

GMSS Data Security Breach & Incident Reporting Policy

Review Date: February 2022

Document Control

Title / Reference:	Data Security Breach & Incident Reporting Policy
Status:	Approved
Version:	V2.0
Date Issued / Ratified:	29/03/2020
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 & 3 rd party partners
Links to other strategies, policies, procedures etc:	<ul style="list-style-type: none"> • 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 <p>This list is not exhaustive</p>

Change History

Summary of Changes	Name	Date	Version
New Document	IG Team	Sept 18	1.0
Review of Procedure	IG Team	Nov 19	2.0
Changed from Procedure to Policy. Amendments to make policy clearer	IG Team	Feb 20	2.0

Review

Name	Role	Date	Version
IG Group	IG Group	Mar 20	2.0
Governance Committee	Governance Committee	Mar 20	2.0
Senior Management Team	Senior Management Team	Mar 20	2.0

Approval

Name	Role	Date	Version
IG Group	IG Group	Mar 20	Mar 20

Governance Committee	Governance Committee	Mar 20	Mar 20
Senior Management Team	Senior Management Team	Mar 20	Mar 20

Distribution

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

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.....	5
2. Purpose & Scope.....	5
3. Definitions.....	5
4. Roles and Responsibilities.....	8
5. Data Security Breaches / Incident Investigation Process	10
6. Cyber Security Incident Reporting and Management Process	13
7. Reporting.....	13
8. Lessons Learned	13
9. Training and Awareness	14
10. Classification of Information	14
11. Legislation & Guidelines.....	14
12. Equality Statement.....	14
13. Monitoring and Review.....	15

Appendices

Appendix A: Guide to Notification of Data Security & Protection Incidents.....	16
Appendix B: Breach Assessment Grid.....	17

1. Introduction

Greater Manchester Shared Services (GMSS) has a responsibility to ensure data security (personal data) breaches and / or information governance incidents are reported and managed efficiently and effectively. Where personal data breaches affect the 'rights and freedoms of an individual, the General Data Protection Regulation 2016 (GDPR) (Article 33) imposes a duty to report these types of personal data breach to NHS Digital and to the Information Commissioner's Office (ICO). In some cases, these will also be reported to the Department of Health and Social Care (DHSC). These are reported using the Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

This policy describes the process for staff to follow regarding recording, reporting and reviewing of data security breaches and incidents. This supports GMSS's overall incident reporting process which is an integral part of personal, clinical and corporate governance.

The information contained within this procedure is taken from the "Guide to the Notification of Data Security and Protection Incidents" produced by NHS Digital (2018). Further detailed information about data breach reporting can be found in this document and must be referred to when reading this procedure and grading any personal data breach / incident. The guidance can be found on the following link: <https://www.dsptoolkit.nhs.uk/Help/29>

It is a contractual requirement to include statistics on data security breaches in the annual report and the Statement of Internal Control (SIC) presented to the Senior Management Team (SMT) and GMSS must keep a record of any data security breaches, regardless of whether it is required to notify these to the ICO. The IG Team co-ordinate and maintain a Data Security Breaches / Incident Reporting Logbook.

GMSS is not subject to the Security of Network Information Systems (NIS) Regulations 2018 and is therefore not required to report breaches under this regulation.

2. Purpose & Scope

This policy sets out the process across GMSS for the reporting and management of data security breaches / incidents.

This policy applies to:

- Members of staff directly employed by GMSS and for whom GMSS has legal responsibility.
- Staff covered by a letter of authority / honorary contract or work experience.
- All third parties and others authorised to undertake work / process data on behalf of GMSS.

3. Definitions

Personal Data Breach

As per Article 4(12) of the GDPR, a "personal data breach" 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.

The traditional view that a personal data breach is only reportable when data falls into the wrong hands is now replaced by a concept of a 'risk to the rights and freedoms of individuals' under Article 33 of GDPR. These types of breaches are graded as per the guidance from NHS Digital using a risk scoring 5x5 matrix and may be notifiable to the Information Commissioners Office (ICO) if they attain a grade as described in the "Guide to the Notification of Data Security and Protection Incidents" <https://www.dsptoolkit.nhs.uk/Help/29>.

Personal data

This is data defined as any information relating to an identified or identifiable living individual.' An "Identifiable living individual" means a living individual who can be identified, directly or indirectly, by reference to:

- An identifier such as a name, an identification number, location data or an online identifier, or
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

All paper records that relate to a living individual and any aspect of digital processing such as IP address and cookies are deemed personal data. GDPR also introduces geographical data and biometric data to be classified as personal data.

Special Categories of Personal Data

Under GDPR, these are:

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- The processing of genetic data,
- Biometric data for uniquely identifying a natural person,
- Data concerning health,
- Data concerning a natural person's sex life or sexual orientation.

For data security breach reporting purposes, special categories of data also include:

- Vulnerable children,
- Vulnerable adults,
- Criminal convictions/prisoner information,
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual,
- Communicable diseases as defined by public health legislation,
- Sexual health,
- Mental health.

Breach Types

The Article 29 Working Party, an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission, now known as the European Data Protection Board (EDPB) under the EU General Data Protection Regulation (GDPR),

categorised data security breaches into 3 categories which were associated with confidentiality, integrity and / or availability, known as The CIA Triad (see below).

A definition of each category of breach is detailed below:

- Confidentiality Breach – Unauthorised or accidental disclosure of, or access to personal data,
- Availability Breach – Unauthorised or accidental loss of access to, destruction of personal data,
- Integrity Breach – Unauthorised or accidental alteration of personal data.



Table 1 outlines the ICO categorisation of data breaches in conjunction with the type of breach category as identified by the Article 29 Working Party.

Please note further details regarding the types of breaches under each of the CIA Triad can be found in the “Guide to the Notification of Data Security and Protection Incidents” <https://www.dsptoolkit.nhs.uk/Help/29>.

Table 1 – ICO and Article 29 Working Group classification of data security breaches

	ICO Categorisation	Type of Breach (Art 29 Working Party)
A	Data sent by email to incorrect recipient	Confidentiality
B	Cyber security misconfiguration (e.g. inadvertent publishing of data on website; default passwords)	Confidentiality
C	Cyber incident (phishing)	Confidentiality
D	Insecure webpage (including hacking)	Confidentiality
E	Cyber incident (key logging software)	Confidentiality
F	Loss or theft of paperwork	Availability
G	Loss or theft of unencrypted device	Availability
H	Loss/theft of only copy of encrypted data	Availability
I	Data left in insecure location	Availability
J	Cyber incident (other - DDOS etc.)	Availability
K	Cyber incident (exfiltration)	Availability
L	Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)	Availability
M	Insecure disposal of paperwork	Availability
N	Insecure disposal of hardware	Availability
O	Other principle 7 failure	Integrity
P	Cyber incident - unknown	Integrity

4. 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 across the entire organisation (GMSS) to support service delivery and continuity. Information Governance provides a framework to ensure that information is used appropriately and is held securely.

Caldicott Guardian

The Caldicott Guardian is the conscience of the organisation and is responsible for ensuring that national and local guidelines on the handling of confidential personal information are applied consistently across the organisation. They are responsible for

ensuring patient identifiable information is shared in an appropriate and secure manner.

Senior Information Risk Owner (SIRO)

The SIRO takes ownership of GMSS's information risk framework. As a member of the Senior Management Team, the SIRO acts as an advocate for information risk and provides written advice to the Managing Director on the content of their annual governance statement in regard to information risk.

Data Protection Officer (DPO)

The DPO informs and advises staff about their obligations to comply with GDPR, the Data Protection Act and other relevant legislation. The DPO monitors GMSS's compliance with data protection policies and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities.

Heads of Service

Heads of Service take responsibility for ensuring that the Data Security, Protection & Confidentiality framework is communicated and implemented within their service, and ensure that all staff remain compliant, including any temporary or contract staff.

Information Asset Owner / Administrator (IAO / IAA)

The IAO / IAA are responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

Information Governance Team

Has responsibility to:

- To co-ordinate and investigate reported DS&P incidents, maintain an Incident / Data Security Breaches Reporting Logbook, make recommendations and act on lessons learnt.
- To liaise with GMSS Information Governance Lead, DPO, SIRO and IT Services / IT Security Manager as appropriate pertaining to data security incidents.
- To escalate incidents to GMSS Information Governance Lead in order to inform the Senior Information Risk Owner / Caldicott Guardian / DPO as appropriate.
- To grade the incident and report it where necessary on the Data Security & Protection Toolkit Incident Reporting Tool in conjunction with the DPO and log on the local IG Incident / Data Breaches Reporting Logbook.

GMSS IT

GMSS IT and the IG Team will work together if there is any Data Security Incidents/Breaches that are IT related.

The IT Security Manager will be alerted to any Cyber Security Incidents and will investigate accordingly. If necessary the IT Security Manager will inform the SIRO.

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 are part of these mandatory training requirements.

5. Data Security Breaches / Incident Investigation Process

Staff must follow GMSS's process for incident reporting which includes any data security breaches / incidents. All data security breaches / incidents must be reported initially to the DPO and IG Team AS SOON AS THIS INCIDENT IS KNOWN following GMSS's incident reporting processes (see time scale for reporting section, page 9).

Do not delay reporting of any incident even if you suspect it may not be an incident / breach.

If it is identified as a data security breach / incident, it will be logged on GMSS's Data Security Breaches / Incident Reporting Logbook. GMSS Lead / SIRO / CG / DPO and IG Team will assess the incident using the NHS Digital's guidance (see figure 1 below).

Incidents are graded according to the significance of the breach on a scale of 1-5 (1 being the lowest and 5 being the highest) and the likelihood of those serious consequences occurring on a scale of 1-5 (1 being the lowest and 5 being the highest). Please note incident / breaches are graded according to the impact on the individuals it concerns and not the organisation.

Article 34 requires GMSS to notify the relevant authority when an incident constitutes a high risk to the rights and freedoms of an individual. This is classified when a breach has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

The tables in Appendix A set out how to grade the severity of a data security breach / incident to see if it is high risk and be significant enough to be reported to the ICO. The Breach Assessment Grid in Appendix B ascertains when an incident is notifiable and to whom.

When incidents are notifiable, this is carried out by the IG Team using the NHS Digital Incident Reporting Tool housed in the Data Security and Protection Toolkit (DSPT).

Vulnerable Groups

Where a data security breach relates to a vulnerable group in society, a minimum risk assessment score of 2 for likelihood and significance is stated unless the incident has been contained (see Appendix A).

Time scale for reporting

Article 33 of GDPR requires reporting of a breach within 72 hours. This is from when GMSS becomes aware of the breach and may not be necessarily when it occurred. However, it is important that all staff report any data security / IG incidents / breaches **AS SOON AS POSSIBLE**. Failure to notify promptly may result in action taken by the ICO by breaching Article 33.

It is mandatory for all staff to report 'near misses' (where there would be a potential breach / incident but was prevented) as well as actual incidents, so that we can take the opportunity to identify and disseminate any 'lessons learnt'.

Informing the public

Article 34 requires that the public are notified if a data security breach results in a high risk to the rights and freedoms of individuals. This notification must include:

- A description of the breach,
- Name and contact details of the DPO or equivalent,
- A description of the likely consequences of the breach,
- A description of the measures taken or to be taken to address and mitigate the breach,
- Its possible adverse effects.

If GMSS does not decide to notify individuals it must have a justified reason to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals it concerns.

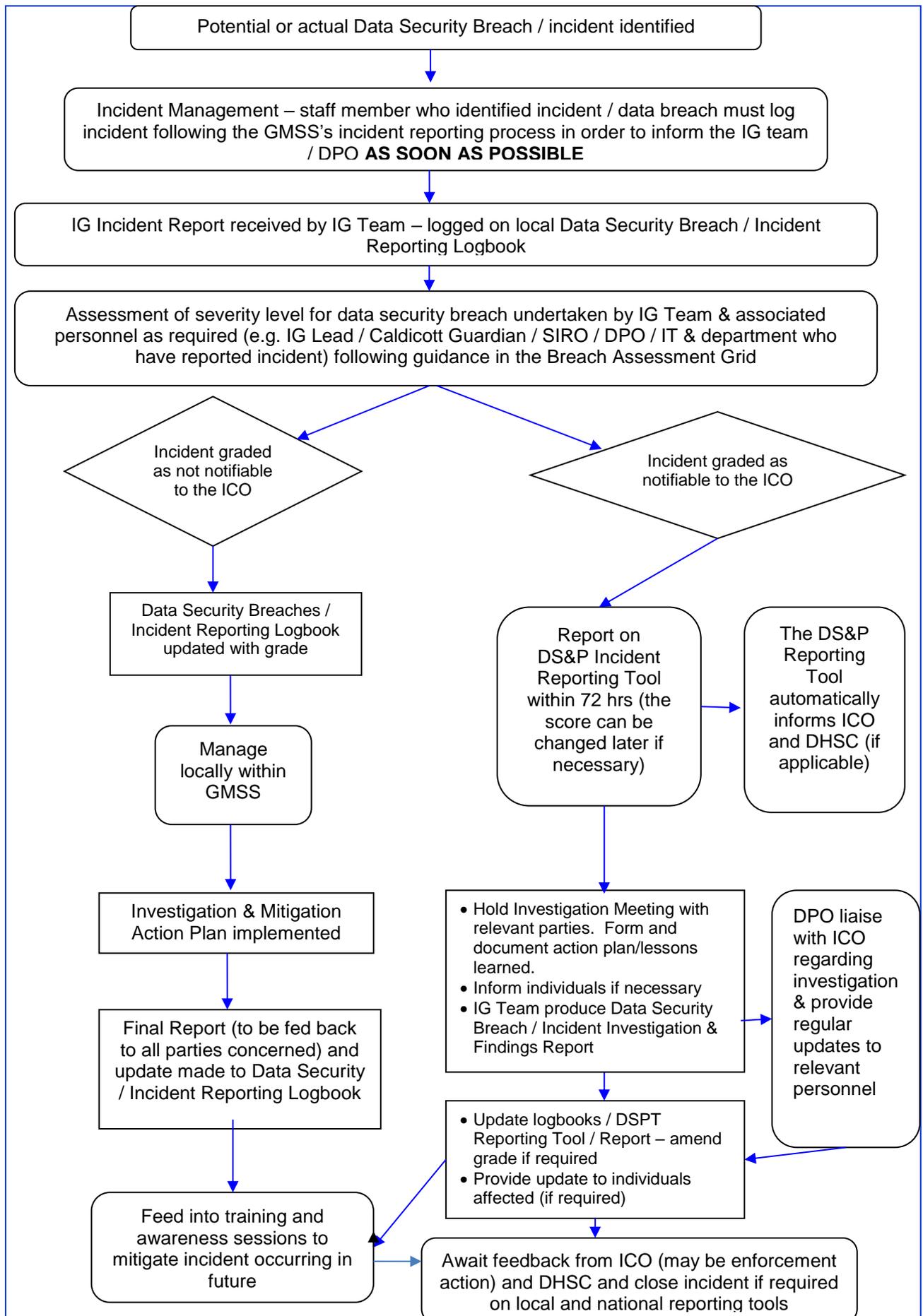
Containment Actions which affect notification status

There may be circumstances where GMSS is aware of a breach but there are containment actions that remove the need for notification to the ICO but will still be recorded locally. For example, notification may not be necessary when:

- Encryption is used to protect personal data;
- Where personal data is recovered from a "trusted partner" organisation. A trusted partner is classified when the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error and to comply with instructions to return it. Even if the data has been accessed, GMSS could still possibly trust the recipient not to take any further action and return and co-operate with GMSS's instructions;
- Where GMSS can null the effect of any personal data breach.

The flowchart (Figure 1) sets out the overall process for reporting, managing and investigating data security & protection incidents / personal data breaches for GMSS.

Figure 1 – Data Security Breach / Incident Reporting Flowchart



6. Cyber Security Incident Reporting and Management Process

In most cases, staff should report incidents via the IT Service Desk as they will tend to be IT related such as PC / laptop not working correctly, phishing emails or denial of access to a system or webpage.

For any Cyber Security Related Incidents staff must log these with the IT Service Desk where IT will also log onto the DATIX system and where applicable provide guidance to staff. Staff must follow the Cyber Incident Management Policy/Procedure located on People Matters.

7. Reporting

Reporting in the Annual Governance Statement / Statement of Internal Control

Reportable incidents that affect the rights and freedoms of an individual need to be detailed in the annual report / governance statement / Statement of Internal Control as outlined in Table 1 below.

Table 1 - Summary of Data Security and Projection Incidents reported to the ICO and/or DHSC.

Date of incident (month)	Nature of incident	Number affected	How patients were informed	Lesson learned

Reporting by NHS Digital

Data breaches reported via the DSPT Incident Reporting Tool will be forwarded to the appropriate organisation indicated in the Guide to the Notification of Data Security and Protection Incidents referenced earlier in this policy, such as the Department of Health and Social Care (DHSC), NHS England and the ICO. Additionally, these organisations may have obligations to work with other agencies, such as the National Cyber Security Centre, for example, and any incident information may be shared onward. For this reason, it is prohibited to include individual information that could identify any person affected by a breach. All incidents will be shared on a monthly basis to the Governance Committee in aggregate form for incident monitoring and trend analysis.

Reporting to the IG Group

Data Security breaches / incidents are reported routinely to the Information Governance Group via the IG Key Statistics Report. Lessons learned are discussed and actioned when necessary to assist mitigation future similar incidents.

8. Lessons Learned

It is essential that action is taken to help to minimise the risk of data security breaches

/ incidents re-occurring in the future. Therefore, lessons learned from data security breaches will be fed back to staff. This may be communicated in IG Updates via The Bulletin and staff briefings.

Staff involved with a data security breach / incident will also be required to complete additional IG Training and / or require further support. The IG Team will determine this with the support of any investigation team assigned if necessary.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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 February 2022.

Appendix A

Guide to Notification of Data Security & Protection Incidents

Establish the likelihood that adverse effect has occurred.

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity of the adverse effect on individuals.

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Both the adverse effect and likelihood values form part of the breach assessment grid.

Appendix B

Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “grey breaches” being reportable / notifiable to the ICO / DHSC via the DSPT incident reporting tool.

Incidents where the grading results are in the red are advised to be notified within 24 hours.

Impact	Catastrophic	5	5	10	15 20 25 Reportable to the ICO DHSC Notified		
	Serious	4	4 No Impact has occurred 3	8 An impact is unlikely 6	12 16 20		
	Adverse	3			9 12 15 Reportable to the ICO		
	Minor	2	2	4	6 8 10		
	No Impact	1	1 2 No Impact has occurred 3 4 5				
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood harm has occurred				