Tameside and Glossop Integrated Care NHS Foundation Trust

Policy title:	**Acceptable Use Policy**

Issue date:	April 2020	**Review date:**	April 2023

Version:	2.6	**Issued by:**	Chief Information Officer

Aim:	The aim of this policy is to: • Clarify organisational policy regarding acceptable and unacceptable use of internet, email services and network access; • Explain the requirements for accessing email via personal devices; • Reduce or avoid security threats by increasing awareness and disseminating good practice; • Cease the copying/distribution of copyrighted materials; • Encourage effective use of the organisation's resources; • Protect the Organisation against potential liability.

Associated documentation:	**17 REFERENCES** **Internet Resources** General Data Protection Regulation (2016/679) http://www.eugdpr.org/ Regulation of Investigatory Powers Act 2000. http://www.legislation.gov.uk/ukpga/2000/23/contents Telecommunication (Lawful Business Practice) (Interception of Communications) Regulations 2000. http://www.legislation.gov.uk/ukpga/2005/13/contents Employment Code of Practice, Information Commissioner's Office. http://www.legislation.gov.uk/ukpga/2005/13/contents Obscene Publications Act 1959. http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents Protection of Children Act 1978. http://www.legislation.gov.uk/ukpga/2005/13/contents Criminal Justice Act 2003. http://www.legislation.gov.uk/ukpga/2003/44/contents Criminal Justice and Public Order Act 1994. http://www.legislation.gov.uk/ukpga/1994/33/contents Computer Misuse Act 1990. http://www.legislation.gov.uk/ukpga/1990/18/contents Freedom of Information Act 2000. http://www.legislation.gov.uk/ukpga/2000/36/contents Disability Discrimination Act 2005. http://www.legislation.gov.uk/ukpga/2005/13/contents Sex Discrimination Act 1975. http://www.legislation.gov.uk/ukpga/2005/13/contents Race Relations Act 1976. http://www.legislation.gov.uk/ukpga/2005/13/contents NHS.NET Guidance http://www.legislation.gov.uk/ukpga/2005/13/contents Copyright, Designs and Patents Act 1988. http://www.legislation.gov.uk/ukpga/1988/48/contents Regulation of Investigatory Powers Act 2000. http://www.legislation.gov.uk/ukpga/2000/23/contents Telecommunication (Lawful Business Practice) (Interception of Communications) Regulations 2000. http://www.legislation.gov.uk/uksi/2000/2699/regulation/3/made

	Organisation Policies Conduct and Disciplinary Policy. http://tis/documents/ConductDisciplinaryPolicy.pdf Confidentiality Disclosure Policy. http://tis/documents/ConfidentialityPolicy.pdf Data Protection Policy. http://tis/documents/DataProtectionPolicy.pdf Corporate Record Management Policy (retention of records) http://tis/documents/CorporateRecordsManagementPolicy.pdf
Appendices:	Appendix 1 Organisation email disclaimer Appendix 2 Guidelines on the use of email Appendix 3 Further details of legal issues Appendix 4: Remote Email Access Appendix 5: The use of Office 365 Appendix 6 Equality Impact Assessment
Approved by:	Peter Nuttall (SIRO)
Date:	

Review and consultation process:	The policy has been revised by the Chief Information Officer and the Information Security & Information Governance Manager to include wider IT issues than the original policy, which dealt with Internet and Email only. The previous policy was developed in consultation with the Deputy Director of Human Resources. The following groups had an input for the consultation process: • Human Resources Policy Development Group • Staff Partnership Forum • Local Negotiating Committee
Responsibility for Implementation & Training:	

V 2.3

Revisions:		
Date:	**Author:**	**Description:**
V2.2	Chief Information Manager Information Security & Information Governance Manager	Released for approval from SIRO General update with new format. Added new section Appendix 2 Section 12 – Cyber Security Amended the Data Protection Laws to reflect the DPA (2018), and the GDPR.
V2.3	Chief Information Manager Head of Information Governance	Changes to HSCN from N3 as the secure network; Aligned to support the pan-government DCB1596 secure email standard; Adopted NHS Mail AUP (V2) clauses throughout to close gaps in assurance; Added Appendix 5 – The Use of Office 365.
V2.6	Head of Information Governance	Completed update after input from the IT Department.

Distribution methods:	Email Intranet

1. INTRODUCTION

1.1. The Organisation recognises that computer based information systems and services have the potential for enormous benefit to employees. The facilities give tremendous support to the management and delivery of Organisation services, and for communicating with partner organisations and stakeholders. It is Department of Health policy, adopted by the Organisation, that all NHS staff have the facility of internet and email access available in their workplace.

1.2. However, the Organisation also recognises that these services can be misused, and thus the associated risks and pressures, including litigation and security concerns, legal and regulatory compliance and productivity of staff must be addressed. A basic principle of employment law is that employers can be held vicariously liable for the actions of the employee in the course of employment. In the course of employment is interpreted by the courts very widely, and thus accidental or intentional misconduct of employees is often included.

2. SCOPE

2.1. This policy applies to all employees of the Organisation, volunteers, other NHS and health organisations, and other contracted staff; having the facility to use the Organisation's email and internet services, plus anyone granted access to the Organisation's network whilst engaged in work for the Organisation at any occupied location, and/or on any corporate owned or approved computer asset.

2.2. This policy manages access and ownership of all removable media devices.

2.3. The policy also covers:

- Web gateways
- Direct email
- Webmail
- Instant messaging
- NHS mail accessed from corporate equipment.

2.4. The principles of this policy apply to staff who have been granted access to internet and email services from home for Organisational business. Further details will be published in the Remote Working Policy workers.

2.5 **Tameside and Glossop Integrated Care NHS FT Information Governance Structure**

Information Governance Assurance Structure

The Information Governance Structure for Tameside and Glossop Integrated Care NHS Foundation Trust facilitates the information governance service for the following Organisations:

- Tameside and Glossop ICFT, (Integrated Care NHS Foundation Trust), which encompasses the Community provision;
- Tameside and Glossop CCG, (Clinical Commissioning Group), who are a separate legal body and has a Service Level Agreement with Tameside and Glossop ICFT for IT Services and Information Governance assurance;
- Tameside and Glossop GP Surgeries, IT provision only, known within this document as GPIT.

*The ultimate accountability for information governance assurance remains with each statutory organisation

3. DEFINITIONS

Copyrighted Material	A set of exclusive rights granted by the law of a jurisdiction to the author, owner or creator of an original work, including the right to copy, distribute and adapt the work.
Email	**Is the facility to communicate messages or information electronically to:** • Employees using local tgh.nhs.uk email. • Employees on NHS mail. • Other NHS organisations and supporting organisations. • Other contacts associated with the organisation.
Internet Services:	**Is the facility for:** • The use of the Organisation's connection via HSCN or dedicated links to the internet domain or www/world wide web. • The use of Organisation's information servers, i.e. both the intranet and internet sites for Tameside & Glossop Integrated Care NHS Foundation Trust and Tameside General Hospital.
HSCN	Is the NHS secure highway for transportation of information between NHS organisations and supporting organisations who are authorised to do so.
Offensive material:	**Is material that** • Is pornographic or obscene. • Involves threats or violence. • Promotes illegal acts, racial or religious hatred or unfair discrimination. • Is found to be offensive by the recipient. This list is not exhaustive: these are sample types of offensive material or practice.
Network Storage:	Commonly known as the G, F, M, or S:Drive, this is an area on the Organisation's storage array network (SAN), which allows folders, documents, emails, applications and data to be stored.
Endpoint:	Is any piece hardware or device that connects onto the Organisational network.

4. DUTIES

4.1. The Chief Executive is responsible for ensuring that the Organisation has effective policies to assist staff and control risks. The legal responsibility for employee for IT system use including emails and for internet misuse by an employee rests both with the Chief Executive and the employee responsible.

4.2. **Senior Information Risk Owner**

The Senior Information Risk Owner (SIRO) will:

- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework;
- Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control;
- Review and agree action in respect of identified information risks;
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;
- Provide a focal point for the resolution and/or discussion of information risk issues;
- Ensure the Board is adequately briefed on information risk issues

4.3. **Director of Performance and Informatics**

Has the responsibility for IT Services, which has a Chief Information Officer (CIO), through whom this policy will be delivered.

4.4. **Chief Information Officer**

Is responsible for:

- Overall responsibility for all IT services
- Ensuring compliance to external standards and policies, e.g. NHS Digital
- Keeping the policy under review in light of incidents and legislation.
- Reporting non-compliance to this policy and other security violations via the Organisation risk management procedure.

4.5. **Head of Information Governance**

Is responsible for:

- Advising on the security of personal data under Data Protection legislation.
- Keeping the policy under review in light of incidents and legislation.
- Reporting non-compliance to this policy and other security violations via the risk management procedure.
- Maintaining the links with other Information Governance areas, principally the Corporate Records Management Policy and strategy.
- Raising initial awareness of the policy at the corporate induction.

4.6. **IT Services Department**

Are responsible for:

- Ensuring the availability of internet and email services and their supporting infrastructure.
- Managing the security and integrity of data, via anti-virus, mail content, web filtering and content, and anti-spam products.
- Managing the internet filtering and content by testing the integrity of web sites and categorisation of sites not yet categorised by the Web Management product.
- Managing the mail-store, and the establishment and maintenance of shared mailboxes and calendars on behalf of staff.
- Undertaking programmed and ad hoc monitoring arising out of internet and email security products.
- Maintaining the Microsoft Active Directory for the Azure AD Connect
- Maintaining the currency of employees in appropriate sources (starters and leavers).
- Producing documentation and reports on internet and email usage and misuse.
- Reporting non-compliance to this policy and other security violations via the risk management procedure.

4.7. **Line Managers**

Are responsible for:

- Ensuring all staff read, understand, and sign the declaration.
- Ensure that awareness to this policy is highlighted at their local induction programme.
- Monitoring staff compliance to the policy.
- Monitoring staff time spent on personal use of the internet and email services.
- Managing their starters, transfers, and leavers processes
- Instigating further investigations arising out of suspected misuse.
- Taking action regarding misuse in accordance with the Conduct and Disciplinary Policy.
- Reporting non-compliance to this policy and other security violations via the risk management procedure.
- Taking care in relation to both external and internal emails that they cannot be considered to be contractually binding.

4.8. **Staff**

All staff are responsible for:

- Complying with this policy and associated guidelines.
- Reporting non-compliance to this policy and other security violations via the risk management procedure.
- Housekeeping of the mailbox store in line with guidelines for corporate records management.
- Ensure that any personal information including patient and staff identifiable is held in a safe area with access to the approved people.
- Adhering to the NHS mail Acceptable Use Policy when using NHS mail.
- Ensuring that all materials used in publications/communications is not bound by copyright.

5. POLICY STATEMENT

5.1. Computing facilities are to be used for business. Authorised access to the internet and email services via the network will be granted to employees and/or authorised personnel who have read and agreed this policy.

5.2. Inappropriate use of local email and internet services will lead to disconnection and may lead to disciplinary action.

5.3. The Organisation employs specific software to protect the network and enforce compliance with this policy, and with legislation. The Organisation therefore routinely monitors the overall patterns of internet and email usage, e.g. attempts to access blocked sites, use of inappropriate language. In so doing, the Organisation will at all times seek to act in a fair manner and respect staff rights for privacy of their personal data under the Human Rights Act 1998 and the Data Protection Act (2018). (See also the Data Protection Policy).

5.4. The Organisation reserves the right to monitor all email transmitted to external sources via the email system, and received from external sources, for inappropriate content.

5.5. The Organisation prohibits access to websites that contain offensive material, or which are deemed not to contribute to business, e.g. gaming and shopping or social media. This includes the usage of copyrighted material copied from the internet or external sources.

5.6. There may be circumstances under which it is necessary for a designated and authorised person other than you, to view the contents of your files and folders within your email and calendar folders. For example, if you have a secretary or PA that organises your diary, or if IT are working accessing the folders regarding a ticket that has been logged.

5.7. You must familiarise yourself and regularly check the Information Governance and IT Services Intranet site which includes important policy documentation, service status information, training and guidance materials, information about known issues with the service and user/administration guides.

5.8. All staff must complete their annual Information Governance mandatory training.

6. LEGAL ISSUES

6.1. All staff using internet and email must clearly understand the legal issues involved from both their own perspective and from that of the Organisation. The laws of defamation, obscenity, discrimination and harassment, copyright and confidentiality all apply to staff use of email and internet.

6.2. Under the Data Protection Act 2018, staff may be required to supply emails or documents relating to data subjects if requested as part of a Subject Access Request. Non-disclosure, amending, or deleting this information after it has been requested is a criminal offence.

6.3. Further details of the legal issues are given for reference purposes at Appendix 3.

7 ACCEPTABLE USE

7.1 General

- Users must ensure that they terminate each session in accordance with the Information Security Policy and the Confidentiality Disclosure Policy, and all computers, printers and peripheral hardware must be shut down at the end of the working day.
- All devices are to be restarted at least once every 24hrs. This is a personal and departmental responsibility.
- The internet and email services are provided primarily for business and must be used responsibly.
- Access outside of normal working hours will be at the discretion of the line manager or head of department, but in accordance with the standards in this policy

7.2 Email

Staff should:

- Ensure that the identity of the receiving recipient's email address is correct, and that messages or data sent by the Organisation or NHS mail do not cause distress or offence to the receiving recipient, including chain mail messages, and jokes.
- Guard against accidental breaches of confidentiality by entering a wrong address or forwarding a message to inappropriate recipients.
- Initiate the Out of Office assistant on the email service giving details of alternative contacts or arrangements for planned periods of absence.
- Set up shared email accounts and calendars, for managers/consultants and their secretaries through the IT Service Desk, rather than sharing usernames and/or passwords.
- Ensure delegation rights are set up when and where appropriate to give peers and/or assistants rights to administer mailboxes either routinely or in the event of absence.
- Use the sensitivity categories on email carefully (normal, personal, private, confidential) wherever possible.
- Clearly state to the recipient when material is private and confidential.
- Include 'private' within the title of the email in private emails (i.e. non-business). These emails will not be opened, unless they contravene other rules of the monitoring software or providing, they do not contain profanity or for other good reasons such as being involved within a specific investigation.
- Inform their line manager if unsolicited offensive or sexually explicit emails are received, who will be responsible for deciding whether further investigation or disciplinary action is appropriate.
- Report to the IT Service Desk if files, for the purpose of business, are attached that are above 70mb in size, are compacted using a zip programme, or are a restricted file type such as an image, to ensure they are not quarantined and/or subsequently removed.
- ensure that any exchange of sensitive or personally identifiable information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated.
- complete a Bulk Transfer request when sending more than 50 records, (not limited to health records)
- should report immediately to the Information Governance Department if sensitive or patient data has been shared with an incorrect recipient.

7.3 Internet

Staff should:

- Use newsgroups and web discussion boards only in relation to business.
- Use the internet when appropriate to do so, in order that the productivity of their department is not compromised.
- Exit a site immediately on finding that they have inadvertently accessed a site containing offensive or sexually explicit material and report the web address or URL to the IT Service Desk.
- Use approved images, including Microsoft approved SmartArt, Icons, and http://www.photolibrary.nhs.uk/ or use the corporate identity templates when creating documents and/or slideshows http://tis/Pages/corporateidentitytemplates.asp
- Use the image library for inserting approved images onto tis webpages which is available using the content manager

7.4 Removable Media

Staff should ensure that

- Removable media shall only be used by staff and contractors who have an identified and agreed business need for them.
- The use of removable media by sub-contractors or temporary workers must be subject to the same risk assessment and authorisation process.
- Only removable media that have been approved for use.
- Removable media may only be used to store and share NHS information that is required for a specific business purpose.
- Where person identifiable information or business sensitive information is being taken out or brought into the Organisation, a departmental process must be in place to record the information stored on the device.
- All incidents involving the use of removable media must be reported to the IT Services immediately and in accordance with Incident Reporting procedures.
- Removable media should not be taken or sent off-site unless a prior agreement or instruction exists. A record must be maintained of all removable media taken or sent off-site or brought into or received by the organisation.
- Removable media must be physically protected against their loss, damage, abuse or misuse when used, where stored and in transit.

7.5 Network Storage

Staff should:

- Ensure that information is stored on the network storage area. Information should not be stored locally on the C: Drive
- Housekeep files and folders on the network storage area to minimise duplication, wasted storage space and poor version control, but with due regard to retention periods set out in the Corporate Records Management Policy.

7.6 Access Control

- All staff and contractors shall be given network access in accordance defined by their roles.
- All staff and contractors accessing the computing services agree to uphold the Acceptable Use Policy and other relevant policies and guidelines by logging on and/or using the IT services.
- All staff and contractors who access the networks remotely shall only be authenticated using the Remote Working Policy.
- Diagnostic and configuration ports shall only be enabled for specified business reasons.
- Segregation of networks shall be implemented as determined by the results of the risk assessment.
- Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation on networks.
- All users shall ensure that they lock their screens whenever they leave their desks to reduce the risk of unauthorised access.
- All users shall keep their passwords confidential and unique user identities shall not be shared.
- Access to information systems shall be granted using a formal user registration process.
- Managers shall approve user access rights notify the IT Service Desk of any changes to user roles and responsibilities.
- Managers will contact the IT Service Desk when a user account is no longer required, e.g. through staff resignation or a change in duties to disable the account immediately.
- Managers are responsible for requesting the removal of access to areas on the network when transferring between departments

8 UNACCEPTABLE USE

Below is a list of unacceptable use of internet and email services which can be defined as actions which could bring the Organisation into disrepute, interfere with the business, or jeopardise the security of data, networks, equipment or software.

Inappropriate email messages going out of or coming into the Organisation will be subject to quarantine and removal by the message content management process. Inappropriate web sites are subject to restriction by the web content management process. This list is not an exhaustive list:

8.1 General

Staff must not:

- Use the internet and/or email services for personal financial gain, or for personal or private advertising.
- Use another staff member or party's username or password to access the business networked services or allow another user to use his/her own reference or accessed services.
- Use another staff member or party's means of access with or without their knowledge.
- Attempt to introduce and transmit material (including but not restricted to, computer viruses, Trojan horses and worms) designed to be destructive to computer systems, or to try to get circumvent precautions designed to prevent such material.
- Display any sexually explicit images or documents, or any other images that are discriminatory, including screen savers.
- Delete other users' files or interfere in any way with the contents of their directories, particularly if given temporary or shared access.
- Remove computer software such as desktop icons, wallpaper or screensavers from its location or tamper with it in any way.

8.2 Email

Staff must not:

- Send personally identifiable information outside of ICFT without the appropriate level of protection and security.
- Use email to engage in activities or to transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive. This includes disparagement or defamation concerning race, religion, colour, sex, sexual orientation, national origin, age, or disability, and incorporates sending, receiving, soliciting, printing, copying or replying to such messages.
- Express personal views in such a way that they are likely to be interpreted as being the official policy/view held by the Organisation.
- Use personal email software/webmail (Hotmail etc) for business or personal communications whilst at work.
- Send unwanted email (junk email or unsolicited marketing material commonly known as SPAM), chain letters and offers, hoax virus warning, amusing animations and graphics, unsolicited mail or communication lists via the email system, as these can impact systems and disrupt email services.
- Use email services to harass any other person external or internal to the Organisation.
- Commit the Organisation to purchasing or acquiring goods or services without correct authorisation in line with the Organisation's Standard Financial Instructions.
- Use their own disclaimer on email messages sent to recipients outside of the Organisation. The Organisation has a legal disclaimer which is automatically attached to all external email messages as they leave the network. The standard disclaimer is shown in Appendix 1.
- Deliberately release confidential information. This is a disciplinary offence, as set out in this policy and the Confidentiality & Disclosure of Information Policy.
- Use email services to forge email signatures.
- Send or receive person identifiable information to or from doctors.net email accounts, these accounts are not secure.
- Create 'forwarding rules' which automate sending information outside of the @tgh.nhs.uk domain
- Initiate a SPAM attack from within the Organisation.
- attempt to disguise your identity, your sending address or send email from other systems pretending to originate from the @tgh.nhs.uk service. Where there is a need to provide someone

else with the ability to send email on your behalf, this should be done via the delegation controls within the service.
- Store personal identifiable information within calendars or other outlook folders, this includes patient information as well as staff information.

8.3 Internet

Staff must not:

- Use non-work related chat-rooms or similar services.
- Surf the internet for non-work related subjects during contracted work time.
- Access sites containing offensive material or download any material from such sites. This includes but is not limited to sexual content, extreme political content.
- Play computer games across the network or using any organisational equipment.
- Copy any material from the Internet which is protected by copyright law.
- Use 'cloud' storage for work related information/data unless endorsed by the Change Control Advisory Board.

This list is not exhaustive but indicates the types of activity that may be regarded as misconduct. Staff should always bear in mind that they may be called upon to justify the use of internet and email to their manager, both in terms of time and content.

8.4 Instant Messaging

Instant messaging is a way of communicating from one user to another and differs from email in that the conversations happen in real-time.

Staff must not:

- Use Instant messaging without prior approval from IT via the Change Control Advisory Board

8.5 Streaming Media

Media that is distributed over a data network can be streamed such as radio or television or non-streamed such as video or audio. The user does not have to wait to download a large file before seeing the video/TV programme or hearing the sound, because it is sent in a continuous stream that is played as it arrives.

Staff must not:

- Use streaming media on site for personal or private use.

8.6 Social Media and Personal Sites

A social media service focuses on the building and verifying of online social relationships for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others.

Most social media services are primarily web based and provide a collection of various ways for users to interact, such as chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups.

Staff must not:

- Use social media sites on the organisation's network for personal or private use.

8.7 Network Storage Access

Staff must not:

- Store any database or information system that holds personal identifiable data without approval from the Change Control Advisory Board.
- Delete or remove any database or information system without consulting and adhering to the Corporate Records Management Policy.
- Store any information on the computer's hard drive. The data will not be backed up which in the case of a hard drive failure may render the information lost. Or in the event of theft, personal identifiable data and other sensitive information could be lost.

8.8 Removable Media

Staff must not:

- Use removable devices to permanently store information.
- Loan removable media devices to anyone.
- Attempt to install applications / or programs from removable media onto any computer assets
- Use USB drives or other mechanisms to subvert the security controls is expressly forbidden.

9 PRIVATE USE

9.1. Staff should use internet facilities primarily for business, but private use is allowed at the line manager's discretion, in order to increase competence and understanding. However, in allowing such private use, requires employees to act responsibly, ensuring that it is limited, occasional, reasonable, or incidental, and in accordance with this policy. Employees must never allow use of the facilities to interfere with their job performance or work responsibilities. Staff who abuse this privilege will be subject to Conduct and Disciplinary action.

9.2. Similarly, staff may use email e.g. to communicate with family members, but this personal use should be limited to lunch or other breaks, or after normal working hours.

9.3. Personal use should not include operating a business including a private patient service, campaigning for political causes or candidates, or promoting or soliciting funds for a religious or other personal cause and must comply with the provisions of this policy.

9.4. It is not permissible to use the address for private correspondence, or for delivery of goods purchased over the internet.

9.5. Out of hours usage does not lessen the legal responsibility regarding inappropriate material and/or harassment, misrepresentation and other issues, and thus the principles of this policy apply to private use as well as business use.

9.6. All files and correspondence created is considered organisational property, any personal emails must be marked clearly. The removal of personally owned files or folders after employment is at the Head of Department's discretion and may be conducted with the Line Manager present and/or at the IT Services Department.

9.7. Where an email is identified as private in its header, the message content will not be accessed, unless that message contravenes the rules built into the monitoring software. Where an employee is suspected of abusing the privilege of private use of email, the volume of misuse will be the major focus of investigation. However, if the Organisation suspects an employee of engaging in criminal activity in the workplace and reasonably believes that this may involve the sending or receipt of emails, the Organisation will have a right to access the contents of messages marked as private.

10 MONITORING OF USER ACTIVITY

10.1. It is the responsibility of the IT Services Department to undertake more in depth investigation where appropriate. This can involve the reading of business and personal email contents and attachments to verify the validity of the content. A similar process is undertaken to assess and categorise web pages and webmail. The specialist software includes monitoring tools which can produce activity reports. Restrictions can be imposed on individual machines or groups of machines, and this can be at the request of the IT leads or Managers or Head of Departments. Internet activity reports must be requested via the IT Service Desk and is only accessible to senior managers.

10.2. Anti-virus

Is implemented on:

- Client and server machines.
- Dedicated email server.
- Email gateways.
- All email will be scanned for viruses

10.3. Mail Content

Email gateways.

- This software scans incoming and outgoing emails for inappropriate material such as language, images, and certain file types. It also places restrictions on file size and file type and adds the authorised disclaimer on outgoing messages.
- Messages found to be in contravention of the rules set up within the software are quarantined and assessed for release or deletion in line with the IT Services operational procedures. Ad-hoc processes are also carried out as requested via the IT Service Desk.

10.4. Web Filtering

Is active on all devices and block access to websites that have been categorised in the web filter as:

- Weapons based
- Private homepages
- Criminal activities
- Suspicious
- Drugs
- Bandwidth
- Extremist sites
- Adult material
- Streaming media
- Gambling
- Webmail
- Social networking

Regular reports on staff access are viewed by Senior Management Teams, and ad-hoc audits can be made upon request. The change request form to apply for changes must be placed in writing via the IT Service Desk web portal and sponsored by a senior manager.

10.5. Anti-spam

Is implemented on:

- Dedicated email server.
- Email gateways.
- These services trap, quarantine/remove incoming mail that appears to be spam.

10.6 Removable Media

Removable media such as USB memory devices and DVDs are prohibited on site with few exceptions, these exceptions will require approval via the Change Control Advisory Board, please contact the IT Service Desk for more information.

10.7 Smartphones and Removable Devices

All staff that have smartphones and/or removable devices such as laptops and tablet devices are required to ensure that all security patches have the most up to date security patches installed as per section 8.1 of the Remote Working Policy. Please contact IT if further clarity is required.

11 POLICY DEVELOPMENT & CONSULTATION

The policy has been revised by the Chief Information Officer and the Head of Quality Assurance to include wider IT issues than the original policy, which dealt with Internet and Email only. The previous policy was developed in consultation with the Deputy Director of Human Resources. The following groups had an input for the consultation process:

- Human Resources Policy Development Group
- Staff Partnership Forum
- Local Negotiating Committee

12 IMPLEMENTATION

The Policy will be published on the intranet and included in the local induction check list. Awareness will be carried out via the induction, mandatory update training for clinical and non-clinical staff, and local induction programmes. Guidance material on use of email can be obtained via IT Services.

13 MONITORING OF POLICY COMPLIANCE

Any breach of this policy will be investigated in accordance the Conduct and Disciplinary Policy.

Routine monitoring reports at aggregate level concerning the use of the web-browser may be made available to Directors and Managers on request.

14 REVIEW

This policy will be formally reviewed three years after the approval of this updated policy or earlier depending on the results of monitoring.

15 APPENDICES

Appendix 1 – Email Disclaimer
Appendix 2 – Guidelines on the use of email
Appendix 3 – Further details of legal issues
Appendix 4 – Remote email access
Appendix 5 – The use of Office 365
Appendix 6 – Equality Impact Assessment

17 BIBLIOGRAPHY

- The Legal Guide to Employee Monitoring, Hammonds.
- Email Policy Best Practices: implementing and enforcing email policies to maximise regulatory compliance, Nancy Flynn, 2005.
- How to write an Acceptable Use Policy, Surf Control.
- Employee email and web use: a fresh perspective, Morgan Cole Information Security Team, 2003.
- Email and Internet Policy, Glasgow Caledonian University.
- Internet and Email Acceptable Use Policy, Hampshire Partnership NHS Trust.
- Acceptable use of ICT Facilities Policy, Version 2.0, University of Salford.
- Employment Practices Code, and Supplementary Guidance, the Information Commissioner.

Tameside and Glossop Integrated Care NHS Foundation Trust

APPENDIX 1: EMAIL DISCLAIMER

DISCLAIMER : This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed.

If you are not the intended recipient, please do not disclose, copy or distribute information in this email or take any action on its contents. Any views or opinions expressed are those of the author and do not represent the views of Tameside & Glossop Integrated Care NHS Foundation Trust unless otherwise explicitly stated. The information contained in this email may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this e-mail and your reply cannot be guaranteed.

****

"Please support your hospital and encourage family and friends to become Foundation Trust members via the link below"

https://secure.membra.co.uk/TamesideApplicationForm/

Tameside & Glossop Integrated Care NHS Foundation Trust
Fountain Street
Ashton-Under-Lyne
OL6 9RW
0161-922-6000

APPENDIX 2: GUIDELINES ON THE USE OF EMAIL

1. Introduction

These guidelines apply to everyone in Tameside & Glossop Integrated Care NHS Foundation Trust and should be read in conjunction with the Acceptable Use Policy.

2. The Purpose of Email Guidelines

2.1. Email is increasingly becoming the primary business tool for both internal and external communication and as a result should be treated with the same level of attention given to drafting and managing formal letters and memos. Email messages should not be treated as an extension of the spoken word because their written nature means they are treated with greater authority. As well as taking care over how email messages are written it is necessary to manage email messages appropriately after they have been sent or received.

2.2. There is a common misconception that email messages constitute a temporary form of communication. This misconception about how email messages can be used could result in legal action being taken against Tameside & Glossop Integrated Care NHS Foundation Trust or individual employees. All email messages are subject to Data Protection and Freedom of Information legislation and can also form part of the corporate record. Staff should also be aware that email messages could be used as evidence in legal proceedings or disclosed to another person if they are the data subject of the email. These guidelines set out the obligations all members of staff must observe when dealing with email messages.

2.3. There are two main sections within the guidelines: the first concentrates on sending email messages and the second concentrates on managing email messages that have been sent or received. Staff should ensure that they are familiar with the content of the guidelines and use them as a point of reference when dealing with email messages.

3. Sending emails and when to use email

Email is not always the best way to communicate information as email messages can often be misunderstood, sometimes as a result of email overload, when replies are not always thought through. It is the responsibility of the person sending an email message to decide whether email is the most appropriate method to communicate the information. The decision to send an email should be based on a number of factors including:

- The subject of the message
- The recipient's availability
- The speed of transmission
- The speed of response
- The number of recipients

3.1 The Subject

3.1.1. Email messages can be used for different types of communication and can constitute a formal record of proceedings. The types of communication which email can be used for include general business discussions, disseminating information, agreement to proceed and confirmation of decisions made. Although email can be used for these types of communication, it may be necessary to consider whether the sensitivity of the information would be more appropriately communicated in a different way. Dealing with sensitive subjects in emails is addressed in more detail in section 5.

3.1.2. It should also be noted that there are certain subjects that should be avoided in email messages as they could be construed as discriminatory; this is covered in more detail in the section on email misuse, section 9.2 within the Acceptable Usage Policy.

3.2 Recipient's availability
Email messages are often sent unnecessarily due to the ease and convenience of writing an email message. There are times when email might not be the most appropriate way of communicating with people, for example if a message needs to be passed onto a person in the same office speaking to them face to face might be more productive, particularly if they receive large volumes of email. If the person to whom the message is being delivered is not located in the office it might be better to phone them, depending on the subject or nature of the communication. When a message needs to be communicated to someone who is difficult to locate, for example they work in more than one office, then an email message should be sent in preference to speaking to them either face to face or via the phone.

3.3 Speed of transmission
Email messages can be sent and delivered to the recipient quickly, which makes sending an email message a good way of transmitting information if the information is needed quickly and the recipient is expecting the information. However, where information needs to be communicated as a matter of urgency it is better to use the telephone.

3.4 Speed of Response
Although email message can be sent and delivered quickly there is no guarantee that the message will be read or acted upon immediately. One of the perceived advantages of using email is that it can be responded to at the recipient's convenience. If a message needs to be acted upon immediately or requires a quick decision email is probably not the best way of communicating the information. Where an immediate action or response is required it is probably better to speak to the person directly and send email confirmation if it is deemed to be necessary.

3.5 Number of Recipients
3.5.1. Although email is often considered to be a good way of disseminating information to large groups it should be noted that there are some restrictions. The ability to send an email to everyone in the Organisation is restricted to the Communications Team, IT Services (in case of significant impact on service) and the Executive Directors. If a message needs to be conveyed to everyone, the message should normally be placed on the Intranet on the Home page and the Announcements page, and staff should check these daily at http://tis/pages/default.aspx and http://tis/Pages/Announcements.aspx

3.5.2. If an email needs to be sent to particular divisions or departments, or staff groups (e.g. DNMs, senior managers) please use the pre-set distribution lists.

4. Writing Business Email Messages
Email communications are often perceived as being closer to informal speech rather than formal writing. Emails can be sent quickly and often with little thought regarding their contents. What the sender may construe as acceptable could be construed as rude and abrupt by the recipient. When writing business email messages it is important that consideration is given to the way in which the message is being conveyed. This includes thinking about the title, the text and the addressees. As a way of helping staff to draft emails in an appropriate fashion for business use guidelines to drafting email messages have been developed. These guidelines are intended to be a reference tool. It is up to the sender to decide to what degree to follow the guidelines, depending on their knowledge and level of familiarity with the recipient.

4.1 Subject Line
- Ensure the subject line gives a clear indication of the content of the message.
- Indicate if the subject matter is sensitive.
- Use flags to indicate whether the message is of high or low importance and the speed with which an action is required.
- Indicate whether an action is required or whether the email is for information only.

4.2 Subject and Tone

- Greet people by name at the beginning of an email message.
- Identify yourself at the beginning of the message when contacting someone for the first time.
- Ensure that the purpose and content of the email message is clearly explained.
- Include a signature with your own contact details containing as a minimum:
    - Full name
    - Job title
    - Department
    - Telephone number
    - Work mobile telephone number (if applicable)
- Ensure your signature is not unnecessarily long.
- Ensure that the email is polite and courteous.
- The tone of an email message should match the intended outcome.
- Make a clear distinction between fact and opinion.
- Proofread messages before they are sent to check for errors.
- Try to limit email messages to one subject per message.
- Include the original email message when sending a reply to provide a context.
- Where the subject of a string of email messages has significantly changed start new email message, copying relevant sections from the previous string of email messages.
- Ensure email messages are not unnecessarily long.
- Ensure that attachments are not longer versions of emails.
- Summarise the content of attachments in the main body of the email message.

4.3 Structure and Grammar

- Try to use plain English.
- Check the spelling within the email message before sending.
- Use paragraphs to structure information.
- Put important information at the beginning of the email message.
- Avoid using abbreviations.
- Avoid using CAPITALS.
- Try not to over-use of bold text.
- Do not use emoticons.

4.4 Addressing

- Distribute email message only to the people who need to know the information.
- Using ‘reply all’ will send the reply to everyone included in the original email. Think carefully before using ‘reply all’ as it is unlikely that everyone included will need to know your reply.
- Use the ‘To’ field for people who are required to take further action and the ‘cc’ field for people who are included for information only.
- Think carefully about who should be included in the ‘cc’ field.
- Ensure the email message is correctly addressed.

4.5 General

- Be aware that different computer systems will affect the layout of an email message.
- Avoid sending email messages in HTML format as if an email recipient is using an email system that does not allow HTML the layout will be affected.
- Be aware that some computer systems might have difficulties with attachments.
- Observe the restrictions on attachment size 70mb on local organisation email and 20mb on NHSmail.
- Try not to forward messages unnecessarily.
- Never say anything in an email that you would not say face to face. Correspondence by email should never be used as an alternative to replace communicating with another employee in person.
- The inappropriate use of upper case in email is generally interpreted as ‘SHOUTING’ and should be avoided.
- It is your responsibility to make sure your details, (extension, job title, office location etc) held in the email system is correct and up to date. This includes email signature(s)

5. Dealing with Sensitive Subjects

5.1. The privacy and confidentiality of the messages sent via email cannot be guaranteed. It is the responsibility of all members of staff to exercise their judgement about the appropriateness of using email when dealing with sensitive subjects. Staff are advised that although all external emails have a disclaimer at the footer of the email to protect the Organisation from information being disclosed to unauthorised personnel, there is no guarantee that this will protect individual personnel from potential legal action if emails sent include unsupported allegations, sensitive or inappropriate information.

5.2. Staff must ensure that all information of a sensitive nature that is sent via email is treated with care in terms of drafting and addressing. Sensitive information sent via email that is incorrect might provide a case for initiating legal proceedings against the person sending the information and/or the Organisation. Sensitive information can include commercial information, or information about specific individuals or groups.

5.3. When sending email messages that contain sensitive information the following aspects MUST be considered:

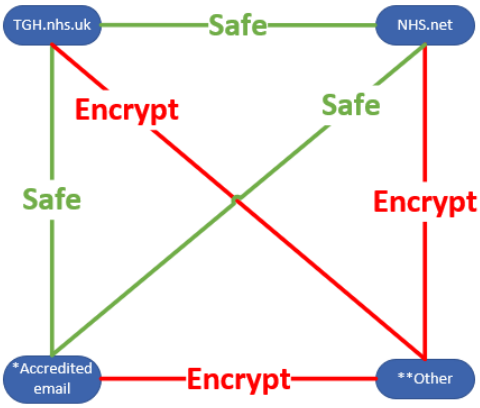
- Email messages containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message, for example an email message containing comments about the performance of a specific staff member or a group of staff. This should decrease the likelihood of the message being forwarded to unintended recipients.
- Email messages containing personal information are covered by the Data Protection Act and must be treated in line with the principles outlined in the Act. Under the Data Protection Act personal information includes opinions about an individual or the personal opinions of an individual. Email messages containing this type of information should only be used for the purpose for which the information was provided, be accurate and up to date, and must not be disclosed to third parties without the express permission of the individual concerned.
- Email messages that contain information that is not supported by fact should indicate that it is the sender's opinion that is being expressed.
- Email messages must be encrypted when personal information is being sent outside the Organisation. The best way to do this is for both sender and recipient to use NHSMail.

6. Sending confidential information outside of the Organisation.

6.1 Staff must take care when sending personal information outside of the organisation via email. Sending personal information must be secure.

It is very important that all staff check that the correct recipients are selected prior to sending using any method. NHSMail is a national system and there are many people with the same name in different organisations across the country.

6.2 Commonly used email routes



* Public bodies/authorities working on the Secure Email Standard. Check before sending

** All others, including public bodies and authorities without the Secure Email Standard. Webmail such as gmail, Yahoo, hotmail, doctors.org

6.2.2 Not all governmental/public departments use secure NHS accredited email accounts. The sender must check prior to sending any personal information outside of the organisation. Personal information that is sent out to personal webmail accounts must be protected adequately. For instance, using encryption or password protecting the data.

NHS Digital have compiled a list of organisations that have attained the NHS accredited email standards https://digital.nhs.uk/services/nhsmail/the-secure-email-standard#list-of-accredited-organisations

6.2.3The password should be given over the telephone to the recipient, and never in the same email or separate email.

6.2.4 Staff should refer to the intranet on how to encrypt documents. Alternatively, contact the IT Department for more information.

7. Managing Email Messages

7.1 Reasons for Organising your Mailbox

7.1.1. It is the responsibility of all members of staff to manage their email messages appropriately. It is important that email messages are managed in order to comply with Data Protection and Freedom of Information legislation. Managing email messages appropriately will also mean that work can be conducted more effectively as it will help to locate all the information relating to specific areas of business.

7.1.2. To manage email messages appropriately members of staff need to identify email messages that are records of their business activities as distinct from non-urgent/less important email messages, e.g. availability for meetings, thank yous.

7.1.3. It is important that email messages that are records are moved from personal mailboxes and managed with, and in the same way as other records. Email messages should be managed within the mailbox and kept only for as long as required before being deleted. Mailbox stores should not be used as a filing system. They should be house kept regularly to ensure mailbox stores are not overloaded with unnecessary emails.

7.2. Making your Mailbox Manageable

7.2.1. Managing an email mailbox effectively can appear to be a difficult task, especially if the volume of email messages received is regularly of a large quantity. Managing an email mailbox should not be about following rigid classification guidelines; it is about following a methodology that works best for the individual.

7.2.2. There are a number of approaches that might aid the management of email messages, including:

- Allocating sufficient time each day or week to read through and action email messages.
- Prioritising which email messages need to be dealt with first.
- Looking at the sender and the title to gauge the importance of the message.
- Flagging where you have been ‘cc’d’ into email messages. These messages are often only for informational purposes and do not require immediate/any action.
- Setting rules for incoming messages so they can automatically be put into folders.
- Using folders to group email messages of a similar nature or subject together so they can be dealt with consecutively.
- Identifying email messages that are records or need to be brought to other people’s attention.
- Keeping email messages in personal folders only for short-term personal. information. Emails that are required for longer purpose should be managed as records.
- Deleting email messages that are kept elsewhere as records.
- Deleting email messages that are no longer required for reference purposes from the in and out box.

8. Management of Shared Mailboxes

8.1.1. Shared mailboxes should be used where there are a group of people responsible for the same area of work. Where there are a group of people responsible for the same work using a shared mailbox can be a way of ensuring that queries are answered quickly when members of the team are away from the office. Access to a shared mailbox is initially given by request to the IT Service Desk and can then be granted by the person who owns the mailbox.

8.1.2. When managing shared email mailboxes, the sections of this email policy relating to, 'reasons for organising your mailbox', 'making your mailbox manageable' and 'identifying and managing email records' should be adhered to. There will also need to be some additional rules relating to when to delete an email message from the mailbox, how to identify an email message as having been answered and the types of email messages that should be treated as records. While it is the responsibility of the owner to ensure that there are specific rules relating to the management of shared mailboxes it is the responsibility of all staff members with access to shared mailboxes to abide by those rules.

8.1.3. It is important to remember that any email that made a significant contribution to the discussion of the business being conducted should be kept as a record and not just the final conclusions. The discussions that take place in the mailbox folder will represent the context within which the final decision was made and must be maintained as a record of the proceedings.

8.2 Identifying an owner

When a shared mailbox is created one person must be identified who can take ownership of the mailbox. The owner should be responsible for developing rules governing how email messages are responded to and how this is communicated to other people using the shared mailbox. It should be noted that the IT Services Department has overall responsibility for maintaining shared mailboxes. If the owner has any specific problems with managing the shared mailbox these should be discussed with the IT Services Department.

8.3 The purpose

The creation of a shared mailbox should be done with a specific purpose, for example to answer queries on a particular subject. It is the responsibility of the owner of the shared mailbox to ensure that the mailbox is used for the specified purpose and to take appropriate action if it is not.

8.4 Access

For shared mailboxes access should only be granted to people who are able to answer the email enquiries that will be received. In shared mailboxes it might also be necessary for the owner to delegate some responsibility to other people who are granted access in terms of managing the emails and ensuring the mailbox is used for its specified purpose. In terms of people sending messages to the mailbox it will be necessary to ensure that a message is given to people who might want to send enquiries giving the email address and the purpose of the mailbox.

9. Identifying and managing email records

9.1 Essential Principles

Email messages can constitute part of the formal record of a transaction. All members of staff are responsible for identifying and managing emails messages that constitute a record of their work. When an email is sent or received a decision needs to be made about whether the email needs to be retained as a record.

9.2.1 Identifying Email Records

A record is 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.' When deciding whether an email message constitutes a record, the context and content of the email message needs to be considered. A guiding principle on identifying email records might be that as soon as the email message needs to be forwarded for information purposes it should be considered as a record. Email messages that might constitute a record are likely to contain information relating to business transactions that have or are going to take place, decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction. For example, during the decision to put out a tender document for a particular service, background discussion about what this should and should not include might take place via email and should be kept as a record.

9.2.2 Who is Responsible?
As email messages can be sent to multiple recipients there are specific guidelines to indicate who is responsible for capturing an email as a record:

- For internal email messages, the sender of an email message, or initiator of an email dialogue that forms a string of email messages.
- For messages sent externally, the sender of the email message.
- For external messages received by one person, the recipient.
- For external messages received by more than more person, the person responsible for the area of work relating to the message. If this is not clear it may be necessary to clarify who this is with the other people who have received the message so that it is unnecessary for all recipients to retain it.

10. Managing Email Records with Attachments

10.1.1. Where an email message has an attachment, a decision needs to be made as to whether the email message, the attachment or both should be kept as a record. The decision on whether an email and/or its attachment constitute a record depends on the context within which they were received. It is likely that in most circumstances the attachment should be kept as a record with the email message as the email message will provide the context within which the attachment was used.

10.1.2. There are instances where the email attachment might require further work, in which case it would be acceptable to keep the email message and the attachment together as a record and keep a copy of the attachment in another location to be worked on. In these circumstances the copy attachment that was used for further work will become a completely separate record.

11. When and Where to Manage Email Records

11.1 When to keep
Most email messages will form part of an email conversation string. Where an email string has formed as part of a discussion it is not necessary to keep each new part of the conversation, ie every reply, separately. There is no need to wait until the end of the conversation before capturing the email string as several subjects might have been covered. Email strings should be kept as records at significant points during the conversation, rather than waiting to the end of the conversation because it might not be apparent when the conversation has finished.

11.2 Where to keep
Personal mailboxes should not be used for long-term storage of email messages. Personal mailboxes should be used for personal information or short-term reference purposes, when these emails are no longer required they should be deleted. Please refer to the Corporate Records Management Policy for record retention details.

12. Cyber Security

12.1 The cyber security threat continues against both public and private computer based services. All users of Organisation IT services must be vigilant when viewing websites and emails.

The creation of email messages with a forged sender address is known as ‘spoofing’. This means that some emails purporting to originating from the Organisation or partner organisations look to be safe and acceptable. Phishing is a technique employed by scammers to gain access of your computer/network, or to gain financial information usually via ‘spoofed’ email.

The NHS has recently fallen victim to ransomware which most likely originated as a phishing attack. Here are some warning signs to look for when receiving emails. Remember not to open any attachments or click on any links if they do not look right. Report any suspected attacks to the IT Service Desk.

12.2 Ways to identify spoof/phishing emails.

- Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious. Create a new email using a known email address to clarify if the email received is legitimate. If it is not, delete it from your inbox and deleted folder.
- Check for generic information. For example, an email asking for you to check and approve the attached invoice when you ordinarily do not approve invoices is likely to be suspicious.
- If the email asks for you complete or action something that you have no prior knowledge of.
- Do not click on attachments or web addresses on emails that you are not expecting.
- Do not respond to an email that you consider to be questionable even if from a believed friendly source, hackers can spoof email addresses. Report all suspected spoof emails to the IT Service Desk.

APPENDIX 3: FURTHER DETAILS OF LEGAL ISSUES

Email is admissible as evidence in a court of law and messages can be classified as legal documents. Internal emails may also need to be disclosed under the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and the Freedom of Information Act 2000. Emails should be treated like any other communications and care should be taken to ensure that the content is accurate, and the tone is appropriate.

The ICFT is entitled to access to the contents of your mailbox, sent/received messages or other audit data as required to support information governance processes, investigations, and/or subject access requests without your prior consent.

1. Employee Monitoring

Under the Regulation of Investigatory Powers Act 2000, and the Telecommunication (Lawful Business Practice) (Interception of Communications) Regulations 2000, employers can monitor communications on a private network, either with the consent of all parties to the communications, or for a specific reason, complying with the criteria set out in the Act and Regulations.

2. Defamation and Libel

Defamation law protects the reputation of individuals and corporate organisations. It includes libel (a more permanent statement, which would cover email and web defamation) and slander (a transient statement).

Facts concerning individuals or organisations must be accurate and verifiable, and views or opinions must not portray their subjects in any way that could damage their reputation. Web pages and email messages are regarded as published material.

Each repetition of the statement may be a fresh defamation, so what may have been intended as a joke for a limited audience could spread across the Organisation and beyond, each time possibly attracting a court action.

3. Confidentiality

The Organisation has a duty to protect the confidential information that it holds about patients and staff. The law surrounding confidentiality is constantly developing, but the essential elements are found in the common law duty of confidentiality, and the Data Protection Act 2018. The Act is based on a set of principles relating to the fair and lawful handling of data and requires that the Organisation has appropriate organisational and technological measures in place to safeguard the personal data that it processes. Failure to comply with the Act attracts penalties ranging from fines to criminal sanctions for directors.

4. Discrimination and Harassment

The Organisation has a duty to provide its staff with a safe place of work. Failure to do this means that an employee can resign and then claim constructive dismissal. The Organisation could be found liable for stalking, sexual, or racial discrimination if it fails to prevent stalking, sexual, or racial harassment, and there is no maximum limit for compensation for such harassment.

5. Obscenity

The Obscene Publications Act 1959 makes it an offence to publish, distribute, circulate, or sell any article, sound, film, record, picture (including cartoon images) or photograph that is obscene or the effect of which would "deprave and corrupt" those likely to read, see or hear the material. It is not an offence merely to hold pornography, unless it relates to children, but distributing or showing it is.

The Protection of Children Act 1978 makes it illegal to make indecent images of children and show them. The Criminal Justice Act 1998 created the offence of mere possession of an indecent image of a child. The Criminal Justice and Public Order Act 1994 added pseudo photographs (computer generated images or those that alter images of adults to look like children). Downloading or emailing child pornography is deemed to be making an image or showing it.

The Organisation, as employer, may be vicariously liable for the crimes of its employees, e.g. in circumstances where a manager encourages or condones the crime. The Organisation will be liable for a corporate criminal offence under the Protection of Children Act if the crime occurred with the consent or connivance of or was attributable to the neglect on the part of any director, manager, secretary or other officer of the Organisation. That officer will also be personally liable as well as the employee who committed the offence.

6. Copyright Infringement

Under the Copyright, Designs and Patents Act 1988 and subsequent regulations, any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of his/her rights. This includes copyright MP3 files, books, diagrams, photographs etc. Staff must not make, transmit or store an electronic copy of copyright material on the Organisation network without the permission of the author.

7. Computer Misuse Act 1990

It is a criminal offence to gain unauthorised access to a computer system to make any unauthorised modification of computer material (including the introduction of a computer virus) or to interfere with any computing system provided in the interests of health and safety.

8. Data Protection Act 2018

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Under the Data Protection Act all data subjects have the Right of Access. This gives data subjects the right to request their personal information.

It is important to remember Subject Access Requests are not limited to patient records, but also include emails regarding individual's, employment, and/or management. The Data Protection Policy manages the non-health records. Health records are managed via the Subject Access Policy.

Care must be taken when sending emails or documents which contain sensitive subjects relating to individuals who have the right to view information including emails relating to them.

It is a criminal offence under the Data Protection Act if personal information is deliberately deleted or amended after a Subject Access Request has been placed. Additionally, action could be taken by the Information Commissioner's Office including fines and undertakings.

9. Data Security & Protection Toolkit

The Data Security & Protection Toolkit replaced the previous Information Governance toolkit in April 2018. The toolkit is an online self-assessment tool that enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards.

All organisations that process to NHS personal data and systems must use the toolkit to provide assurances they are practising good data security standards and personal information is handled correctly. The Secure Email Standard DCB1596 requires the ICFT continually meets the Data Security & Protection Toolkit requirements the email service.

10. Litigation Hold

Litigation Hold or Hold Orders is a state where all processing on an email account where:

- Emails are removed, deleted, or destroyed;
- Emails are amended, edited

A litigation hold may be placed on your account, if there is a legal requirement. If this is the case, you will not be permitted to amend or delete emails.

If there is a requirement place a Litigation Hold IT will contact you with the reason behind the hold.

APPENDIX 4: REMOTE EMAIL ACCESS

The following specifically relate to those using Office 365 remotely. Remotely means on any device Organisation owned or privately owned and includes personal mobile devices.

All connections must be in accordance with the Remote Computer Working Policy

Personal confidential information must not be stored on any device not owned by the Organisation. This includes but is not limited to:

- Mobile phones;
- Tablet devices;
- Privately owned laptops/desktops, for instance privately owned by the account holder of their family;
- Non-Organisation owned, for example library device;
- Commercial company.

Following a suspected breach or incident involving a mailbox the Organisation may seek to wipe the device remotely with little or no warning. This may extend to your personal device if you have installed or use Organisation email.

It is the account holder's responsibility to ensure all data relating to the Organisation is removed prior to leaving the organisation. Failure to complete this may incur the device to be remotely wiped with little or no warning.

Devices with Organisation email installed may be subject to Subject Access Requests. The Organisation may instruct staff to search for personal confidential information.

APPENDIX 5: THE USE OF OFFICE 365

Office 365 gives staff many benefits including ease of use and the ability to access emails on a myriad of platforms, even without connecting remotely to the ICFT's services. The ICFT has gained assurance for the use of a secure email standard. To ensure that this standard is enforced users of the service must maintain excellent standards when processing data.

1. When accessing your email account from a non-corporate device i.e. a home computer, personally owned laptop, or in an internet café, you should only access the service via the web at https://www.office.com and not through an email programme such as Microsoft Outlook, unless you have explicit permission from the IT Department to do so.

2. Do not save any personal identifiable information on personal or non-corporate devices. Any devices which is believed to store personal identifiable information locally may be remotely wiped, (the whole device) without warning.

3. In the event of a theft or loss of device which has Office 365 the owner must contact the IT department without undue delay to report the incident. If the device has been stolen a crime reference number will be required. The IT Department will remote wipe the device without warning.

4. If you are accessing Office 365 from a non-corporate device i.e. a home computer, personally owned laptop, or in an internet cafe, you do so on the understanding that the connection is managed appropriately and securely being careful not to save the password when logging in and ensuring that the connection is securely severed without any ICFT information saved to a non-ICFT device.

5. All non-corporate devices must have up-to-date and reasonable security measures in place to ensure that all ICFT data remains confidential, available, and has integrity.

6. If using Teams or collaborating on shared documents staff are reminded not amend, delete, or disclose any documents without a legitimate relationship or reason to do so.

7. ICFT IT administrators are entitled to view and access files and folders when supporting incidents.

8. Information Governance Department retains the right to audit and access files and folders when supporting an investigation, audit, Subject Access Request (DPA18), or via the Freedom of Information Act request.

Tameside and Glossop Integrated Care NHS Foundation Trust

APPENDIX 6: EQUALITY IMPACT ASSESSMENT

Name of Policy: Internet & Email Acceptable Use Policy

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

.