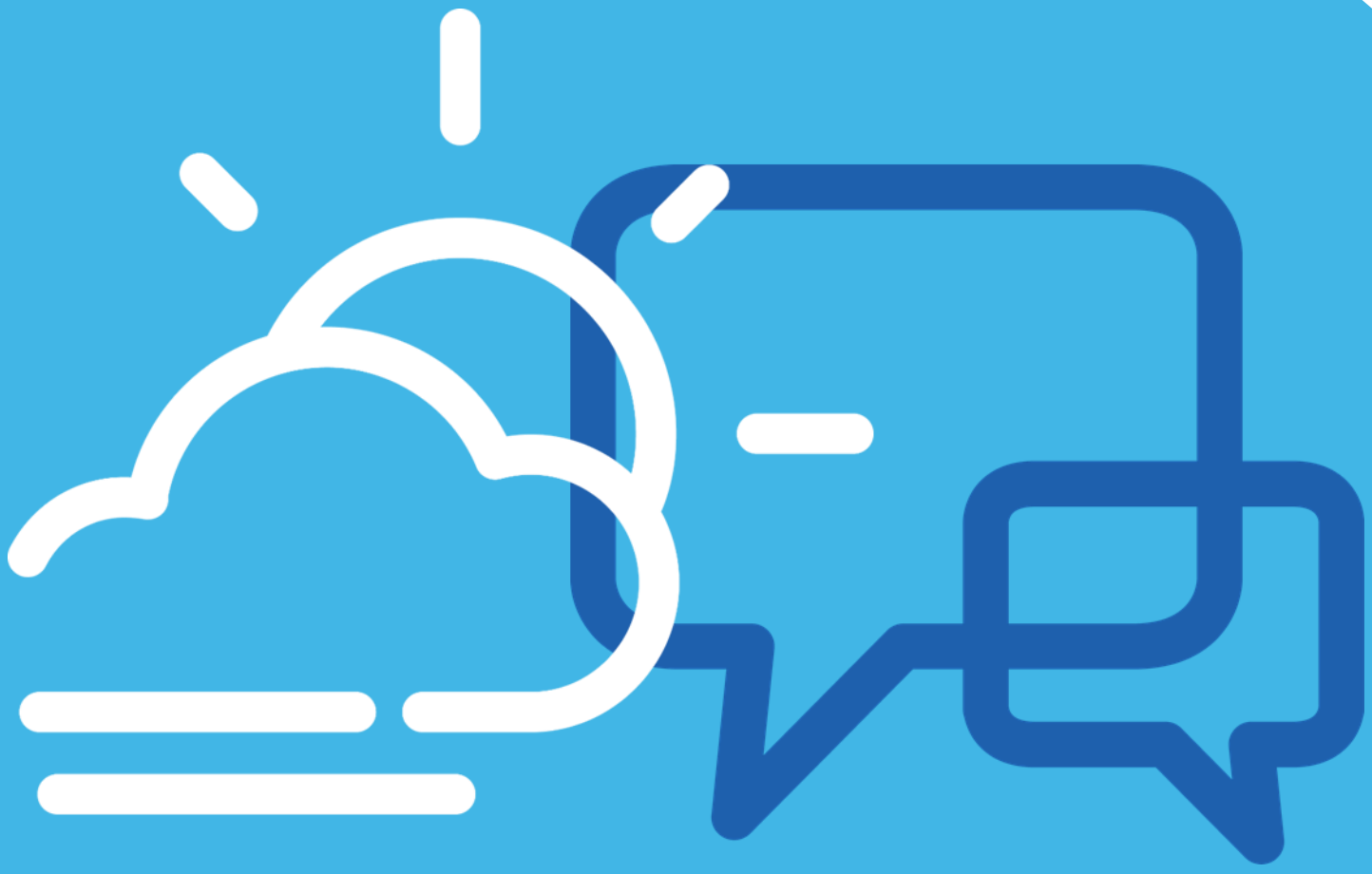
NHS
Greater Manchester Mental Health
NHS Foundation Trust

Safe Haven Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	Safe Haven Policy
Executive Summary:	This policy provides the basis for the standards and procedures adopted when personal information is transferred between staff, departments and partner organisations either in digital or hardcopy format.
Executive Lead:	Director of Finance, Capital and IM&T
Document Author:	Sarah McDonald (Head of IM&T Service Delivery)
Document Purpose:	Policy
Target Audience:	All employees of Greater Manchester Mental Health NHS Foundation Trust and partners.
Additional Circulation List:	N/A
Date Ratified:	15/01/19
Ratified by:	Information Governance Steering Group
Consultation:	Representatives from all directorates via membership of the IGSG.
Cross Reference:	Related trust policies and procedures including the Internet and email usage policy Incident Accident and near miss policy
Superseded Docs	Safe Haven Policy IG12 V1.0
Date of Equality Impact Assessment:	November 2018
Board Objective Reference:	Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes Objective 3 – To engage in effective partnership working Objective 4 – To invest in our environments Objective 6 – To achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Regulation 15 – Premises & Equipment Regulation 17 – Good Governance
Risk Register Reference:	N/A
Contact Details for further information	Head of IM&T Service Delivery Sarah.Mcdonald@gmmh.nhs.uk 0161 358 1751
Document Status	This is a controlled document. Whilst this document may be printed, the electronic version posted on the Trust intranet is the controlled copy.

Contents

1. Introduction

The Trust is required to have a Safe Haven Policy to ensure that the transfer of person identifiable information into and out of the Trust and within the Trust between departments and sites, is as secure as possible.

1.1. Purpose

This policy is intended to:

- protect the information processed by GMMH;
- meet the requirements of the Caldicott Guardian as outlined in the Caldicott Report, ensure compliance with relevant legislation including General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and
- satisfy the requirements of the Data Security and Protection toolkit.

This policy forms part of the Trusts compliance with Principle 6 of General Data Protection Regulation *'Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental losses'.*

1.2. Scope

This policy covers all person identifiable information which may relate to staff, service users, carers or third parties held and used by the Trust.

Person identifiable information is any information which on its own or in conjunction with other information would allow an individual to be identified, this would include but not is not limited to name, address, date of birth, NHS Number, NI Number, description, photograph, etc.

All forms of data processing means are governed by this policy, including but not limited to, phones, fax, electronic records, paper records etc.

2. Definitions

General Data Protection Regulation - The General Data Protection Regulation sits within the Data Protection Act 2018. It is the legislation that provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers all staff records. It expands the rights of individuals to control how their personal data is collected and processed, and places a range of new obligations on organisations to be more accountable for data protection.

There are six principles identified under GDPR that set out standards for information handling and sets the foundation for personal data to be:

1. lawful, fair and transparent;
2. limited for its purpose;
3. adequate and necessary;
4. accurate;
5. not kept longer than needed;
6. integrity and confidentiality (security).

GDPR also details a separate accountability principle which details organisations' responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate compliance and accountability.

Additional definitions:

Breaches and penalties - Under GDPR fines of up to 20 Million euros, or 4% of turnover, can be levied and criminal convictions imposed on the individual and/or organisation responsible.

Caldicott Report – A code of conduct produced from a report written by Dame Fiona Caldicott in 1997 and updated in 2014. The report highlighted seven key principles, regarding the ways in which patient information is used in the NHS in England and Wales. The guidelines ensure that confidentiality is not undermined during the development of information technology in the NHS.

Common Law – refers to law and the corresponding legal system developed through decisions of courts and similar tribunals, rather than through legislative statuses or executive action.

Data Protection Act 2018 - The Data Protection Act 2018 supersedes the Data Protection Act 1998.

Data Protection Officer - The GDPR introduces a legal duty to appoint a Data Protection Officer (DPO) for all public authorities and organisations that carry out certain types of processing activities.

DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (Information Commissioner's Office (ICO)).

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The Trust's DPO will help demonstrate compliance and is part of the enhanced focus on accountability within the Trust.

Legislation – a law or laws passed by an official body.

NHS Code of Practice: Confidentiality – The Code's purpose is to provide

guidance to the NHS-related organisations on patient information confidentiality issues.

Personal Information/Person Identifiable Data – Personal Information is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private, e.g. name and private address, name and home telephone number etc.

Safe Haven – a location or department, (or in some cases a piece of equipment), situated on trust premises where arrangements and procedures are in place to ensure person identifiable information can be held, received and communicated securely.

Sensitive personal information – The General Data Protection Regulation classes certain information as sensitive, this could be where the personal information contains details of criminal records, health information, political views, racial origin, sexual life, Trade Union membership or religious beliefs. For this type of information even more stringent measures should be employed to ensure the data remains secure.

Special Category data - Replaces the term Sensitive personal data under GDPR and applies to the following:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Trust – Greater Manchester Mental Health NHS Foundation Trust.

3. Duties

Data Security is the responsibility of all staff members.

3.1. Chief Executive (CEO)

The CEO has overall responsibility and will delegate responsibility for the oversight and implementation of information asset management to a Director on the Board of GMMH. This Board member will be appointed as the Senior Information Risk Owner.

3.2. Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (Director of Finance, Capital and IM&T) acts as an advocate for information risk on the Board and in internal discussions will provide written advice to the Chief Executive on the content of the Annual Statement of Internal control in regards to information risks.

3.3. Caldicott Guardian

The appointed Caldicott Guardian (Medical Director) for the Trust must approve all procedures that relate to the use of patient information.

3.4. Information Asset Owners (IAO)

Nominated IAOs are responsible for safe havens within the service they work and are expected to take ownership of, and seek to improve, safe havens within their services.

3.5. Information Asset Assistants (IAA)

IAAs are responsible for assisting and supporting IAOs and Managers within the organisation to ensure that this policy is built into local processes and that there is ongoing compliance.

3.6. Managers

Managers are responsible for ensuring this policy is built into local processes and that there is on-going compliance and improvement.

3.7. Information Governance Manager

The Information Governance Manager based at the Trust is responsible for co-ordinating improvements in: data protection, the confidentiality code of conduct, and information security. The Information Governance Manager is assisted by the Information Governance Team.

3.8. All Staff

All staff are required to comply with Information Governance requirements including

the Safe Haven Policy, e.g. staff who work with person identifiable and/or sensitive information which is received or transmitted as securely and confidentially as possible.

3.9. Data Protection Officer (DPO)

A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). The data protection officer is responsible for overseeing data protection and Information Governance strategy and implementation to ensure compliance with GDPR requirements. The DPO will monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for all data subjects including the Safe Haven Policy.

4. Processes and Procedures

4.1. General Principles

Safe Haven procedures should be in place in any location personal information is being received, held or communicated especially where the personal information is of a sensitive nature, e.g. Service user information.

Before transferring personally identifiable information anywhere always consider the following:

1. Is the transfer of information necessary in a personal identifiable form – follow the Caldicott principles?
2. Has the appropriate consent been obtained?
3. Is the transfer legal?
4. Have you established that the intended recipient needs this information and is entitled to see it?
5. Does the recipient have an obligation similar to yours to protect the information? Refer to the Information Sharing Protocol.
6. If in doubt discuss the transfer with your line manager, or contact the information governance team.

4.2. Location/Security Arrangements

A safe haven is often a dedicated physical space; where this is the case the following considerations should be noted:

- it should be a room that is locked or accessible via a coded key pad known only to authorised staff;
- the office or workspace should be sited in such a way that only authorised staff can enter that location, i.e. it is not an area which is readily accessible to any members of staff who work in the same building or office, or any visitors.
- If sited on the ground floor, any windows should have locks on them and a

review should be undertaken to ensure that information cannot be viewed from the window.

- The room should conform to health and safety requirement in terms of fire, safety from flood, theft and environmental damage.
- Manual paper records containing person identifiable information should be stored in locked cabinets. Do not leave medical notes unattended at any time.
- Computers should not be left on view or be accessible to unauthorised staff; the screen should be locked or the computer logged out off when not in use.
- Equipment such as fax machines in Safe Havens should have a code password or be manned at all times, and equipment should be turned off out of office hours.

4.3. Email

ALL personal identifiable data (PID) must be removed from emails and a unique identifier such as the NHS number or PARIS ID used. In exceptional circumstances where PID may be required the email must be encrypted. See the internet and email usage policy regarding how to encrypt internal emails.

GMMH.nhs.uk to GMMH.nhs.uk is a secure system however any email sent that includes person identifiable data must be encrypted. All external emails containing PID must also be encrypted. See the internet and email policy regarding how to encrypt emails sent externally.

NHS.net to NHS.net is a secure system. All external emails containing PID must also be encrypted e.g. NHS.net to GMMH.nhs.uk must be encrypted following the NHS.net encryption guidance.

4.4. Answering Machines

Where an answer phone is likely to receive messages which may be deemed to be confidential, e.g. where callers leave their personal details (such as names and addresses), the messages should be checked and transcribed in a location where they cannot be overheard. The answer phone should be protected by pin number access or be in a locked room when unattended to prevent unauthorised access.

4.5. Fax Machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following rules must be applied:

- the fax is sent to a verified ‘Safe Haven Fax’ location where only staff that have a legitimate right to view the information can access it.
- The sender is certain that the correct person will receive it and that the fax number is correct.
- The recipient is notified when the fax is being sent and is asked to acknowledge receipt.

- Care is taken in dialling the correct number.
- Confidential faxes are not left lying around for unauthorised staff to see.
- Only the minimum amount of personal information should be sent, where possible data should be anonymised or a unique identifier used.
- Faxes sent should include a front sheet, which contains a suitable confidentiality clause. See appendix E.
- A dedicated member of the team ensures all incoming faxes have been claimed and not left on the fax. All efforts must be made to ensure the intended recipient receives the fax. Where the intended recipient is not available the information must be given to a deputy to ensure business continuity.

4.6. Communication by Post

Once the information is received from Royal Mail or other sources it should be protected from theft, unauthorised access whether accidental or malicious, and damage.

All sensitive records must be locked away when not in use. When in use they must be stored face down in public areas and not left unsupervised at any time.

In-coming mail should be opened by a designated person with post responsibility and not left on peoples desks; the post must then be date stamped and actioned accordingly by the relevant person. Where post has been opened on behalf of the intended recipient it must be stored where no-one can gain unauthorised access. Procedures should be in place to cover staff who have left or are away and whose post may need to be opened.

There may be times when post addressed to GMMH will be marked as 'Confidential' by the sender. If the person to whom the letter is addressed to is not available, it is a manager's decision whether or not to open the letter.

Items marked 'Private and confidential' or 'To be opened by addressee only' may only be opened by the addressee. It is reasonable to expect that staff may receive private correspondence in the line of their duties, e.g. Wage slips, letters from HR etc. However under no circumstances is it permitted for staff to have private mail, (not in the line of their duties), sent to a GMMH address. This includes letters and parcels of a personal nature, e.g. orders from a website such as eBay. **The Trust reserves the right to open all mail addressed where it suspects this type of activity has occurred. Please contact the Information Governance Manager for further advice.**

4.7. Monitors/Screens

All monitors/screens should be 'locked' if the equipment is to be left logged in and unattended for short periods of time, e.g. leaving your desk for a short period of time.

A password protected auto lock screen saver is in place on all trust PCs.

When not in use all laptops and PCs must be logged off and shut down by the user.

The Trust has an automatic shutdown facility in place. At 7:30pm every evening any machines that have been inactive for 30 minutes or longer will automatically be logged off. This function does not replace user responsibility to log off and shut down (it is a checking mechanism). If the machine has not been logged off by the user and automatic shutdown is activated any work not saved will be lost. The IT department will keep a log of all machines shut down via the automatic shut down for investigation and escalation by the Information Governance Manager and where appropriate the Senior Information Risk Owner.

4.8. Printers

Printers will be situated in a secure location where only authorised staff can access the printer. At the end of every working day/shift any documents left on the printer must be either locked away for safekeeping if it is known who they belong to. If it is not known who the information belongs to it must be placed in the confidential waste.

4.9. Safe Haven Procedures

Please refer to:

- Appendix A for Incoming Communications.
- Appendix B for Outgoing Communications.

4.10. Incident Reporting

Staff should compete incident reporting in line with the GMMH overall incident reporting processes as soon as possible via Datix, as per the Trusts Incident, Accident and Near Miss Policy.

The key points from the Incident Reporting and Investigation procedure are summarised below:

- all incidents must be reported immediately by the member of staff involved, using DATIX, which must be checked, graded and signed off by their line manager before being input via DATIX WEB or sent to the Risk Management Team within 24 hours for recording in the DATIX system;
- the SIRO will ensure that external bodies are notified in accordance with their individual requirements;
- all incidents will be investigated to an extent commensurate with their potential severity;
- as a minimum, the line manager should consider whether appropriate action has been taken, whether any lessons can be learned from identification of root or contributory causes, and whether any further action is necessary. This should be recorded on DATIX;

- for more serious incidents, a Team Management Review (TMR) and Root Cause Analysis must be carried out and the incidents will be recorded on the Data Security and Protection toolkit and this will send them directly to the ICO for further investigation.

Example incidents
Misdirected fax – fax sent to incorrect recipient.
Misdirected fax – In receipt of information not intended for you.
Incorrectly addressed post.
In receipt of incorrectly addressed post.
Overheard conversation – sensitive details being discussed in public.
Inappropriate access - Unauthorised access to secure network folder or systems.

5. Training Requirements

Please refer to the Trust Mandatory Training Matrix for full details.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
Data Flow Mapping	Quarterly	Report to IGSG	Minutes	Information Governance Manager	Information Governance Steering Group
Audit	Ad hoc	Audit	Reports	Information Governance Manager	Information Asset Owner
Incidents	-	Reports	Minutes/ Reports	Information Governance Manager	Information Governance Steering Group/ Information Asset Owners

7. Resource/Implementation Issues

The current Information risk hierarchy in place across the Trust including the SIRO, IAOs and IAAs and will support the implementation of this policy. The IG team will support all directorates and provide ad-hoc training where required.

8. Risk Issues

The Information Governance team complete an annual Data Flow Mapping report highlighting the risks with regards to sending and receiving information across the Trust.

Non-compliance with this policy could result in a data breach which may attract a substantial financial penalty for the organisation and seriously damage the Trust's reputation.

9. Requirements, Supporting Documents and References

9.1. Requirements

Board Objective Reference:	Objective 1 – To promote recovery by providing high quality care and delivering excellent outcomes Objective 3 – To engage in effective partnership working Objective 4 – To invest in our environments Objective 6 – To achieve sustainable financial strength and be well-governed
CQC Regulation Reference:	Regulation 15 – Premises & Equipment Regulation 17 – Good Governance
Other requirements:	General Data Protection Regulation Data Protection Act 2018 Freedom of Information Act NHS Risk Management Strategy

9.2. Supporting Documents

- Information Governance Staff Handbook
- Email and Internet Usage Policy
- Incident Accident and Near Miss Policy

9.3. References

- Information Governance Policy
- Information Governance Staff Handbook Data Quality Policy
- Records Management Policy Information Security Policy
- Information Asset Management Policy.

10. Subject Expert and Feedback

Head of IM&T Service Delivery
Sarah.Mcdonald@gmmh.nhs.uk
0161 358 1751

11. Review

Trust policy for review is every five years, however this policy will be reviewed annually in line with the Data Security and Protection Toolkit, or sooner in the light of organisational, legislative or other changes.

12. Appendices

See following pages.

Appendix A – Incoming communications/information

1 Faxes

1.1 The fax machine should be located so that access is restricted and controlled. (Going forward Fax machines will be removed and Electronic Faxing Technology will be in place, which will be more secure).

1.2 A nominated member of staff in each area will be charged with the responsibility of handling and distributing confidential faxes to the appropriate recipient(s).

1.3 A designated person will be responsible for ensuring all documents received via fax are distributed by the end of the working day/shift and not left on the fax machine.

1.4 During periods when the premises are unattended by GMMH staff, access to fax machines should be restricted. Where this is not possible, the fax machine should be switched off.

The Trust will take every opportunity to notify partner organisations of its arrangements for the receipt of safe haven faxes, including, where appropriate, the times at which faxes may be received in a secure manner.

2 Telephones

2.1 Confidential information may be received by telephone from a range of sources (partner organisations, patients and relatives etc.).

2.2 It is likely to be impractical to provide separate facilities for the receipt by telephone of such information and therefore the recipient should take steps to ensure that confidentiality is not breached when receiving such calls.

2.3 Appropriate steps include:

- Ensuring, through awareness training, that only GMMH staff authorised to do so accept and receive confidential information by telephone.
- Ensure that you cannot be over-heard if you are obliged to provide confidential information (e.g. repeating names, addresses, checking spelling etc.)
- Ensure that, if making notes or recording information, it cannot be seen by unauthorised persons.

3 Post

3.1 Post received by GMMH will be processed in a secure area.

3.2 A nominated member of staff will be responsible for the distribution of post.

3.3 Any post marked as ‘To be opened by addressee only” or other such marking indicating a requirement of confidentiality will only be opened by the addressee. (E.g. wage slips)

3.4 Undeliverable post of a confidential nature is returned to sender.

3.5 Admin staff at Trust HQ will ensure all post returned as undeliverable via the PO Box return address is processed in a 'safe haven' environment and sent on to the intended recipient or where the recipient can't be identified returned to sender.

4 E-mails

4.1 Person Identifiable information should only be sent in email if absolutely necessary – this needs to be encrypted.

5 Verbal information

5.1 Confidential and sensitive information may also be received by "face to face" contact. In such circumstances the guidance given below should be followed:

- Provisions should be made which enable sensitive information to be given verbally in a secure and confidential manner. This consists primarily of a room or area in which information may be divulged or discussed without risk of being overheard by unauthorised persons.
- If it is suspected that confidential information is about to be verbally imparted to the organisation the individual concerned should be advised of the arrangements for such disclosures.

6 Network Drive Location

6.1 Any person identifiable information (including patient or staff information) that is received and stored on the network must be stored on a network drive securely and in a designated folder that has access restricted to only those who need to access the data in order to perform their role. This acts as a safe haven.

No person identifiable information should be stored directly on the PC/laptop/desk top/tablet/etc.

6.2 Safe Haven folders should have access restrictions imposed by Support Central and Support Central should be advised that new access requests for that location must be approved by the Information Asset Owner of that directorate (Assistant Director). Once authorised the completed request form (Appendix D) should be sent to IM&T Support Central.

Appendix B – Outgoing communications/information

1 Faxes

The key elements are:

- Determine whether or not the receiving fax is a Safe Haven fax.
- If it is not, ensure that the recipient waits by the fax machine during transmission of the information, (a new Electronic Faxing System will be in place, which is more secure).
- Double check the fax number before sending the information
- Use the stored number facility for regularly used recipients.
- Ask the recipient to confirm receipt.
- Ensure there is a cover page with the fax that clearly states who the fax is being sent to.
- The sender is to ensure their contact details are included in the fax cover sheet. Please see appendix E for a fax cover sheet.

2 Telephones

2.1 The use of telephones to give out confidential information raises the issue of confirmation of the identity of the recipient. Sensitive information should not be given by telephone in circumstances where the identity of the recipient cannot be established with absolute certainty.

2.2 In addition, notwithstanding confirmation of the recipient's identification, the caller should satisfy themselves that the recipient is authorised to receive the information.

2.3 Where it is necessary to transfer confidential information by telephone between two parties on a regular basis, a password protocol, known only to authorised personnel, should be implemented.

3 Post

3.1 All post must be addressed to a person within a team rather than just a team name. If any doubt exists about the recipient's details, confirmation should be sought prior to dispatch of the information.

3.2 The envelope must have the Trust P.O. Box address stamped on the back.

3.3 Advice should be sought from the Information Governance team or the Assistant Director of Information Management & Technology in relation to the transfer of bulk data (classified as 51+ items/files containing personal details)

3.4 If mobile media is to be used to dispatch information the media must be encrypted.

3.5 If posting a copy of a medical record or information of a particularly sensitive nature that would not usually be in the public domain such as board reports in

advance of a scheduled board meeting. Information of this nature must be sent via special delivery or via the Trust approved Courier Company. This type of service offers a fully auditable tracking system and requires the addressee to sign for the package upon delivery.

4 E-mail

4.1 The secure government email systems (NHS Mail, GSI etc) can be used to securely exchange emails of a sensitive or personal nature. The following steps must be taken to ensure the correct recipient is used:

- Verbally confirm with the recipient what their secure email address is.
- Send a test message to ensure you have typed the correct email address and state which organisation they work at. NHS emails are formatted using the recipients first name and family name, however as there maybe more than one person with the same name you must ensure you state the organisation also. e.g. joe.bloggs@nhs.net

  'Hi Joe, this is Mary from GMMH. Can you confirm this is the correct email address for Joe at Bolton CCG?'

4.2 Confidential information should not generally be sent by email unless it is encrypted.

4.3 Confirm the email address of the recipient ensuring that you understand the spelling of any awkward words, and if necessary (e.g. the address has not been used previously or has not stored electronically after verification) send a test message.

4.4 The subject window must not contain person identifiable information. It is advisable to use the subject line to describe the subject of the email rather than who the email is about e.g. Salary resolution, service user care package.

4.5 Confidential information should not be sent to shared or group email boxes unless staff are completely sure of the group members and their security arrangements.

4.6 When emailing outside of the organisation, consider converting any attachment to a PDF File to ensure that it cannot be edited. Adobe Writer is required in order to do this. A document could also be set to 'Read Only' in Word (Tools/Options/Security/Password to Modify).

5 Verbal Information

5.1 Where confidential information is to be imparted on a "face to face" basis, the providers of the information should satisfy themselves that the recipient is authorised to receive the information.

5.2 Sensitive Information should only be given verbally when it may be done so in a secure and confidential manner. In general this requires facilities in which confidential information may be discussed without fear of being overheard by unauthorised third parties.

6 Text Messaging

6.1 The use of text messaging can be valuable in certain services but criteria must be agreed in advance with the patient/client as to the content and circumstances when this method of contact will be used.

Any requests to use text messaging must be authorised via the Privacy Impact Assessment process before the project is implemented.

7 Network Drive Locations

7.1 Patient Identifiable data should only be sent outside of the safe haven location for Direct Care purposes (where there is a risk if the information is not received) and should conform to the procedures set out for the transmission methods above.

7.2 Patient Identifiable data for Secondary Uses should not be sent outside of the safe haven location.

There are two options for transmissions of data for Secondary Use:

- The first is to suitably anonymise the data so patients are not identifiable.
- The second, for where patient level data (but not identifiable data) is required, is to pseudonymise the data so individual records can be viewed which do not identify the patient. The Pseudonymisation must be approved and performed by the Business Intelligence team.

8 SharePoint

8.1 SharePoint can be used as a secure location for document management. Where possible SharePoint should be used by staff to communicate meeting agendas, minutes, data quality reports etc. with other GMMH staff rather than sent via email. Safe Haven areas can be created on SharePoint which allows the secure sharing of information by granting authorised staff access to the information via a password log in. This removes the need to ‘send’ information via other means e.g. email/post.

8.2 Authorised access groups must be established to ensure only authorised personnel can access specific areas within SharePoint. To establish a SharePoint area which contains person identifiable information/corporate sensitive information a Privacy Impact Assessment must be completed and authorised (PIA templates can be located on the IG pages of the intranet, once complete these must be authorised by the IG team).

9 Display Boards

9.1 Boards containing patient information should only be sited in areas that are solely accessible to those who are required to see/use the information. A risk assessment should be undertaken which includes assessing the risk of patient information being disclosed.

Appendix C – Safe Haven Access Process

Network folder access request

The Trust has already established Safe Haven network folders these are folders that have restricted access to only those staff with a justified reason for access, e.g. the Information Governance (IG) team may have shared folders which are only accessible by IG and some folders which are only accessible to the Information Governance Manager only as the nature of the information stored could be sensitive and confidential.

The access request form below will be used for any new access requests to Safe Haven locations. For example this may be a new member of staff, or a member of staff changing roles or taking on further responsibilities, though other valid circumstances may exist. Also, should a member of staff already have access to a Safe Haven and move job roles, this access should be reviewed by the line manager and revoked if appropriate.

Process

When a need for new access to an identified Safe Haven location arises, the direct line manager of the employee should complete the attached form and obtain approval from their Information Asset Owner (deputy/assistant director) if different from the line manager.

The form should then be sent to Support Central and logged as a job. The forms will be kept as a record of access by the IT Department. The Support Central team will then implement the request.

If you believe a new Safe Haven location needs to be set up, please complete the New Safe Haven Folder request form located on the intranet (Appendix D). The Database Approval Form will need to be completed and signed off by the Information Asset Owner.

Appendix D – Safe Haven Access Request Form

Greater Manchester Mental Health NHS Foundation Trust

Name of Employee	
Job Role	
Base Location	
Full Network Location(s) for which access is required (e.g. (\\pioneer\data\IMT(N))	
Why is this access needed? (E.g. is there a specific task the employee is required to do that requires this data?)	

Access Level Required: Please tick

Supervisor ☐ Read ☐ Write ☐ Create ☐ Erase ☐ Modify ☐

File Scan ☐ Access control ☐

I confirm that I have read and understood the Procedure for requesting new access to a network drive location that contains Person Identifiable or Sensitive Information (Safe Haven).
Applicants signature: _____

Signature (Line Manager):		Date:
Name:		
Job Title:		
Tel:		

TO BE COMPLETED BY THE INFORMATION ASSET OWNER:

Approved: Yes / No

IAO signature: Date / /

Once completed please log a job with support central

Appendix E – Fax Cover Sheet

Greater Manchester Mental Health NHS Foundation Trust

Fax Cover Sheet

To:

Department:

Company:

Fax number:

From:

Department:

Company: Greater Manchester Mental Health NHS Foundation Trust

Telephone Number:

Return Fax Number:

Number of pages including cover sheet:

Message:

Do not state any specific details on this section
e.g. 'Please see details as discussed attached, I look forward to your response' or 'Please see enquiry attached'

The information contained in this fax is intended only for the use of the individual or entity to which it is addressed, and may contain information that is PRIVILEGED, CONFIDENTIAL and exempt from disclosure under applicable law. If you have received this message in error, you are prohibited from copying, distributing, or using the information. Please contact the sender immediately using the details provided above who will arrange collection of the information. Remember that faxes sent or received by our staff may be subject to disclosure under the Freedom of Information Act.