeguards to protect personal data.

Intelligence Services Processing

- It ensures that the laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and Enforcement

- It enacts additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- It allows the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches.
- It empowers the Commissioner to bring criminal proceedings against offences

where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

Section 170 of the Data Protection Act 2018

Section 170 of the DPA builds on Section 55 of the DPA 1998 which criminalised knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller, and the sale or offering for sale of that data. The provision was most typically / commonly used to prosecute those who had accessed healthcare and financial records without a legitimate reason. This adds the offence of knowingly or recklessly retaining personal data (which may have been lawfully obtained) without the consent of the data controller.

Section 171 of the Data Protection Act 2018

Section 171 criminalises the re-identification of personal data that has been 'de-identified' (de-identification being a process such as redactions to remove / conceal personal data).

For example, using a method or system to reverse the redaction creating a new set of identifiable information.

Section 173 of the Data Protection Act 2018

Staff are reminded that under Section 173 of the DPA 2018 it is a criminal offence for GMSS or a person employed by GMSS to alter, deface, block, erase, destroy or conceal data with the intention of preventing disclosure of information that a data subject enforcing his / her rights would have been entitled to receive. Any member of staff taking such action would be liable on conviction to a fine.

For example deliberately withholding or destroying information that if disclosed to a data subject as part of their request for access to their own data (right of access request) might cause embarrassment / damage to a member of staff or GMSS.

Transfer of data outside the UK

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Please contact the IG team if you wish to transfer to an organisation / individual outside of the UK.

8. The Common Law Duty of Confidentiality

All NHS bodies and those carrying out functions on behalf of the NHS / GMSS have a duty of confidentiality to patients / service users and a duty to abide by professional ethical standards of confidentiality.

Everyone working for or with NHS / GMSS records who handles stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidentiality to the service user and to his / her employer.

The duty of confidentiality is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

The duty of confidentiality owed to a deceased individual user is consistent with the rights of living individuals.

9. Caldicott Principles

In 2013 the Caldicott Review was undertaken within the NHS and the principles as highlighted below were created.

The 7 Caldicott Principles are:

Principle 1 – Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 – Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 – Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 – Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 – Everyone with access to personal confidential data should be aware of the responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

10. National Data Guardian Standards

The National Data Guardian Standards were created from the third review undertaken by Dame Fiona Caldicott who is now known as the National Data Guardian for Health and Care. The review in 2016 made recommendations to the Secretary of State for Health aimed at strengthening the safeguards for keeping health and care information secure and ensuring the public can make informed choices about how their data is used. The NDG review outlines new data security standards for the NHS and social care, a method for testing compliance against the standards, and a new opt-out to make clear how people's health and care information will be used and in what circumstances they can opt out.

The full report is called Review of Data Security and Opt Outs, and can be accessed on the link below.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

The Data Security Standards are:

Data Security Standard 1 (Personal Confidential Data)

All staff ensure that personal data is handled, stored and transmitted securely whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Data Security Standard 2 (Staff Responsibilities)

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3 - Training

All staff complete appropriate annual data security training and pass a mandatory test.

Data Security Standard 4 - Managing Data Access

All staff Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5 - Process Reviews

All Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security

Data Security Standard 6 - Responding to Incidents

Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection

Data Security Standard 7 - Continuity Planning

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Data Security Standard 8 - Unsupported Systems

No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9 - IT Protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10 - Accountable Suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

11. Disclosing Information

A Guide to Confidentiality in Health and Social Care and GMSS Data Security (IG) Handbook provides advice on using and disclosing confidential service user information and has models for confidentiality decisions. All staff must adhere to this guidance.

If a staff member wishes to disclose Personal information then advice should be sought from GMSS IG Team.

Consent of the individual is usually required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

Under common law, personal information may be disclosed without consent for example:

- In order to prevent abuse or serious harm to others;
- Where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.

All individuals must:

- Exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- Ensure the physical security of all confidential documents, including storage of files on PCs.

Staff should never give information to a person claiming to be the friend, relative or representative of a member of staff/patient/service user. Unless appropriate checks have taken place to ensure that person has a legitimate reason for access. Action of this kind may be viewed as a breach of confidentiality and may lead to an investigation; this may result in disciplinary action being taken.

12. Personnel Information

In keeping with good Human Resources practice, GMSS retains and processes personal data on its employees. In addition, GMSS may from time to time, retain and process “Special Categories of Data” as defined by GDPR for example, in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring, for the prevention of fraud or other illegal activities.

GMSS may process such data and such data may be legitimately disclosed to appropriate employees and GMSS professional advisors, in accordance with the principles of the Data Protection Act and GDPR.

GMSS takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/ her may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with GMSS HR Lead.

13. Information Security

The information held and managed by GMSS 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.

Information Security – Requirements

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 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.

GMSS will develop, implement, maintain and test where required, local business continuity plans. Such plans will be a contractual obligation of any relevant supplier.

GMSS will ensure that appropriate controls are applied to all types of communication, internal and external, to ensure the communication is secure, appropriate and reaches the intended recipient.

GMSS will undertake risk assessments to identify, quantify and prioritise information security risks in accordance with GMSS Information Risk Policy. Controls will be selected and implemented to mitigate the risks identified.

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.

Asset Management

GMSS information (electronic and hardcopy), software, computer and communication equipment, will be accounted for and have an owner.

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.

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.

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

14. 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 NDG 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.

15. 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.

16. 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.

17. 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.

18. 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.