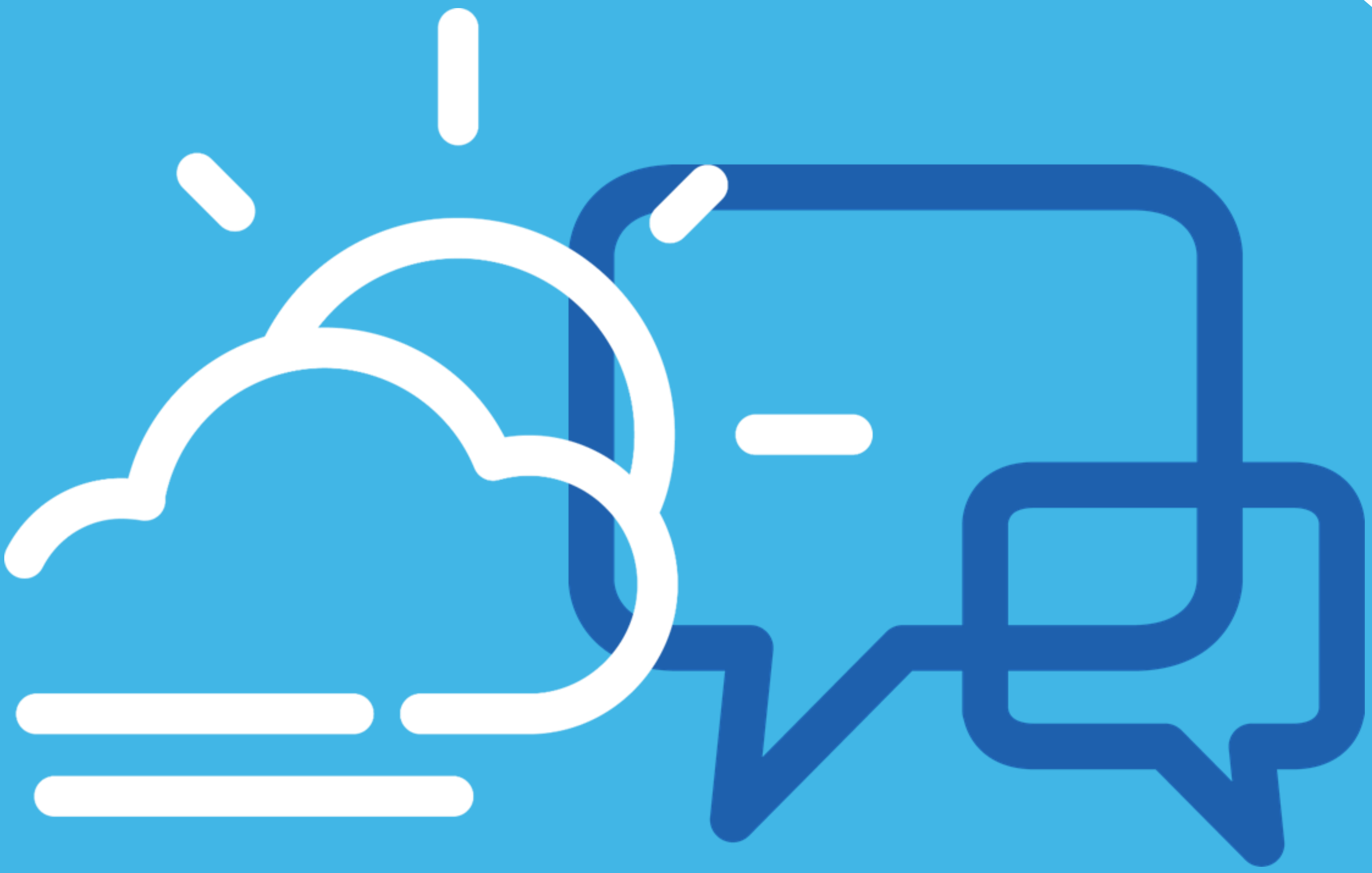
NHS
Greater Manchester
Mental Health
NHS Foundation Trust

Email and Internet Usage Policy

Greater Manchester Mental Health NHS Foundation Trust



Improving Lives

Document Name:	**Email and Internet Usage Policy**
Executive Summary:	This policy provides the basis for the standards and procedures to be adopted when using the Trust email and Internet systems to ensure that all GMMH staff are aware of the acceptable trust standards.
Executive Lead:	Ismail Hafeji, Director of Finance, Capital and IM&T
Document Author:	Sarah McDonald (Head of IM&T Service Delivery)
Document Purpose:	Policy
Target Audience:	All staff, contractors and third parties using email and intranet services.
Additional Circulation List:	Information Governance Steering Group, IAA, IAO.
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 Information Security Policy
Superseded Docs	Former GMW Email and internet usage policy
Date of Equality Impact Assessment:	17/10/18
Board Objective Reference:	3 – To engage in effective partnership working 5 – To enable staff to reach their potential & innovate 6 – To achieve sustainable financial strength & be well-governed
CQC Regulation Reference:	17 – Good governance
Risk Register Reference:	N/A
Contact Details for further information	Information Governance Team Sarah McDonald (Head of IM&T Service Delivery) Sarah.mcdonald@gmmh.nhs.uk Tel: 0161 3581751
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

Email and Internet are important business communication tools which, when used responsibly, provide many benefits to the Trust. Unfortunately if used inappropriately emails and Internet can be damaging to an organisation, therefore all Greater Manchester Mental Health NHS Foundation Trust (GMMH) staff need to be aware of their responsibilities. This document defines the email and Internet policy for GMMH.

1.1 Purpose

This document establishes the organisational and user responsibilities for the Trust email and Internet system.

1.2 Scope

The email and Internet policy applies to all users of GMMH email and the Internet system and the relevant people who support the system.

2. Definitions

2.1 Definitions and abbreviations

DPA	Data Protection Act 2018
DPO	Data Protection Officer
GDPR	General Data Protection Regulation 2018
IAA	Information Asset Assistant
IAO	Information Asset Owner

2.2 Email, Skype for Business, Internet and Intranet

Email is a system for sending and receiving messages electronically over a computer network or between personal computers.

The Internet is a massive network of networks (a network infrastructure). It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet.

The World Wide Web is a way of accessing information over the medium of the Internet. It is an information-sharing model that is built on top of the Internet.

The Trust Internet is our public website published on the World Wide Web. It is accessible to everyone with Internet access. Publication on the Internet means staff can access the information from home or from any Internet linked computer.

The term Intranet refers to a website with restricted access, published on secure networks, not the World Wide Web.

Skype for Business or skype are instant message systems used within the trust, this communication method is also included in this policy.

2.3 GDPR

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.

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' responsibilities for complying with the principles, and to have appropriate processes and records in place to demonstrate compliance and accountability.

Breaches and penalties
Under GDPR fines of up to 18 Million euros or 4% of turnover can be levied and criminal convictions imposed on the individual and/or organisation responsible.

3. Duties

3.1 Board/Lead Committee

The board is responsible for ensuring that all required policies and procedures are in place and available to staff and others.

The Information Governance Steering Group is the lead committee and is the accountable body responsible for the ratification of this policy.

3.2 Chief Executive Officer

The CEO is responsible for identifying a lead for email and intranet usage. This is the Director of Finance, Capital and IM&T.

3.3 Director of Finance, Capital and IM&T

The Director of Finance, Capital and IM&T is the accountable officer for the Trust.

The Director of Finance and IM&T is responsible for ensuring that the policy for email and intranet usage is up to date, relevant and is accessible for users. This responsibility is designated to the Associate Director of IM&T.

3.4 Associate Director of IM&T / Data Protection Officer

The GDPR introduces a legal duty:

- to appoint a Data Protection Officer (DPO) for all public authorities, and
- on organisations that carry out certain types of processing activities.

The Associate Director of IM&T is the Trust's nominated lead DPO.

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 (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.

3.5 Managers

Managers must ensure that this policy is made available to their team and are responsible for ensuring that all staff read and understand this policy; this should be checked at team meetings.

3.6 Employees

Access to the Internet is provided primarily for work-related purposes, including research related to studies approved by the Trust and professional development and training.

In addition to responsibilities for appropriate use of the internet in the workplace, staff are required to ensure that any information they publish on the internet including social media, does not pose a risk of damage the reputation of the organisation or breach the confidentiality of individual members of staff and/or patients.

In relation to email, this is just another method of communication; it can sometimes be difficult to establish the tone of an electronic message, the Trust expects staff to use email in the same manner as memos/letters and maintain a professional approach. As a general rule, emails should be written as if they were on Trust headed notepaper.

All staff must adhere and abide by the Email and Internet Access Policy. All staff should have an understanding of their responsibilities and the risks associated with the use of email and Internet.

4. Processes and Procedures

4.1 Email, Skype for Business and Internet Usage

Staff ID photographs will be uploaded onto the active directory to be viewed on email and Skype for Business within the Trust. Photographs will not be visible outside of the Trust and will not be attached to emails. Staff may request a new photo for this purpose if they so desire.

4.1.1 Inappropriate use of Email, Skype for Business and Internet

No member of staff is permitted to access, display, or download from Internet sites that hold ‘offensive’ material; to do so is considered a serious breach of security and conduct and may result in dismissal. Examples of what is considered offensive material include: hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political beliefs and disability. This list is not exhaustive. Other than instances that demand criminal prosecution, your employer is the final arbiter on what is or is not offensive material or what is or is not permissible access to the Internet.

Copyrighted material must only be used in accordance with the laws that protect copyright, designs and patents.

Use of the Internet facility for commercial activities other than in the conduct of Trust business is prohibited.

Staff are prohibited from using email to engage in activities or to transmit content that could be deemed as harassing, discriminatory, menacing, threatening, obscene, spreading rumours, and defamatory or in any way objectionable.

It is unacceptable to:

- send, solicit, print, copy and/or reply to text images or jokes that disparage others based on their race, religion, colour, sex, sexual orientation, nationality, disability or age;
- send, solicit, print, copy and/or reply to messages that are disparaging or defamatory;
- send aggressive and/or harassing messages that may cause fear, stress or anxiety to colleagues, clients or others;
- spread gossip, rumours and/or innuendos about employees, clients, suppliers or other outside parties;
- send, solicit, print, copy and/or reply to messages that contain sexually oriented images or foul, obscene or adult-oriented language;
- send, solicit, print, copy, and/or reply to messages or images that are intended to alarm others, embarrass the trust, negatively impact on employee productivity, or harm employee morale.

Internet usage is monitored and controlled by web site filtering. The broad categories of blocked websites are shown in Appendix 1.

4.1.2 Profile pictures

Staff must only use photographs that are appropriate as their profile pictures on Trust systems. The photographs are used as an extra checking mechanism to ensure the person contacting you is contacting the correct person and, as such, the photograph must be of the appropriate staff members face in a professionally acceptable circumstance.

It is unacceptable to use photographs of family members or inanimate objects.

4.1.3 Sending Person Identifiable Data via 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 Appendix 4 for guidance on 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. Please see Appendix 5 for guidance on how to encrypt emails sent externally.

NHS.net to NHS.net is deemed to be 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.

4.2 Planned and Unplanned absence

Staff are advised not to save any personal emails within their work inbox. During planned absence, e.g. where staff members are on annual leave, then it is the staff member's responsibility to ensure that they have correctly utilised the out of office function to inform senders of their absence and suggest alternative contacts. Staff must also ensure that all relevant information is stored in a location easily accessible to all staff members in that team.

In the event of unplanned absence, the manager of the staff member can request that an out of office message be placed on the account to advise of alternative contacts. This can be requested through IM&T's Support Central.

4.2.1 Access to Email of staff who are not available

If access to a user's account is deemed necessary in their absence, consent for access should be sought from the account holder if at all possible. If consent cannot be obtained, access must be requested by the Information Asset Owner or the line manager. Requests for access should be made to the IG team using the form in Appendix 3 and approved by a Director. Requests should be specific and include the name of the subject line of the relevant email. Blanket requests to access entire email accounts are not appropriate.
Staff should be aware that all corporate files are the property of the Trust and may be accessed in an emergency or other unplanned event where a member of staff is absent.

4.3 Video and Audio Conferencing

Only Trust approved software should be used for video and audio conferencing. When initiating conferences, confirmed email addresses should be used only.

Guidance on conferencing can be found below:

Item	Control	Guidance	Legislation/ Policy
Patient Consent	Local procedure	The informed consent of patients should be sought before engaging in an online consultation. The recommendation is that this would normally be done face to face before online meetings take place, for example at the diagnosis consultation with the clinician. For one off meetings this may not be practicable and individual risk assessments should be undertaken. Points to consider when seeking consent are that the patient has the capacity to consent and they understand the risks of sharing data online. In addition, the patient my want to give consent for a chaperone, family member or other carer to be involved in the meeting. See patient confidentiality at the end of this table.	Data Protection Act GDPR NHS Code of Practice: Confidentiality Care Records Management Principles
Assure invite list	Use assured contact details	For example, if inviting NHS staff only use emails on the secure NHS email system. If inviting patients use the email address or telephone number held on record.	Data Protection Act GDPR DH Care Record Management
Verify meeting details	Local procedure	If multiple meetings are organised, you should ensure that the attendee is being invited to the correct one. For example, check the date and time and other attendees to verify a match.	Data Protection Act GDPR
Verify Identity of participant(s)	Use of an assured digital identity where possible Local procedure to verify identity if un-assured digital identity is used	While assured contact details may have been used, the wrong person may have been invited. For example, the wrong J Smith was selected from the list of possible people. A local procedure should be used to check at the start of each meeting that the correct participants have joined.	GDPR Duty of Confidentiality Care Record Guarantee Care Records Management Principles
Verify Patient(s) Identity	Use of an assured digital identity where	A local procedure will be required to ensure a consistent and robust approach is taken. It may not be enough to rely on seeing that a person with the expected	Care Record

	possible Local procedure to verify identity if un-assured digital identity is used	name has joined the meeting and further identity checks should be carried out in a similar way to those used on many telephone services.	
Who initiates the meeting	Local process or procedure	Patients should be able to request an online meeting. However, it is recommended that electronic meetings are not initiated by patients. Care professionals should always initiate the meeting using the details in the patient record. Care must be taken to ensure that once started it is the verified patient in the meeting. As you would for a telephone conversation.	Public Service Guarantee for Data Sharing – guarding access
What protocol or procedure is used to start the meeting	Local process	There should be an agreed procedure to start a meeting. This includes selecting the chair-person who will be responsible for the meeting and would issue the privacy statement. If the meeting is recorded any additional requirements are articulated and accepted by the attendees.	Data Protection Act GDPR Public Service Guarantee for Data Sharing NHS Code of Practice: Confidentiality
Where are the participants Physical location	Local procedure to verify end user locations are secure	Guidance should be issued on where online meetings should be held. This would suggest that conversations including Patient Identifiable Data are not held in public locations such as internet cafes. In some cases, it may be required to check with attendees (as part of the protocol used to start the meeting) that they are in a private location in which they cannot be overheard. Even if using earphones meeting participant contributions may still be audible to others in the vicinity. Any devices used to support the online meeting services are expected to meet minimum requirements of devices.	Data Protection Act GDPR Public Service Guarantee for Data Sharing – guarding access

4.4 Posting information on social networking sites & the Internet

The term ‘social networking’ is used to cover such Internet sites as Facebook, and Twitter. It also includes blog sites, Internet homepages, and other user-interactive services. The following must not be uploaded/posted to social networking websites:

- person identifiable information on trust patients and/or their relatives;
- person identifiable information of another trust employee in relation to their

employment, including judgements of their performance and character;

- photographs of trust employees taken in their work situation or in their working uniform which is not directly related to their employment and which would be deemed as inappropriate;
- defamatory statements about GMMH trust, its staff, services or contractors

GMMH social networking standards and advice can be found in Appendix 2.

4.5 Personal Use

Staff members are permitted to use the Internet for non-business use provided that it is in accordance with the requirements of this policy; it is in their own time and is not excessive or detrimental to their job performance. It is expected that staff will act responsibly in doing this, being aware of the image they are presenting to visitors to their work area. Personal Internet browsing must not distract staff from their work or prevent other Trust staff from using the Internet for work related purposes. Inappropriate and excessive use will be reported on.

NHS GMMH email accounts are provided primarily for business use; however, the organisation will allow limited personal use of email under the following conditions:

- personal use must not be excessive;
- personal use must conform to the standards set out in this policy;
- personal emails must conform to the standards set out in this policy.

Personal emails should be stored separately from business emails in a folder marked private and confidential.

It is forbidden to forward chain letters, virus warnings, and other warnings as they are often hoaxes. If you receive such a warning contact the IT helpdesk for advice.

4.6 User names and passwords

Each user is responsible for maintaining the security of their individual login and password. Staff must not share their username and password with anyone, they should not write passwords down, nor should they choose passwords that are easily guessable. Staff must not let anybody use their log in.

4.7 Forgotten passwords

If you forget your network password, you can reset this by clicking on ‘Forgotten password’ on the network login screen. If you do not have this feature installed or have not registered, you can request a password reset from the IM&T Support Central, however in order to protect accounts from unauthorised access the Service Desk follow strict procedures and will not reset your password unless your identity can be verified.

4.8 Housekeeping

Emails take up space on the Trust servers. All email users must conduct regular housekeeping and delete unnecessary emails and large attachments. The Trust has a maximum retention period of 2 years for emails. Any emails older than this will be deleted automatically.

All Skype for Business conversations are stored on the Trust servers for a maximum retention period of 2 weeks. Any conversation older than this will be deleted automatically.

4.9 Monitoring

All emails are automatically scanned for viruses and other unwanted content such as SPAM.

Email is not routinely monitored at GMMH, other than permitted by law. The Trust reserves the right to access and disclose the contents of users' emails without the consent of the user. This will only be done when the Trust believes it has a legitimate business need or to comply with Fraud Detection (NHS Protect).

In addition, the content of an email or Skype for Business record may constitute 'personal data' subject to the provisions of the Data Protection Act 2018, GDPR and the Access to Health Records Act. The Trust may therefore access, inspect and disclose such records to the individual who is the 'data subject' under conditions that are laid down in these Acts.

4.10 Leavers

Accounts will be disabled as soon as possible following the user's final working day. It is line managers' responsibility to notify IM&T Support Central when a member of staff leaves the organisation. Emails and other files belonging to a leaver will be deleted at this time.

4.11 Confidentiality

Users should be aware that the nature of email makes it less private than they may anticipate; consequently, the Trust cannot guarantee the confidentiality of non-encrypted emails sent and/or received via its emails system.

The principles of Confidentiality apply to any information sent via email. All personal or sensitive data must be sent in line with Trust standards (see 4.1.3).

4.12 Distribution Lists

Inappropriate use of large distribution lists wastes both network resources and staff time. Additionally, if staff receive many irrelevant emails they are more likely to miss the important ones. GMMH therefore restricts the use of the 'all staff' distribution list to important business related emails, which are relevant to everyone on the list and are time sensitive. Unless information for all staff cannot wait, it should be included in the weekly staff bulletin through the Communication department.

If you do decide that information needs to be emailed to large distribution lists, please observe the following guidelines:

- avoid attachments and graphics - just type or paste the essential information into the email. Attachments and pictures take up much more room and take time and resources to open and save or print.
- If you need to provide a lot of information - put it on the Intranet, website or SharePoint or provide a link but you must remember that you must always keep Personal Identifiable Data secure.

The email system only permits users to send emails to a maximum of 80 recipients.

4.13 Viruses

Email messages are increasingly the source of viruses, which often sit within the attachment. The Trust does have anti-virus protection although occasionally as with any email service a new virus may not be immediately detected by the software.
If you are unsure about the source of an email attachment you should leave it unopened and inform the IT helpdesk.

You must not intentionally introduce or forward any viruses or computer programmes that may cause damage to NHS, GMMH computers or systems and to do so may result in disciplinary proceedings and may also be deemed to be a criminal offence.

4.14 Copyright and licensing

Copyright is the term used to describe the rights under law that people have to protect original work they have created. Copyright protects the work to ensure no one else can copy, alter or use the work without express permission of the owner. You have a responsibility to ensure that copyright and licensing laws are not breached when you compose or forward emails and email attachments.

4.15 Freedom of Information Act 2000

All staff should be aware that under the Freedom of Information Act (FOI) 2000 public authorities must make all types of recorded information available to the public, this includes emails.

As personal emails including personal folder archives are now publicly accessible upon request, the following principles should be followed:

- Where emails or email archives are currently kept for no specific reason, these emails should be deleted.
- Where emails are kept as an audit trail, or as evidence of a decision making process, these emails should be categorised and electronically filed in a documented filing system such as a designated departmental network drive or, where no longer needed, should be deleted, see Records Management

Policy.

- Where not deleted, details of email or personal folder archives should be documented and documentation kept centrally in a departmental electronic filing systems. As personal folder archives are searchable, but may only be accessible, individual members of staff may be called upon to search for pieces of information on a specific topic. Where members of staff are unable, unavailable or unwilling to undertake this work, IM&T may access such archives centrally and items of computer equipment may be confiscated for extended periods of time in order to satisfy the requirements of the Freedom of Information Act.
- Personal Information about patients and staff remains confidential and is protected by the Data Protection Act 2018, GDPR and the Human Rights Act.
- Requests for information under the Freedom of Information Act for information contained within emails must be handled under the agreed Freedom of Information Act process. Please see the Freedom of Information policy which can be found on the Intranet.

4.16 Prevent

Prevent is a Government strategy to stop vulnerable people from becoming radicalised into terrorism. It is generally more common for vulnerable individuals to become involved in terrorist-related activity through the influence of others.

Initial contact may be via peers, siblings, other family members or acquaintances, with the process of radicalisation often being a social one. Such social interaction takes place in a range of unsupervised environments such as gyms or cafés, in private homes and via the internet. Access to extremist material is often through leaflets and local contacts. However, the internet plays an important role in the communication of extremist views. It provides a platform for extremists to promote their cause and encourage debate through websites, internet forums and social networking, and is a swift and effective mechanism for disseminating propaganda material.

GMMH staff should be aware of anyone, including staff members or service users making frequent visits to websites showing images such as armed conflict around the world and providing speeches and access to material from those involved in the radicalising process. For reference and to report any concerns, please contact your Manager, the Head of Risk, Safety and Resilience Manager or the Local Security Management Specialist and refer to relevant trust policies including the Security Policy and Radicalism and Counter Terrorism Policy.

4.17 Questions and Compliance

If you have any questions or comments about this policy, please contact the Information Governance Department via IM&T Support Central. If you do not have any questions the organisation presumes that you understand and are aware of the requirements of the email and Internet policy and will adhere to them.

Failure to comply with the requirements of this policy may result in your email account being suspended or Internet functions restricted, and will be dealt with under the Trust's disciplinary procedures.

5. Training Requirements

Any specific information and training requirements subsequent to this policy should be addressed to the IG team.

6. Monitoring

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee
All members of staff are aware of the existence and detail of this policy.	When policy is updated and in induction training.	IG annual staff survey.	Report and communications email	IAO and IAA.	IGSG
All members of staff operate in compliance with this policy	Breaches/ incidents are reported monthly and annually.	Regular incident/ progress reports	IGSG reports	IAO and IAA.	IGSG

The Trust will monitor the effectiveness of the controls within this Policy through the use of Key Performance Indicators. These indicators will be regularly reviewed and submitted to the Information Governance Steering Group.

7. Resource/Implementation Issues

Managers are responsible for ensuring that their staff are able to implement this policy and must report back up through their management structures to the Director of Finance, Capital & IM&T where additional resources are required.

8. Risk Issues

The email and Internet policy is one component of the overall Information Governance Risks and as such is incorporated into the IM&T risk register which is monitored on a bi monthly basis.

9. Supporting Documents and References

9.1 Requirements

Board Objective Reference:	3 – To engage in effective partnership working 5 – To enable staff to reach their potential & innovate 6 – To achieve sustainable financial strength & be well-governed
CQC Regulation:	17 – Good governance
Other requirements:	Related legislation including GDPR, DPA, FOI.

9.2 Supporting Documents

- Access to IT Server & Comms Room Procedure
- Information Security Policy
- Information Asset Management Policy
- Information Sharing Policy
- Clinical System Access Policy
- Confidentiality Policy
- Safe Haven Policy

9.3 References

- Access to Health Records Act (1990) Link
- Computer Misuse Act (1990) Link
- The Data Protection Act (2018) Link
- General Data Protection Regulation
- The Human Rights Act (1998) Link
- Electronic Communications Act (2000) Link
- Regulation of Investigatory Powers Act (2000) Link
- Freedom of Information Act (2000) Link
- Health & Social Care Act (2001) Link

10. Subject Expert and Feedback

Kevin Orritt – Infrastructure Manager
Email: kevin.orritt@gmmh.nhs.uk Tel: 0161 3571234

Deborah Tonkin – Information Governance Manager.
Email: Deborah.tonkin@gmmh.nhs.uk Tel: 0161 3581573

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 1 – Web Filtering

The following categories of web sites are automatically blocked:

- Adult/Sexually explicit
- Chat rooms
- Criminal activity
- Downloads
- Gambling
- Games
- Hacking
- Hosting sites
- Intimate apparel
- Intolerance and hate
- Peer to peer
- Personal and Dating
- Phishing and fraud
- Spam
- Spyware
- Tasteless and offensive
- Violence
- Weapons

Appendix 2 – Social Networking Advice

Social Networking Sites and GMMH

GMMH has joined the social media revolution and we currently have pages on Facebook and Twitter.

You can 'like' us on Facebook at https://www.facebook.com/GMMentalHealth or follow us on Twitter @GMMH-NHS.

Whilst we currently do not allow you to use social networking sites at work, we do recognise many of you use them frequently outside of work and we would invite you to keep up to date with GMMH via these networks if you would like to do so.

The standard of your conduct as a member of GMMH staff both online and offline is important. You should think through what this information means for you in practice, and if needed, take steps to change the way you use social networking sites.

- Keep your personal and professional life separate as far as possible. For example, you could keep Facebook just for close friends, use Twitter for sharing information with people you may now know and use LinkedIn for building and maintaining professional relationships.
- If you identify yourself as a member of GMMH staff on Facebook, you should act responsibly at all times and uphold the reputation of the Trust. Even if you do not do this, be aware that conduct online could still jeopardise future employment prospects.
- Protect your own privacy. Think through what kinds of information you want to share and with whom, and adjust your privacy settings. On Facebook, you can adjust privacy settings at group level to share different levels of information with different kinds of friends. Remember that the more your personal life is exposed through social networking sites, the more likely it is that this could have a negative impact.
- Do not use social networks to build or pursue relationships with patients and service users, even if they are no longer in your care. If you receive a friendship request from a current or former patient, Facebook allows you to ignore this request without the person being informed, avoiding causing any offence.
- Do not discuss work-related issues online, including conversations about patients or complaints about colleagues. Even when anonymous, these are inappropriate.
- Never post pictures of patients or service users, even if they ask you to do this. If your mobile phone has a camera, you should not use it in the workplace.
- Never post inappropriate pictures of yourself in a Trust uniform, (such 'inappropriate circumstances' is anything that is not directly associated with your employment and Trust values).

- Social networking sites should not be used for raising or escalating concerns (commonly referred to as whistleblowing). There is separate Trust guidance on raising and escalating concerns which clearly sets out your professional duty to report any concerns which put the safety of people in your care, or the public at risk.
- Remember that everything you post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed, and it is easy to lose control of it. Presume that everything you post online will be shared and is permanent.
- You can take action if you find yourself the target of complaints or abuse on social networking sites. You can remove someone from your friend list and block them from interacting with you, and most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse. If you are very concerned about someone else's behaviour online, you should take steps to raise your concern, including, if necessary with their line manager. In the most serious circumstances, for example if someone's use of a social networking site is unlawful, you should also report the incident to the police.

GMMH staff may put their employment at risk if they:

- share confidential information online;
- post inappropriate comments about colleagues or patients;
- post inappropriate photographs;
- use social networking sites to bully or intimidate colleagues;
- pursue personal relationships with patients or service users;
- distribute sexually explicit material;
- use social networking sites in any way which is unlawful.

Appendix 3 – Access Authorisation Form

NHS
Greater Manchester
Mental Health
NHS Foundation Trust

Information Governance Department
Bury New Road
Prestwich
Manchester
M25 3BL

Date

Form of authority

Staff Granted Administrator Rights to Access Employee Corporate Files

Scope: this form is to be used when unplanned long term absence of a Trust employee prevents access to corporate files that are password guarded.

Reason for requesting access to the data

…………………………………………………………………………………………
……………………………………………………………………………………………

Authorised by…………………………………………Signature………………………

Job title…………………………………………………………………………………….

Staff requesting access

- **Name**………………………………………………**Signature…………………**

Job title……………………………………………………………………………………

Data to be accessed (to be completed prior to authorisation being obtained):
…………………………………………………………………………………………
…………………………………………………………………………………………
……………………………………………………………………………………………..

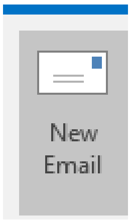
Contains personal confidential data? Yes/No (delete that does not apply)

Name of files……………………………………………………………………

Appendix 4 – How to encrypt internal emails

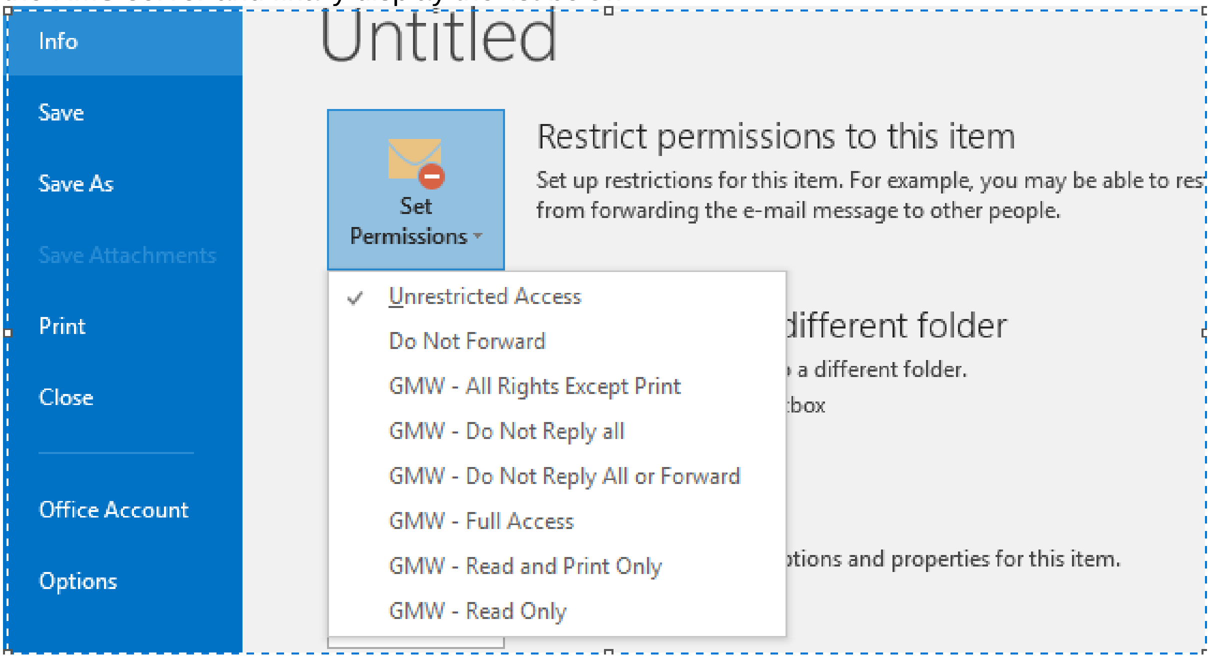
How to Encrypt an Internal Email using RMS

Click on new email



New Email

Click File, then Info and select set permissions. If it's the first time using it, it will connect to the RMS server and finally display the list below



Info

Save

Save As

Save Attachments

Print

Close

Office Account

Options

Untitled

Set Permissions

Restrict permissions to this item

Set up restrictions for this item. For example, you may be able to res from forwarding the e-mail message to other people.

- ✓ Unrestricted Access
- Do Not Forward
- GMW - All Rights Except Print
- GMW - Do Not Reply all
- GMW - Do Not Reply All or Forward
- GMW - Full Access
- GMW - Read and Print Only
- GMW - Read Only

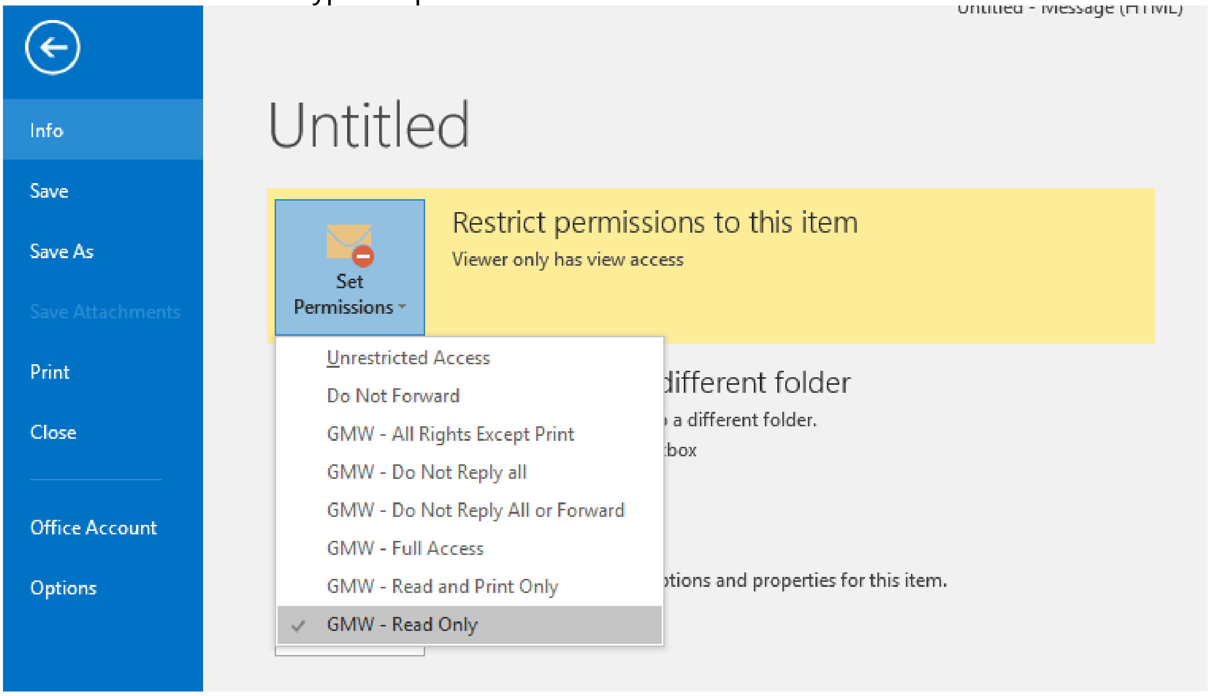
different folder

a different folder.

box

tions and properties for this item.

Select the relevant encryption option needed.



Untitled - Message (HTML)

Info

Save

Save As

Save Attachments

Print

Close

Office Account

Options

Untitled

Set Permissions

Restrict permissions to this item

Viewer only has view access

- Unrestricted Access
- Do Not Forward
- GMW - All Rights Except Print
- GMW - Do Not Reply all
- GMW - Do Not Reply All or Forward
- GMW - Full Access
- GMW - Read and Print Only
- ✓ GMW - Read Only

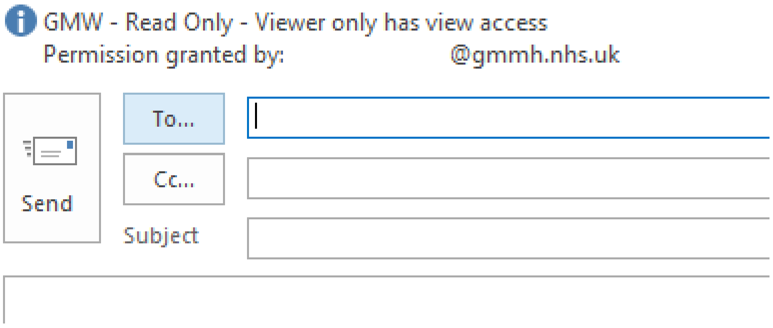
different folder

a different folder.

box

tions and properties for this item.

Click the back arrow when done and complete the email as normal



GMW - Read Only - Viewer only has view access
Permission granted by: @gmmh.nhs.uk

The email is now encrypted and can only be viewed by the GMMH staff if was sent to. If you selected DO NOT FORWARD or READ ONLY, it cannot be forwarded on.
Encrypted emails cannot be read on mobile phones or by any users external to the Trust.

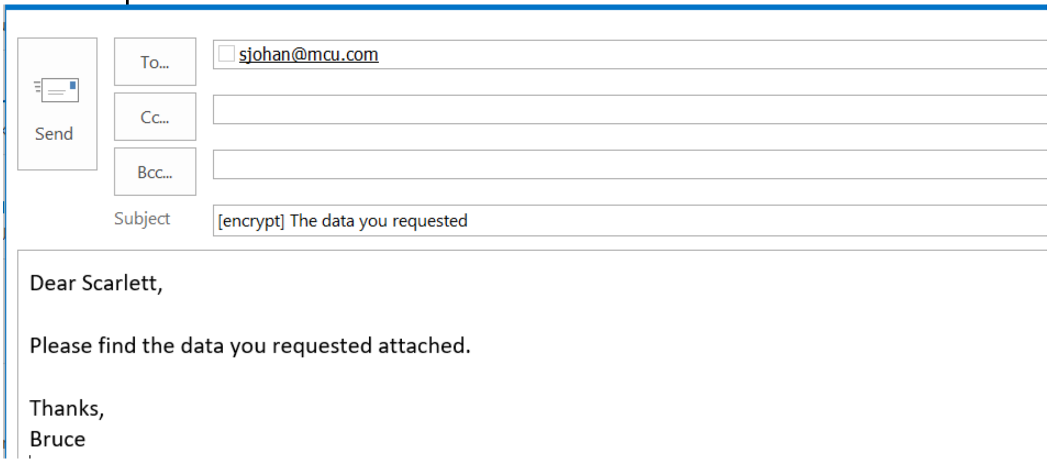
Appendix 5 – How to encrypt external emails

The encryption works by sending an email to the recipient stating that an encrypted email is waiting for them and asks them to create an account using their email address and a password. This is only required to be input the first time. After that, as long as the encryption process is followed, all emails are sent encrypted without the need to input the password. Sending an encrypted message is simple and convenient. There is no software to install or configure. Encryption can be carried out in one of two ways:

Method 1

It can be used on-demand by typing [encrypt] in the subject of the message.

Important Note: that the word encrypt must be in lower case and square brackets as per the example below.



To... sjohan@mcu.com

Subject [encrypt] The data you requested

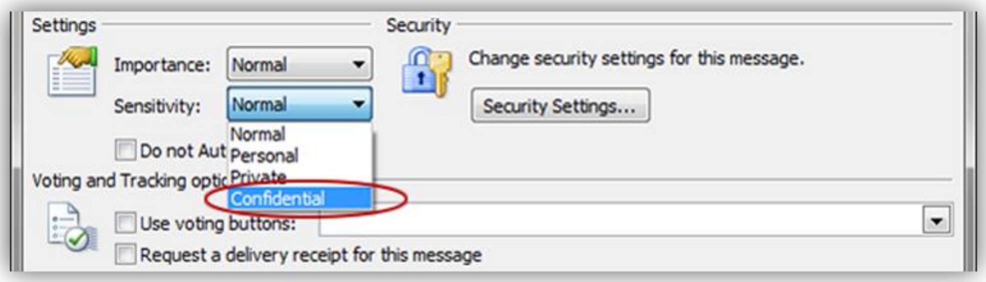
Dear Scarlett,

Please find the data you requested attached.

Thanks,
Bruce

Method 2

A message can be manually encrypted by marking it as confidential in Outlook under the Properties menu of the message.


Settings
Security
Change security settings for this message.
Security Settings...
Normal
Personal
Private
Confidential
☐ Do not Aut
Voting and Tracking optic
☐ Use voting buttons:
☐ Request a delivery receipt for this message

Importance: Normal

Sensitivity: Normal

Once you have sent the encrypted email, you will receive an email confirmation to advise you the message was successfully encrypted.