NHS
Greater Manchester Shared Services

GMSS Secure Transfers of Data Policy

Review Date: February 2022

Document Control

Title / Reference:	Secure Transfers of Data Policy
Status:	Approved
Version:	V1.2
Date Issued / Ratified:	March 2020
Originator of Document and Job Role:	IG Team
File Classification:	Official Data
Retention:	Life of the organisation plus 6 years (place of deposit)
Target Audience:	All GMSS staff & 3rd party partners
Links to other strategies, policies, procedures etc:	• Data Security, Protection & Confidentiality Policy • Data Security, Protection & Confidentiality Framework • Confidentiality Audit Procedure • Data Security Breach & Incident Reporting Policy • Secure Transfer of Data Policy • Acceptable Use of IT / Information Systems Policy • Information Classification Policy • Records Management Policy • Risk Management Policy • Information Risk Policy • Subject Access Request Policy • Registration Authority (Smart Card) Procedure • Data Security, Protection & Confidentiality Staff Handbook **This list is not exhaustive**

Change History

Summary of Changes	Name	Date	Version
Reviewed from Oldham CCG to fit GMSS	IG Team	Nov 16	0.1
Recommend approval by the IG Group	IG Group	Nov 16	0.1
Recommend approval after some amendments	FPG	Jan 17	0.1
Amendments needed	SMT	Jan 17	0.1
Changed to accommodate GDPR	IG Team	Aug 17	1.1
More detailed information added to content following GDPR & DPA 2018 guidance and updated secure email domains	IG Team	Nov 19	1.2
Amendments made to make policy clearer	IG Team	Feb 20	1.2

Review

Name	Role	Date	Version
IG Group		Nov 17	0.1
FPG		Jan 17	0.1

SMT		Jan 17	1.1
IG Team		Nov 19	1.2
IG Team		Feb 20	1.2
IG Group		Mar 20	1.2
Governance Committee		Mar 20	1.2
SMT		Mar 20	1.2

Approval

Name	Role	Date	Version
IG Group		Nov 17	0.1
FPG		Jan 17	0.1
SMT		Jan 17	1.1
IG Team		Nov 19	1.2
IG Group		Mar 20	1.2
Governance Committee		Mar 20	1.2
SMT		Mar 20	1.2

Distribution

Name	Role	Date	Version
Saved in policy folder		Jan 17	1.1
Updated policy tracker		Jan 17	1.1
GMSS Publication scheme		Jan 17	1.1
The Bulletin		Jan 17	1.1
Saved in policy folder		Nov 19	1.2
Updated policy tracker		Mar 20	1.2
GMSS Publication scheme		Mar 20	1.2
The Bulletin		Mar 20	1.2
People Matters		Mar 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 purpose of this policy is to provide guidance to all NHS Greater Manchester Shared Service (GMSS) employees regarding secure transfers of information, specifically where this is personal confidential data and / or business confidential data.

When transferring information staff need to take into account the nature of the information to be transferred and ensure that it has the necessary protection to ensure its security. This is especially important when information contains personal, confidential or special categories of data. This policy sets out different types of transfer and security requirements. However, please seek the advice from the Data Protection Officer / IG Team if a transfer method is not included here to assess the most secure option for your transfer of data.

Routine transfers of personal confidential data and business sensitive data must be logged on the Data Flow Mapping Register as per GDPR. This then enables GMSS to provide transparency and demonstrate integrity regarding the data flows it processes and how these are transferred securely to ensure that patients and staff trust us to process their data.

2. Scope

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.

When information is being transferred from one location / organisation to another, staff must ensure that this is transported securely particularly when this is personal confidential data and / or business sensitive data. This policy sets out a framework to inform staff who are responsible for transferring:

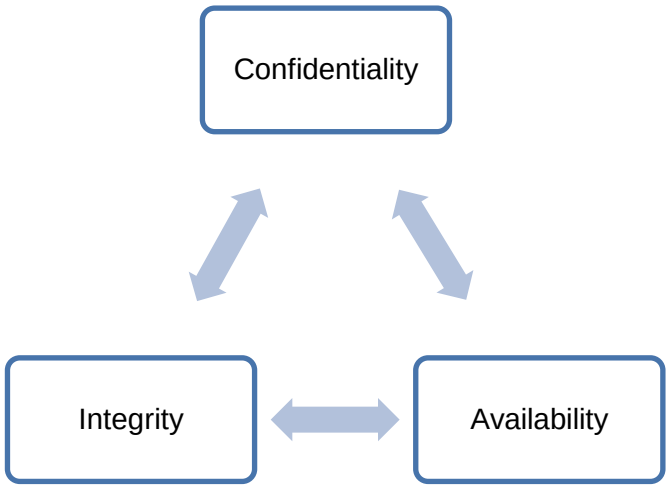
- Routine flows of personal data;
- Special category data;
- Personal staff information;
- Business sensitive and / or commercial in confidence information.

All GMSS staff must maintain the confidentiality of personal data, including any transferring of the same.

Please note compliance of this policy is monitored by confidentiality audits as outlined in the Confidentiality Audit Procedure. These are conducted by the GMSS IG Team. The results of these audits are fed back to the Information Governance Group (IG Group) who monitor compliance and take action where necessary.

3. Confidentiality, Integrity & Security

Data Security can be broken down into three areas - Confidentiality, Integrity & Availability - and these are fundamental when transferring / accessing data.



Confidentiality - Ensuring information is kept confidential and only available to those with a proven need to see it. This data must not be disclosed to others unless a legal statute or patient / public interest applies. For example, it would be unacceptable for a perfect stranger to be able to access personal confidential data from a laptop simply by lifting the lid and switching it on. That is why a laptop should be password-protected and the data on it encrypted when switched off. Also, when this information is transferred it must be done so following secure transfer processes.

Integrity - Information stored in a way that is consistent and unmodified. Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Secure transfer processes such as encryption must be followed when transferring information to ensure this remains secure.

Availability - Information being there when needed. System design must include appropriate access controls and checks so that the information in the system has consistency and accuracy, can be trusted as correct, and can be relied on when needed.

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 ensures 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

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.

Head of Corporate IT & IT Security Manager

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

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. Definitions

Personal Data - This contains details that identify individuals either from one data item or a combination of data items. The following are demographic data items that are

considered identifiable:

- Name,
- Address,
- NHS Number,
- Full postcode,
- Date of birth.

Under GDPR, this now includes location data and online identifiers.

Special Category Data - This is personal data consisting of information regarding:

- Race,
- Ethnic origin,
- Political opinions,
- Health,
- Religious beliefs,
- Trade union membership,
- Sexual life,
- Previous criminal convictions.

Under GDPR, this now includes biometric data and genetic data.

For more information about special categories of data please refer to the ICO guide at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Personal Confidential Data - This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Processing – This 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.

6. Key Legislation / Guidance relating to secure transfers of data

A number of acts and guidance dictate the need for secure transfer arrangements to be set in place. They include (but are not restricted to):

- General Data Protection Regulations (GDPR) 2016
- Data Protection Act 2018
- National Data Guardian Data Security Standards
- Caldicott Principles

General Data Protection Regulation 2016 / the Data Protection Act May 2018

The EU General Data Protection Regulation (GDPR) was approved in 2016 and became directly applicable as law in the UK from 25th May 2018. The Data Protection Act 2018 references GDPR throughout and we have to look at both pieces of legislation side by side.

The aim of the GDPR is to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of personal data.

GDPR / DPA Principles

All staff must adhere to the principles of GDPR / DPA when processing personal and / or special categories of data and demonstrate compliance with these.

Article 5 of GDPR sets out seven key principles which lie at the heart of this data protection regime, this includes ensuring the secure transfer of information. The seven key principles are, Data is:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner 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 ('purpose limitation');

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(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 ('accuracy');

(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 insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(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 ('integrity and confidentiality')."

The seventh principle relates to "accountability" which makes GMSS responsible for complying with GDPR and says that GMSS must be able to demonstrate compliance.

For further information relating to the accountability principle please see: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accountability-principle/

National Data Guardian Data Security Standards

The National Data Guardian (NDG) Data Security Standards have been developed as a result of the National Data Guardian Review of Data Security, Consent and Opt-outs. These outline measures to ensure information at rest and in transit is secure. There are 10 standards which are clustered under 3 leadership obligations to address people, process and technology issues. These are:

Leadership Obligation 1: People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

- **Data Security Standard 1** - All staff ensure that personal confidential 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** - 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** - All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Data Security & Protection Toolkit.

Leadership Obligation 2: Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

- **Data Security Standard 4** - 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** - 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** - 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** - 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.

Leadership Obligation 3: Technology: ensure technology is secure and up-to-date.

- **Data Security Standard 8** - No unsupported operating systems, software or internet browsers are used within the IT estate.

- **Data Security Standard 9** - 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** - 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.

The Caldicott Principles

Before using or sharing confidential information, you must also consider the Caldicott Principles:

- **Principle 1** - Do you have a justified purpose for using this confidential information? The purpose for using confidential information should be justified, which means making sure there is a valid reason for using it to carry out that particular purpose.

- **Principle 2** - Are you using it because it is absolutely necessary to do so? The use of confidential information must be absolutely necessary to carry out the stated purpose.

- **Principle 3** - Are you using the minimum amount of information required? If it is necessary to use confidential information, it should include only the minimum that's needed to carry out the purpose.

- **Principle 4** - Are you allowing access to this information on a strict need-to-know basis only? Before confidential information is accessed or transferred, a quick assessment should be made to determine whether it is actually needed for the stated purpose. If the intention is to share the information, it should only be shared with those who need it to carry out their role.

- **Principle 5** - Do you understand your responsibility and duty to individuals with regards to keeping their information secure and confidential? Are you up to date with your training? Do you understand your responsibility for protecting information?

- **Principle 6** - Do you understand the law and are you complying with the law before handling the confidential information? If not ask!

- **Principle 7** - Do you understand that the duty to share information can be as important as the duty to protect confidentiality. However it's important to remember if you are sharing this is done lawfully and securely!

7. Data Security in the Work Environment

Secure Transfer of Data procedures must be in place in any location / office environment where confidential data is being processed and transferred / transmitted especially when this is personal data / special category data or business sensitive data.

Working environment and practice guidelines should include:

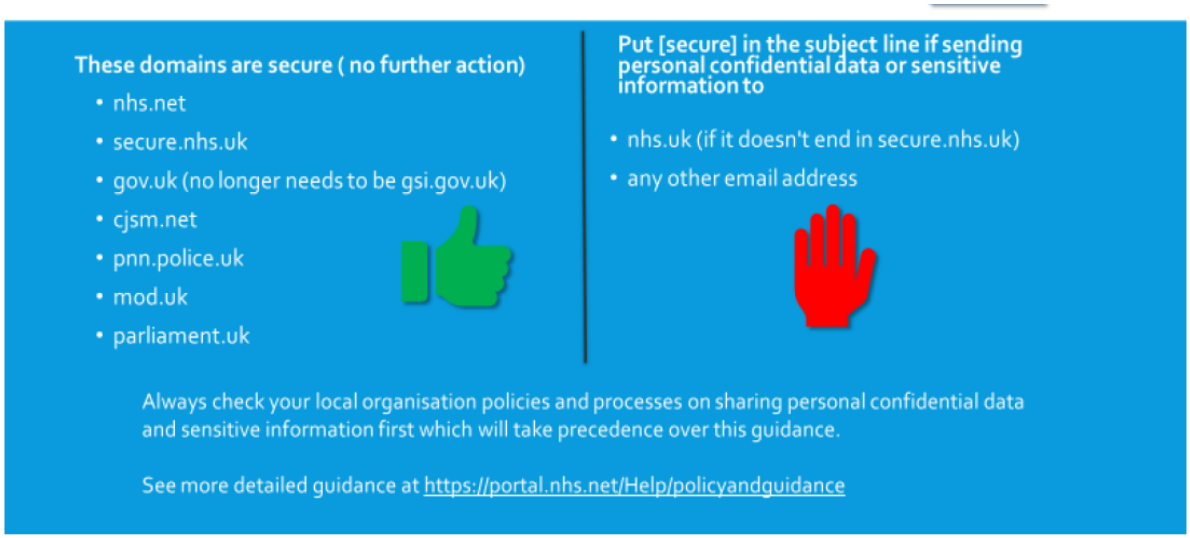
- The office or workspace must be lockable and / or accessible via a coded key pad (or similar device) and be accessible only by authorised staff;
- If offices are sited on the ground floor, windows must be lockable and screens must be located so they cannot be seen by unauthorised personnel through the windows;
- Do not prop locked doors open, they are locked for a reason;
- Escort visitors and check they are authorised;
- Computer screens must not be left on view so that members of the general public or staff who do not have a justified need to view the information can see personal data;
- If moving away from a computer / laptop screen it must be locked. Select **CONTROL + ALT + DELETE** and **ensure you hit the enter key.** Or select the **WINDOWS KEY + L** to quickly lock a screen;
- If you see a colleague's device open and unlocked, lock it for them and remind them to do so in future;
- Computers or laptops must be switched off when not in use;
- Only GMSS approved encrypted laptops / desktops are to be used which include encryption software;
- Information must be held on GMSS's secure network and not on desktops;
- Passwords must not be shared. Strong passwords must be used on all your devices to prevent unauthorised access. You should also use different passwords for each account. Creating strong passwords does not need to be a daunting task if you follow simple guidelines. The National Cyber Security Centre (NCSC) has a range of guidance on good password management, including this article to help set secure passwords: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
- Manual paper records containing confidential data must be stored in locked cabinets when not in use and securely stored when the office / workstation is left unattended. Make sure you lock documents away if away from desk during the day, evenings and weekends. Do not forget that some desks are hot desks and anyone can use them so please do not leave confidential information on the desks;
- The **"secure printing facility"** must always be used when printing confidential / sensitive information;
- Post trays should be situated away from any unauthorised access and situated where they can be monitored and mail must be disseminated to the addressee as soon as possible.

8. Transfers of data by Email

Personal confidential data and / or business sensitive data must always be sent via NHSMail or an NHS approved encrypted email system. NHSMail accounts have the suffix @nhs.net. (firstname.secondname@nhs.net), emails will be sent / received via the encrypted NHSMail service.

Please note NHS accounts which end in @nhs.uk **are not secure.** If you are sending personal confidential data and / or business sensitive data and are unsure whether you are sending to an encrypted email account, always ask.

Organisations external to the NHS such as local authority / councils, local providers e.g. care homes have different email accounts. The list below states those non NHS domains where emails can be sent to and from an NHSMail account and it will be sent encrypted and therefore secure:



When emailing personal confidential data and / or business sensitive data to outside third party organisations that do not have NHSMail, they must have either an approved email encryption software (AES) system in place, or, the NHSMail process for sending emails securely to non NHSMail accounts must be used.

NHSMail process for sending emails securely to non NHSMail accounts

NHSMail users can now send encrypted and secure emails to non NHSMail accounts (non-accredited or non-secure recipients) including Gmail, Hotmail etc.

When you enter **[secure]** in the subject line of the email and click send, the email is encrypted and protected with a digital signature on the NHSMail platform within the UK. The recipient will be asked to authenticate to the service (they will receive an alert from the Trend Encryption Portal and be asked to 'Open Message' where they will need to enter their password). If staff have not previously registered with the Trend Encryption service, they will be redirected to the Trend Micro Private Post website and be required to follow the registration process. It is good practice to inform recipients that they will receive this message as it sometimes looks like a junk email and they may ignore it.

The formatting of the message will be preserved and attachments can be included. Please be aware some attachments are not supported, more information about this can be found in the NHSMail Attachments Guide, by clicking on this link, https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/attachmentsguide.pdf. The sent item will be stored in your Sent Items folder, and any replies received will be decrypted and displayed as normal in

NHSMail. The recipient will be able to reply, forward the email on and it will still remain secure and encrypted.

If you have regular contact with a user and want to set up this line of communication, please advise them that you will be using this method and ask the recipient to set up the 'encrypted channel' in advance (this is where they will need to register on the Trend Micro Private Post website).

For further details please refer to the NHSMail Encryption Guide – this can be forwarded to your recipients in advance to help with the set up. You can access this by clicking on the link https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/encryptionguide.pdf

How to send an encrypted email from an NHSMail account:

- Using your NHSMail account as normal, create a new message as normal;
- Ensure the recipients email address is correct;
- In the Subject field of the email, type the word **[secure]** before the subject of the message. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets are not used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment;
- Type your message;
- Send the email as normal.

Note: [secure] is not case sensitive and [SECURE] or [Secure] for example could also be used.

For more detail on any of the above please refer to the NHS Digital Guidance for Sending Secure Email page https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email

Email Awareness Tips:

- Never automatically "reply all" always check the email addresses are correct and it is appropriate that they are included in your response. If someone within the chain has made a mistake and you "reply all" you will be repeating the error and this could end in an unauthorised disclosure which could result in a GMSS Data Security breach / IG Incident which may be reportable to the ICO. This could potentially result in a monetary fine and more importantly a loss of public trust.

- Always carefully check email addresses before you send an email. NHSMail is a national system which contains similar email address for the same name. E.g. there can be a Mickey.mouse1@nhs.net and a Mickeymouse1@nhs.net The only difference is a dot and it's very easy for a mistake to occur! The incorrect email can automatically pop up in future emails if you do not clear it from your contacts.

- Always ensure you regularly review any distribution lists (DL) you have to ensure all the recipients are still current and correct.

- Do you know the difference between "TO" "CC" and "BCC"? The consequences of not understanding the difference can be a data breach.

- **TO** is the person exactly to whom you are sending the email. Generally the whole purpose of the email is to express or pass information to the person who is in the TO field.

- **CC** stands for Carbon Copy. When writing emails the actual recipients address will be included in TO field of the mail application. People who are not directly involved or acting on the subject matter will be included in CC field for information purposes.

- **BCC** stands for Blind Carbon Copy, which is exactly similar to CC but the email addresses included in the BCC field will not be visible to anyone else other than the particular recipient. This function is particularly important where you wish to send an email to a distribution list without disclosing email addresses to other email recipients who do not need to know the email addresses of others.

- Emails which contain personal confidential data should always be appropriately titled i.e. do not include confidential details in the subject line such as a name.

- If you do send an email in error, you can use the recall facility 'recall this message' (this function is only available in Outlook and not NHSMail web based). If the recipient hasn't read the message, it will be removed from their inbox. If they have opened the message, a recall message will make them aware that the message was not meant for them and they may delete it, although they won't be prompted to do so and may have already read the information.

- If you have sent an email containing personal data in error, you must report it immediately following GMSS's incident reporting procedures and to the GMSS Data Protection Officer (DPO) / IG team so it can be investigated. For further information relating to incidents please follow the Data Security Breach and Incident Reporting Policy which is located on the GMSS Website.

- Tidy up your contacts list and any distribution lists regularly to ensure out of date emails addresses do not pop up automatically and to ensure any leavers / authorised recipients are not included in the distribution list.

- Never disclose passwords or log on details to anyone, even a colleague. These details are confidential and must remain so.

- If you receive an unsolicited email containing an attachment or a link that you have not asked for do not open it or click on it as it as you could be subject to a phishing attack. This is where criminals or hackers sometimes use a link or attachment as a way to install malicious software on your computer.

- **Lastly: Always check the recipients email address is correct before you press send!**

Further information relating to email can be found in the GMSS Acceptable Use of IT Policy which is located on the GMSS Website.

9. Telephone Disclosures

There will be occasions when telephone enquiries are received asking for disclosure of personal confidential data. Where the caller has a legal right to access that information, the following rules should be adhered to:

- Verify personal details including the name, job title and organisation of the person requesting information.
- If the caller is part of an organisation / company, the main switchboard number of that organisation should be obtained and you should ring back.
- Conduct the call in an area that is private / confidential where staff / public cannot overhear – you could be talking about a relative / neighbour of a work colleague who is listening to your conversation.
- Any notes made during the calls should be kept in a secure place (locked away) and not left on any desk.
- If in doubt, the caller should be advised that they will be called back and where necessary, a senior manager or the designated authority for confidentiality issues should be consulted if necessary.
- Any suspect bogus enquiries should be referred immediately to the GMSS Data Protection Officer (DPO) / IG Team as soon as possible and the incident can be logged and dealt with accordingly.
- Always provide the minimum amount of information that is necessary.
- Provide the information only to the person who requested it and do not leave a message.
- Be aware of any press enquiries and refer to the communications team.

10. Transfers of data by post

The following rules must be followed when sending / receiving personal confidential data via post:

Incoming:

- Ensure incoming post is received in an environment away from public / unauthorised interference e.g. not left on desks or in a public area.
- Ensure if post is sorted for onward distribution that it is stored securely prior to dissemination and regular deliveries are made so there is no delay in receipt of the information for the receiver.

Outgoing:

- Check if you need to use a courier / “signed for” Royal Mail service to post to ensure receipt of delivery.
- Always double check the contact details / address of the recipient or the recipient’s representative.
- Ensure the recipient’s contact details are clearly labelled on the envelope / package.
- If the envelope contains confidential data, mark the envelope clearly as ‘Private and Confidential’.
- Use a GMSS letter headed front page or compliment slip.
- Use a secure robust envelope, include a return address where appropriate.
- For important letters / parcels, ask for confirmation of safe arrival.

11. Manual transfers of paper / hardcopy documentation

Paper records / documents / hard copies of electronic information may be required for investigation e.g. by a court or may be needed by another department or multi-disciplinary meeting.

The following rules must be followed regarding confidential paper documentation:

- Paper documents that contain confidential data must be stored in a lockable cupboard or cabinet prior to sending (if they have to be stored).
- Lockable crates must be used to move bulk hardcopy information.
- Only take off site the minimum amount of paper documentation that is necessary.
- Record what paper documentation is taken off site / from a department (particularly if this is patient information), where and to whom the information has gone to in a logbook.
- Ensure documents such as case notes / patient notes are properly 'booked out' of any relevant filing system if this system is in place.
- Never leave personal / sensitive / confidential records / documents unattended – ensure they are always stored securely when not required.
- Ensure the information is returned to its correct location as soon as possible and record that the information has been returned in the log. Or if you no longer need the paper documentation, ensure this is confidentially disposed of using the GMSS's confidential waste processes.

For further information on the security of paper documentation please refer to the GMSS's Records Management Policy (located on GMSS website) and the Records Management Code of Practice for Health & Social Care 2016 on the following link:

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

12. Transfers of data to Photocopiers / Printers

The GMSS has secure printers / photocopiers which require a unique code that identifies you in order for you to collect your printed documents. This code is entered when you are at the photocopier / printer and then you collect your documents securely whist at the printer. Please ensure that when you have printed your documents, particularly if these contain confidential information / personal data, that you check the output tray and do not leave any documentation behind. If there is no secure printing facility available, do not print unless this you are in a secure environment where unauthorised access to the printed material cannot occur.

13. Transfers of data via text message

Staff use mobile phones to text message other staff members regarding work activities. At the present time GMSS does not text patients. The following must be considered before any text messages are used.

- Check the mobile number is correct and be confident that the person using the recipients mobile is the person to whom the message is intended.
- Keep messages short.
- Do not transfer business sensitive or personal confidential data via text.

- Text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased). As mobile phones are easy to misplace or may get stolen, there is a risk of a breach of confidentiality. Mobile phone networks may be open to additional risks of interception.
- Remember, data sent via text message could be released via a Freedom of Information request and / or a subject access request.

14. Transfers of data using Portable Devices

The use of portable devices such as laptops, mobile phones, smartphones / tablets, USB memory sticks to transfer and store information for work purposes must be in line with GMSS policy and authorised by your line manager (and the GMSS IT Services provider, where appropriate).

- Only portable devices that are approved by GMSS and are encrypted to NHS standards (and where appropriate have up to date anti-virus software) can be used for work purposes to transfer data with and / or store data.

- Personally owned portable devices such as laptops, smart phones, smartphone/tablet devices must not contain work related information / information assets and must not be directly connected to the corporate network either by a direct network cable connection or Wi-Fi connection. However, such devices may be connected to the GMSS 'guest' Wi-Fi service in accordance with the full suite of Data Security (IG) policies.

- Data on laptops must always be stored on the secure network folders. When off site, you can access this via VPN / remote access token. Never store data on the local drive of a laptop, this is insecure.

- A staff member needs to complete the required approval forms and have it authorised by their Line Manager in order to be issued with a portable device. These are available on the ServiceNow portal.

- All security and encryption features on portable devices must be utilised such as username and password authentication. Where additional safeguards can be put in place they must be done so such as a minimum 4 digit PIN being allocated to a mobile phone.

- For any issues related to use of the portable device, staff members need to contact the IT Helpdesk.

- When staff leave GMSS, they must return any equipment provided by GMSS. This may be through a designated contact point at GMSS if not directly through the IT service.

15. Transfers of data by the NHS Secure Electronic File Transfer (SEFT) Service

Secure Electronic File Transfer (SEFT) works by providing a secure wrapper around any file, regardless of its size, structure or data content. SEFT provides data security during transmission (by using a 256-bit AES encryption mechanism). The data are

held in secure containers at NHS Digital and only people who are authorised to process the data are allowed access.

SEFT can only be accessed by registered and approved users. Further information can be found here https://digital.nhs.uk/services/transfer-data-securely

16. Transfer of information to cloud storage

'Cloud storage' is where you can upload documents, photos, videos and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet etc). Any changes made to these files are automatically copied across and immediately accessible from other devices you may have.

For work purposes, all data must be stored securely on network folders and these can be accessed remotely via VPN / token access when off site. However there may be occasions when you may need to use cloud storage. Always check with the GMSS IT Security Manager and / or the IT provider to see if this can be approved and also which cloud storage providers are approved to be used for the NHS. For more information about cloud storage, please visit the ICO pages at https://ico.org.uk/your-data-matters/online/cloud-computing/

17. Non Routine Bulk Transfers

Any non-routine bulk extracts (50+ records) or transfers of personal confidential or special categories of data must be authorised by the responsible manager or the Information Asset Owner for the work area and may require approval by the SIRO and / or Data Protection Officer.

18. Transfer of data via social media platforms

Transfer of business confidential information / personal data to social media platforms is not permitted. These platforms must not be used to transfer / store business information or discuss any work related issues.

19. Transfers of data via audio recordings

The recording of audio is a useful tool to record an event, for example, to record minutes of a meeting or review in order for accurate minutes / reports to be produced from this. If any meetings are to be recorded, only approved GMSS equipment must be used and those in attendance at the meeting must be informed. The recording must be deleted from the audio recording device as soon as practicable and the device must always be locked away when not in use. For further information, please visit the ICO pages at:
https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/audio-recordings/

20. Transfers of data via photography and video equipment

Use of digital photography and video recording provide a permanent record of an event for a range of different purposes. Such devices rarely contain the ability to encrypt images stored on the device. As a result there is a risk of unauthorised access if the device, or a removable memory card, is lost or stolen.

Therefore, it is important that images / recordings from a camera / recording device are

transferred to a secure location and the remaining content deleted from the memory card / device as soon as is practical.

21. Transfers of data overseas

If there are any occasions when you need to transfer business sensitive / personal confidential data overseas, always seek the advice from the Data Protection Officer and / or IG Team in the first instance. The security of the transfer and the recipient arrangements for security must be checked prior to any transfers being made.

22. Disposal / Deletion of data

All users must ensure that, where equipment is being disposed of, all data on the equipment / device is securely destroyed. This can be arranged by contacting the GMSS IT Service.

Any paper documentation that is no longer required following transfer must either be filed away securely and / or securely disposed of using the confidential waste bins across the GMSS office. Please ensure that you inform the Data Protection Officer / IG Team if the confidential waste bins are full so these can be emptied as soon as possible.

For further information regarding records management, please see GMSS's Records Management Policy.

23. Training and Awareness

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

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

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

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

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

24. 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.

25. Legislation & Guidelines

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

- Data Protection Act 2018 https://www.gov.uk/government/collections/data-protection-act-2018
- General Data Protection Regulation 2016 (GDPR) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- IG Alliance (IGA) https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga
- Records Management Code of Practice for Health & Social Care 2016 https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016
- Information Commissioners Office (ICO) https://ico.org.uk/
- The NHS Care Record Guarantee
- Independent Information Governance Oversight Panel, 2013 Caldicott 2 - Information: To Share Or Not To Share? The Information Governance Review
- National Data Guardian, 2016 Caldicott 3 - Review of Data Security, Consent and Opt-Outs
- Guidance on sending a secure email from an NHS Mail Account to a non NHS Mail account https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC_Sending%20an%20encrypted%20email%20from%20NHSmail%20to%20a%20non-secure%20email%20address.pdf
- British Medical Association – GDPR Guidance https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr
- Data Security and Protection Toolkit (DSPT) https://www.dsptoolkit.nhs.uk/
- Guidance regarding the Law Enforcement Directive https://ico.org.uk/for-organisations/guide-to-law-enforcement-processing-part-3-of-the-bill/
- The National Cyber Security Centre - Creating passwords
- The National Cyber Security Centre - Password Managers

26. 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.

27. 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.