Information Communication & Technology (ICT) Policy

Birmingham and Solihull Mental Health NHS Foundation Trust

Policy number and category	**IG02**	**Information Governance**
Version number and date	**5**	**February 2025**
Ratifying committee or executive director	**Trust Clinical Governance Committee**	
Date ratified	**March 2025**	
Next anticipated review	**March 2028**	
Executive director	**Executive Director of Finance**	
Policy lead	**Head of ICT**	
Policy author *(if different from above)*	**ICT operations Manager**	
Exec Sign off Signature (electronic)	XXXX	
Disclosable under Freedom of Information Act 2000	**No**	

POLICY CONTEXT:

The ICT Policy (ICTP) has been developed to protect the Trust and its employees from hazards and threats, to ensure business continuity and to minimise any business damage by preventing and reducing the impact of information systems incidents.

POLICY REQUIREMENT

- To ensure the effective operation of information systems and that those systems are delivered when and where they are needed, by maintaining their confidentiality, integrity and availability.
- Ensuring that all members of Trust staff and any Trust appointed contractors are aware of and comply with the relevant legislation as described in this and other associated policies.
- Describing the principles of security and explaining how they shall be implemented in the Trust.
- To introduce a consistent approach to information and cyber security within the Trust, ensuring that all members of staff understand their own responsibilities.

- Creating and maintaining, within the Trust, a level of awareness of the need for information security as an integral part of the day to day business.

- Protecting information that is stored within, on or by assets under the control of the Trust.

Change Record

Date	Version	Author (Name & Role)	Reasons for review / Changes incorporated	Ratifying Committee
January 2025	**5.21**	**XXXX ICT operations Manager**	**Three Yearly Review** **Added a new section 3.4 to cover Artificial Intelligent** **Added into e-mail section 3.30.14 regarding personal use of NHS mail**	**Trust Clinical Governance Committee**

Contents Page

1: Introduction

Rationale

This document defines the Information Communication & Technology Policy (ICTP) for Birmingham and Solihull Mental Health NHS Foundation Trust, hereafter known as BSMHFT. It forms a key component of BSMHFT overall information governance management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

The ICTP applies to all Trust business and covers the information, information systems, networks, and physical environments where information is processed or stored.

The objectives of this ICTP are to ensure the effective operation of information systems and that those systems are delivered when and where they are needed. It will preserve:

Confidentiality

Access to data shall be confined to those with appropriate authority.

Integrity

Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

Availability

Information shall be available and delivered to the right person, at the time when it is needed.

Scope

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by BSMHFT by:

- Ensuring that all members of staff are aware of and comply with the relevant legislations, security guidance and other associated policies.
- Describing the principles of security and explaining how they shall be implemented in the Trust.
- Introducing a consistent approach to security, ensuring that all members of staff understand their own responsibilities.
- Creating and maintaining within the Trust, a level of awareness of the need for information and cyber security as an integral part of the day to day business.

- Protecting information assets under the control of the Trust.

Principles

This policy applies to all staff in relation to the use of electronic devices, information assets and any other storage media such as:

- Encrypted USB memory sticks
- Computers (PC or Laptops)
- Cameras
- Dictaphones
- Smart phone
- Tablets
- Any information systems such as Rio, ESR, E-mail etc.

'The Trust positively supports individuals with learning disabilities and ensures that no-one is prevented from accessing the full range of mental health services available. Staff will work collaboratively with colleagues from learning disabilities services and other organisations, in order to ensure *that service users and careers have a positive episode of care whilst in our services. Information is shared appropriately in order to support this.'*

2: The Policy

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications, end user devices and networks owned or held by BSMHFT by:

- Ensuring the effective operation of information systems and that those systems are delivered when and where they are needed, by maintaining their confidentiality, integrity and availability.
- Ensuring that all members of Trust staff and any Trust appointed contractors are aware of and comply with the relevant legislation, security guidance and other associated policies.
- To introduce a consistent approach to information and cyber security within the Trust, ensuring that all members of staff understand their own responsibilities.
- Creating and maintaining, within the Trust, a level of awareness of the need for information and cyber security as an integral part of the day to day business.
- Protecting information that is stored within, on or by assets under the control of the Trust.
- All Staff must complete all mandatory information governance and cyber security awareness training annually.
- User login or account credentials and Smartcards should not be shared.
- All Trust staff should not access any confidential or sensitive information unless they have a legitimate reason to do so.
- All staff must not store any valuable, confidential and sensitive data locally on any end user devices such as computers, laptops, tablets, smartphones etc. All data should be stored on a Trust file server or other network storage systems.

- It is the responsibility of all Trust staff to maintain passphrase (password) security, by following the Trust password and or security guidance.

3: The Procedure

3.1. Staff must not store any valuable, confidential and sensitive data locally on any end user devices such as computers, laptops tablets, smartphones etc. All data should be stored on a Trust file server or other network storage systems.

3.2. All Trust staff must have completed the Trust Induction process, completed an Information Technology Access Form (ITAF), and be registered on the Trust's Electronic Staff Record (ESR) system before being allowed any access to Trust information systems and hardware, see **Appendix 2**.

3.3. A separate ITAF is required for 3rd Party organisation employees working within the Trust, see **Appendix 3.**

3.4. Responsibilities for Information Security

3.4.1. Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Trust business. All staff are responsible for information security and remain accountable for their actions in relation to NHS and other UK Government information and information systems. Staff shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action.

3.4.2. The responsibility for the security of an information system lies with the Information Asset Owner(s). IAO's are responsible for:

- Understanding what information is held.
- Knowing what is added and what is removed.
- Understanding how information is moved.
- Knowing who has access and why.

Owners of information systems may delegate the operational running of security to an Information Asset Administrator(s) but remain ultimately accountable for that system. The Head of Information Governance (IG) will advise and monitor ownership. A detailed list of information systems and owners will be kept by the IG Department and monitored by the Senior Information Risk Officer (SIRO).

3.4.3. Line Managers are responsible for ensuring that their permanent or temporary staff, contractors and volunteers are aware of:

- The information security policies and procedures applicable in their work areas.
- As per Information Governance Guidelines about their personal responsibilities for information security, refer to Confidentiality Policy.

3.4.4. Line managers are individually responsible for the security of their physical environments where information is processed or stored.

3.4.5. Each system user will comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

3.4.6. When systems from third parties are to be implemented, underpinning contracts will be introduced to ensure that the staff or sub-contractors of the third party shall comply with all appropriate security policies. All requests such as this must use the Trust ICT Request for Change (RFC) process and be ratified by the ICT Change Advisory Body, see **Appendix 4** for RFC process.

3.5. Legislation and NHS Mandatory Requirements

3.5.1. BSMHFT is obliged to abide by all relevant UK legislation. The requirement to comply with this legislation shall be devolved to employees and agents of BSMHFT who may be held personally accountable for any breaches of information security, for which they may be held responsible, see **Appendix 7** for a list of Legislation.

3.5.2. The Trust will abide by the Department of Health (DoH) and the Health & Social Care (HSCIC) Codes of Practice, Statement of Compliance and Data Security and Protection Toolkit.

3.6. Management of Security

3.6.1. At Trust Board level, responsibility for information security resides with the SIRO.

3.6.2. The Information Security Manager is responsible for implementing, monitoring, documenting and communicating security requirements for the Trust.

3.7. Information Security awareness training

3.7.1. Information security awareness training must be included in the staff induction process.

3.7.2. An on-going awareness programme will be maintained in order to ensure that staff awareness is refreshed and updated as necessary. This will be delivered to Trust staff in a number of mediums from Intranet notices, Briefings, Global E-mails, SnapComms, Statutory and Mandatory training, policy and procedural updates.

3.8. Contracts of Employment

3.8.1. Staff information security responsibilities are addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause.

3.8.2. Information security expectations of staff are included within appropriate job definitions.

3.9. Security Control Assets

3.9.1. Each Information Asset, (hardware, software, application or data) has a named Information Asset Owner (IAO), who is responsible for the information security of that asset. There is a suite of documentation that must be completed in order to register an information asset, and the Information Governance Team must be informed about an information asset in order to support and review the completion of the documentation.

3.9.2. Any ICT asset not used must be returned to the ICT department immediately.

3.10. Access Control to Secure ICT Areas

3.10.1. Only authorised personnel who have a justified and approved business need will be given access to restricted areas containing information systems or electronic data storage hardware. Each area should have a secure access keypad or lock that is accessible to ICT staff members and the appropriate on-site staff, where necessary. When access to the area is required, an entry will be recorded in the Access Control Log found in each area. This may also be monitored by the CCTV system.

3.11. Computer/Systems Access Control

3.11.1. Access to computer systems is restricted to authorised users who have a business need. Access is controlled initially by the Trust's IT Access Form (ITAF) with rights to specific systems ratified by the employee's line manager.

3.11.2. Staff who leave the employment of the Trust will have their access to Information Systems revoked via the IT domain account deletion process. This is covered by the Trust ICT Leavers and Movers Process.

3.11.3. ICT system access is monitored and recorded.

3.12. Registration Authority (RA) and Management

3.12.1. RA Smartcards are the primary access/token device utilised within NHS Trusts to access NHS National systems. Please refer to IG09 Registration Authority Policy on the Trust Connect pages.

3.12.2. The RA Smartcard is for use by authorised NHS Personnel who have agreed to the National Policy, Care Record guarantee, NHS Confidentiality Code of Practice and RA Terms and Conditions (T&C) and have been individually sponsored by a BSMHFT RA Sponsor and registered by the BSMHFT RA Team.

3.12.3. Access to information systems via RA Smartcard should be based upon role, area of work and activities per role. Smartcards should not be shared or used to access information if the user does not have a legitimate reason to do so.

3.12.4. The RA Team monitors the use of the RA Smartcard and will report any breaches to the organisations Risk Management Team, RA Manager and Executive Management Team any breaches may result in disciplinary action being taken in line with the Trust disciplinary policy.

3.13. Password Management

3.13.1. Computer passwords (passphrase) used to access any computer systems or software are confidential. It is the responsibility of all Trust staff to maintain password security. Under no circumstances are passwords to be divulged, shared with anyone or left in a public place.

3.13.2. The Trust operates a policy which allows 8 attempts at a passphrase to access a Trust PC device before locking the user account for 30 minutes before another attempt can be made.

3.13.3. Users are automatically logged out of Trust PC's after 4 hours of inactivity to avoid session takeover and save system resources.

3.13.4. Trust Computer Passwords (passphrase) must be a minimum of 12 characters and will require changing every 183 days, see **Appendix 6** for password and passphrase guidelines.

3.14. Password Changing

3.14.1. **All system and device passwords should be changed regularly in accordance with system requirements.**

3.15. Password Protection

3.15.1. Passwords must always be treated as confidential information. As stated above, no employee should give, tell or hint at their password to another person. This includes ICT staff, administrators, managers and colleagues:

- If someone demands your password refer him or her to this policy and report the incident to your line manager who will escalate to the ICT team
- Don't leave your passwords written down.
- Don't leave your passwords where others can find them electronically. Never store passwords in a text file or send them in Email.
- Do not share your password.

Important:

No one from ICT or other departments should ever ask you for your password. The ICT Service Desk uses a passphrase scheme similar to internet banking when dealing with passwords for the Trust Network.

Failure to comply with or adhere to the password management as defined above and in Password guidelines in Appendix 6 may result in disciplinary action. Please refer to the Trusts Disciplinary policy

Further information can be obtained from the ICT Service Desk on (0121 301) 5111.

3.15.2. All Trust social media accounts must have strong passphrases (passwords) and implement MFA were possible.

3.16. Multi Factor Authentication (MFA)

3.16.1. Multi Factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, MFA is a core component of a strong identity and access management and will be used to access Trust resources whenever possible. See **Appendix 13** for more information on MFA and the Trust resources that current require MFA for Access.

3.17. Use of Information Systems

3.17.1. All users of information systems are responsible for ensuring their use is appropriate and care is taken to maintain and protect the integrity and quality of the data held on that system.

3.17.2. Staff should ensure that where service users are present in an area where systems are used, they do not come into contact with any login IDs or passwords. Staff should ensure that confidential information is protected and secured at all times. Service users should not, under any circumstances, use Trust PCs.

3.18. Application Access Control

3.18.1. Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier. 3.18.2. Access to information systems is controlled initially by the Trust's ICT Access Form with rights to specific systems ratified by the employee's line manager. Access to further systems should be processed through the Trust ICT Request for Change (RFC) process.

3.18.3. Users will need to have completed any appropriate ICT training before accessing clinical systems, see **Appendix 12.**

3.19. Equipment Security

3.19.1. In order to minimise loss or damage to ICT assets, equipment shall be physically protected from threats and environmental hazards. For example, information systems are housed within secure Comms rooms locked with a key or secure number keypads. Access to such areas is restricted to authorised personnel only. Authorised staff entering these areas must complete an access control log detailing time of entry, exit and the nature of the work being carried out. Access control logs are regularly audited and reviewed by ICT senior staff. Desktop equipment is protected by secure access to the areas in which they are held and in more vulnerable areas by security cages.

3.19.2. Staff who use Trust ICT equipment outside of Trust business premises shall take appropriate precautions to avoid damage or theft of equipment. Trust ICT equipment should not be left in vehicles overnight.

3.20. Equipment Disposal

3.20.1. ICT equipment disposal is subject to NHS Guidelines for the disposal of IT Equipment and the Waste Electrical and Electronic Equipment (WEEE) legislation. BSMHFT has an approved process for the disposal of ICT equipment to ensure that data is securely destroyed, and confidentiality is maintained.

3.21. Information Risk Assessment

3.21.1. Once identified, information security risks shall be managed on a formal basis. They shall be recorded within an ICT Information Risk Register which forms

part of the overall Trust Risk Register. The ICT Information Risk Register is reviewed at the Information Governance Steering Group (IGSG) meeting, quarterly with the ICT SIRO and is reported back to the Risk Management Committee. Any implemented information security arrangements shall also be a regularly reviewed feature of BSMHFT risk management annual programme, via the same procedure.

These reviews shall help identify lessons learnt and best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

The reporting of information security incidents is included on incident training and as part of the information governance induction, which is mandatory for all staff.

3.22. Information Security Events and Weaknesses

"Serious incidents that occur on health/social care premises or on other premises where health/social care is provided to a person, and where service users and others are affected, that may result in death or has the potential to cause serious harm (serious near miss) or where the actions of health/social care staff are likely to cause public concern".

3.22.1. All information security events and suspected weaknesses are to be logged via Eclipse. Refer to RS02 The Reporting, Management & Learning from Incident Policy, available on Connect under Policies and Procedures.

3.23. Data Protection / Confidentiality

3.23.1. BSMHFT has a designated Confidentiality Policy, IG01 Confidentiality Policy, which is located on Connect under Policies and Procedures. In addition, the Trust has a Data Protection Officer, who is the Head of Information Governance.

3.24. Data Storage

3.24.1. Sensitive or confidential data SHOULD NOT be stored locally on PCs or laptops (C:\ drive).

3.24.2. All Trust staff with access to a computer have a home drive (H:\), this drive is for information that staff need to access but is not relevant to other members of their team or department.

3.24.3. There are departmental and cross departmental shared drives that use other letters of demarcation, where information that is relevant to that team, department or other departments. Any information that is stored in these shared drives is for shared access within the department.

3.24.4. In the event of a network outage, any Trust information should be saved to Trust issued encrypted USB sticks. Further advice regarding Trust Standard secure USB sticks can be found on the ICT Services page on the Trust Intranet or via the ICT Service Desk.

3.25. Protection from Malicious Software (Computer Viruses)

3.25.1. BSMHFT use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff are expected to co-operate fully with this policy. Users shall not install software on BSMHFT PCs or laptops unless specific permission via ICT has been granted. Data files generated or updated outside of the Trust on external media such as CDs, DVDs etc. are potentially dangerous therefore they should not be used without first contacting the IT Service Desk to ensure they are safe.

3.25.2. Should a virus be detected on any PC, any use should cease, and the incident must be reported ***immediately*** to the ICT Service Desk on 0121 301 5111.

The ICT Department will log and action the incident and advise when the PC can be used.

3.25.3. An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis by system owners.

3.25.4. The Trust has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of National security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above Act and the Human Rights Act 1998 and will be subject to authorisation by the Associate Director responsible for ICT.

3.26. Accreditation of Information Systems

3.26.1. BSMHFT shall ensure that all new information systems, applications and networks have been registered as an information asset, with an identified Information Asset Owner, and have in a place a Business Continuity Plan (BCP), a System Level Security Plan (SLSP) and an ICT Support Model before they commence operation.

3.26.2. All departments must involve ICT when evaluating, trialling and procuring any information system (hardware and software). ICT will then ensure that all technical and Information Governance aspects of the system are taken into consideration. All New systems must be approved via the System strategy Group (SSG) before implemented into the Trust Information System estate.

3.27. System Change Control

3.27.1. Changes to information systems, applications or networks shall be reviewed and approved by the Trust's Change Advisory Board (CAB) as part of the Trust's RFC process.

3.27.2. As part of any system / network device implementation or replacement, default system/ device passwords **must be changed** and should comply were possible with the Trust Passphrase requirements.

3.28. Software Licensing

3.28.1. BSMHFT monitor all software licenses and ensure that all information products are properly licensed and approved by the CAB. Users shall not install software or applications on BSMHFT ICT equipment. Should a requirement arise, the request should follow the Trusts' RFC process and be ratified by the CAB.

3.29. Data Encryption and the use of Mobile or Portable Devices

The NHS Chief Executive has clearly stated that no personal identifiable information or other sensitive data should be stored or transported unencrypted on any portable media. In a further statement it was stated that 'any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted to 'NHS standards'.

3.29.1. All laptops have been encrypted.

3.29.2. No personal identifiable data should be stored on any Trust laptop, PDA or mobile phone.

The Trust has introduced a standard secure USB memory stick for use on Trust PCs and laptops. This device is available via the ICT Service Desk. These sticks are issued with guidance but essentially, they will allow staff to transfer (not store) sensitive information between Trust sites and store nonsensitive information.

No USB Memory Sticks other than the BSMHFT standard secure memory stick can be used in BSMHFT IT Equipment.

The use of cameras, camera phones or other similar recording equipment is prohibited within the Trust without the permission of senior management or as defined within staff job roles. This applies particularly to clinical areas or where Service Users may be in attendance.

The ability to access mass storage devices in Trust PCs and laptops has been disabled and only Trust issued USB sticks and cameras are permitted. Mass storage devices include, but are not limited to, the following items:

- External Hard Drives
- Media Cards such as SD, XD and MMC
- Non-Trust Issued USB Sticks
- Cameras
- MP3 players.

3.30. Electronic Mail (E-mail) Use

3.30.1. Electronic mail (E-mail) is the primary digital method of communicating within BSMHFT and has been provided to aid the provision of health and social care and this should be your main use of the service. BSMHFT use the national NHSmail system (nhs.net).

3.30.2. All employees of BSMHFT should ensure that information communicated via E-mail is accurate, and the email is being sent to the correct recipient. Care should also be taken to ensure that the E-mail cannot be misconstrued.

3.30.3. E-mail communication is considered another form of publishing and therefore defamation law applies, see **Appendix 8**.

3.30.4. The Trust issues guidelines for the use of the corporate E-mail system, which can be viewed on the ICT Connect pages. NHSmail guidelines are available see **Appendix 14** for links to NHSmail polices and guidance.

3.30.5. Staff contact details are provided in the NHSmail Directory to support the delivery of health and care - these details will be shared across the NHSmail address book and approved, federated 3rd party organisations.

3.30.6. All data retained within the service remains the property of BSMHFT. Details about the management of data within the E-mail service is detailed within the Transparency Information.

3.30.7. BSMHFT ICT Team maintains day to day administration responsibility for your E-mail account.

3.30.8. Where accounts are no longer used, they are automatically removed after a period of inactivity as defined in the NHSmail policies

3.30.9. You must not attempt to disguise your identity, your sending address or send E-mail from other systems pretending to originate from the NHSmail E-mail service. Where there is a need to provide someone else with the ability to send E-mail on your behalf, this should be done via the delegation controls within the service.

3.30.10. You must not send any material by E-mail that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic. If you need to transmit sexually explicit material for a valid clinical reason, then you must obtain permission from your local Caldicott Guardian.

3.30.11. You must not use E-mail service to harass other users or groups by sending persistent E-mails to individuals or distribution lists.

3.30.12. You must not forward chain E-mails or other frivolous material to individuals or distribution lists.

3.30.13. Patient or sensitive data should not be stored in calendar appointments - this is essential to ensure data is not accidentally seen by inappropriate colleagues.

3.30.14. All communication you send through the NHSmail services is assumed to be official correspondence from you acting in your official capacity on behalf of your organisation. Should you need to, by exception, send communication of a personal nature you must clearly state that your message is a personal message and not sent in your official capacity.

3.31. E-mail Security

3.31.1. As E-mail is the primary digital method of communicating both internally and externally to the Trust, all staff need to be mindful of the sensitivity of the data they are transferring (particularly patient identifiable information) via E-mail and that data is secure. **Appendix 5** details the various E-mail routes that can be used in the Trust and whether they are secure.

3.31.2. Ensure you establish contact via other means before exchange of any confidential or sensitive information.

3.31.3. If you need to exchange sensitive data outside of BSMHFT to other E-mail systems that do not comply with the DCB1596 secure E-mail standard or the pan-government secure E-mail standard, the E-mail must be encrypted. Instructions on how to do this can be found on the ICT help pages.

3.32. E-mail Inbox and Storage

3.32.1. The E-mail system is a communication tool to support the secure exchange of information and is not designed as a document management system. Documents, E-mails or messages that are required for retention/compliance purposes should be stored within BSMHFT's document management system in accordance with Records Retention policies. It is the mailbox owner's responsibility to ensure the mailbox is kept within quota to avoid restrictions being imposed and impacting business processes.

3.33. E- Mail Information Governance requirements

3.33.1. The General Medical Council (GMC) Good Medical Practice guidance requires doctors to keep clear, accurate and legible records. It is important that E-mails do not hinder this. You should ensure that any relevant clinical data contained in E-mails is immediately documented in the patient record. This could mean that the E-mail is saved into the patient record, or a synopsis of the conversation is entered. Failure to do so could have implications on patient safety.

3.33.2. BSMHFT is entitled to seek access to the contents of your mailbox, sent/received messages or other audit data as required to support information governance processes without your prior consent. Such requests are strictly regulated.

3.34. Owners of shared mailboxes responsibilities

3.34.1. Knowing who are the members of the shared mailbox and why.

3.34.2. Understanding the purpose of the shared mailbox that they are owners of.

3.34.3. Removing ownership from staff who should no longer need to be allocated as owners

3.34.4. Removing members access to the shared mailbox if the member no longer works for the Trust or has moved to a different team within the Trust and no longer require access.

For more information on Shared mailboxes see **Appendix 16**

3.35. Using BSMHFT services to exchange sensitive information.

3.35.1. The E-mail service is a secure service. This means NHSmail is authorised for sending sensitive information, such as clinical data, between organisations using NHSmail and:

- Other E-mail systems that comply with the Data Coordination Board (DCB)1596 secure E-mail standard

- Other E-mail systems that comply with the pan-government secure Email standard.

A full list of approved services can be found in **Appendix 10.** If you intend to use the service to exchange sensitive information you should adhere to the guidelines in **Appendix 9**.

3.35.2. You should make sure that any exchange of sensitive 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.

3.35.3. Caldicott Guidelines and local Information Governance principles should apply whenever sensitive information is exchanged.

3.35.4. As with printed information, care should be taken that sensitive or personal information is not left anywhere it can be accessed by other people, e.g. on a public computer without password protection.

3.35.5. When you are sending sensitive information, you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time-sensitive information such as referrals.

3.35.6. If you accidentally share sensitive or patient data with an incorrect recipient, it is your responsibility to report this in line with your local information governance policies and processes. This is a local data breach and should be treated accordingly. You should always try and recall the email immediately after realisation that it has been sent to the wrong recipient. Follow this up with a separate email to the wrong recipient asking them to confirm they have not received the email, and if they have, ask them to confirm deletion.

3.35.7. If personal identifiable information is visible to other people, it is your responsibility to make sure those people have a valid relationship with the person. If they do not, you must secure the information, so it is no longer visible.

3.35.8. You must always be sure you have the correct contact details for the person (or group) that you are sending the information to. If in doubt, you should check the contact details in the BSMHFT directory or NHS Directory.

3.35.9. If it is likely, you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

Remember that personal information is accessible to the data subject i.e. the patient, under General Data Protection Regulation (GDPR) legislation.

3.36. Bulk Data Transfer

3.36.1 The Trust regularly has a requirement to transfer sensitive data to official organisations for example, patient data to Commissioners for reporting purposes. This carried out using a Secure FTP (Fixed Transfer Protocol) system which is completely secure. All requests for this form of transfer are facilitated by the IT team. Please contact the Service Desk on 0121 301 5111 for further information.

3.36.2 There are some guidelines on the steps that are to be followed when setting up a FTP contact with a partner organisation. To obtain a copy of the guidelines, please follow the RFC process.

3.37. BSMHFT Internet and Intranet Facilities

3.37.1 The Internet/Intranet facility is provided by BSMHFT to help staff perform their work, so that they can access information, do specific work-related research, learn about the application of new ideas/technologies and evaluate these effectively for potential benefits of the BSMHFT and its clients/staff alike.

3.37.2 The Internet service also exposes the Trust to potential threats (e.g. copyright violations; Infection by viruses, defamation, pornography and sexual harassment proceedings etc.). The Trust monitors all internet traffic and will disclose any information to line managers where there is a suspicion of improper internet use. The Trust internet is also filtered, so that access to any sites that are not Trust business related or improper are blocked.

3.37.3 If there is a website that is blocked and there is a Trust business reason for it to be allowed, a request can be sent to the ICT to have the website opened.

3.37.4 Guidelines on the use of the Internet is included in the Trust's Network Access Form which is completed and signed by all employees prior to access to the Trust's network, information systems, Internet and Intranet, which are located on the ICT pages within Connect. Employees will be held personally liable for any deviation from this Intranet/Internet policy and it is in the employee's interest to adhere to this.

3.37.5 The Trust has a service known as "Internet Access for Service Users". This allows service users to access the Internet under controlled conditions. Its use is regulated by a Local and Trustwide policy and any deviation from those policies will be reported to the appropriate manager and may result in the removal of the service to the relevant individuals or groups.

3.38. Microsoft 365 (M365)

3.38.1 Microsoft 365 is BSMHFT's primary digital method of producing documentation, M365 is a cloud-based service that contains a suite of applications such as Outlook, Word, Excel, PowerPoint, and using collaboration services such as Microsoft Teams to provide mobility and better collaboration to aid the provision of health and social care. BSMHFT ICT Team is responsible for the administration of the licenses and licensed administrative obligations in accordance with all relevant NHS or BSMHFT policies. You should ensure that you only use M365 for this purpose and in an appropriate manner.

3.38.2 All employees of BSMHFT should ensure that information documented via M365 is accurate and care is taken to ensure that information cannot be misconstrued.

3.38.3 Under the Enterprise Agreement (EA) all data stored in M365 is retained by Microsoft while our EA is valid. Files that have been deleted by BSMHFT staff are retained for 90 days and then permanently removed.

3.38.4 Where accounts are no longer used, they are automatically removed after a period of inactivity as defined in the NHS or BSMHFT policies.

3.38.5 Information stored in applications such as Teams, SharePoint and OneDrive are still subject the policies outlined in the NHS or BSMHFT policies and therefore should be planned and managed effectively to ensure the data:

- Is valued and trusted.
- Is available and can be shared with anyone who may need it.
- Is secured and protected.
- Meets NHS or BSMHFT policies.

3.39. M365 Security

3.39.1 Patient or sensitive data contained in M365 should not be stored on any personal devices. This is essential to ensure the data is not accidentally exposed to those that should not see it.

3.39.2 BSMHFT Staff are responsible for protecting their M365 account and password from exposure.

3.40. Artificial Intelligence Applications (GenAI)

3.40.1 Specialist AI and machine learning applications, tools and techniques must only be used in the Trust as part of projects, or under operational procedures, explicitly approved through formal Trust governance processes.

3.40.2 Standard 'Generative AI' applications, such as Microsoft Copilot or ChatGPT, or those built into approved Trust software, may be used routinely to support Trust business. However, to maintain the security of our data and IT systems, and to avoid potential data leaks or security incidents, employees must adhere to the following:

- Do not use Trust credentials, email addresses, or telephone numbers as a login to publicly available Generative AI applications.
- Do not install Application Programming Interfaces (APIs), plug-ins, connectors, or software related to Generative AI systems without explicit ICT approval.
- Do not implement, run or use on Trust systems in any other way any software or computer code generated by Generative AI. Employees who write and use code as a formal part of their role may, however, use Generative AI to create draft code provided it is fully reviewed and validated before use.

3.40.3 To maintain the confidentiality of our Trust's sensitive information, including but not limited to employee and patient personal information, our intellectual property, and copyrighted material, employees and contractors must only share information with approved parties in accordance with associated data sharing agreements. To maintain confidentiality:

- Do not enter personal information of employees, patients, or other third parties into any Generative AI application. Treat the application

as you would an employee of another company with whom we have no formal relationship.

- Do not input Trust intellectual property into generative AI applications.
- Do contact your manager if you are unsure whether information you are planning to input falls into any of the above categories.
- Do review the Trust's acceptable use policy, data protection policy, data breach policy and procedures for reporting data breaches.

3.40.4 To protect our employees and clients from harm, and to protect the Trust from reputational damage, employees must only use Generative AI in ways consistent with BSMHFT's policies and procedures. All text and any other output generated using Generative AI must be reviewed thoroughly by the person planning to use or distribute it before such use or distribution in the same way as content created in more traditional ways. All content must be reviewed and edited as necessary before use to ensure it is factually accurate, fit for its intended purpose, and not inappropriate, discriminatory or otherwise harmful to our employees or patients.

To protect our employees, patients, and the Trust:

- Do review output created using Generative AI applications to make sure it meets the Trust's standards of equity, ethics, and appropriateness.
- Do not use any output that discriminates against individuals based on race, colour, religion, sex, national origin, age, disability, marital status, political affiliation or sexual orientation.
- Do not use Generative AI applications to create text, audio, or visual content for purposes of committing fraud or to misrepresent an individual's identity.
- All employees and contractors are expected to comply with applicable laws, regulations, and Trust policy regarding use or development of Generative AI content or tools, and failure to do so may result in disciplinary action.

3.40.5 Where Generative AI is used in generating content for publication or other sharing external to the Trust, including with patients, it must be considered whether the use of the Generative AI application should be cited, either to maintain transparency with patients and employees or to protect the Trust from claims against copyright infringement and/or theft of intellectual property. When considered necessary, a clearly visible note should be added to the document describing how it was created.

Where a Generative AI tool is used to help summarise any conversation or meeting, participants should be made aware in advance that the meeting will be recorded with that intention. The record produced must indicate the use of Generative AI in its creation and must be checked thoroughly for accuracy and

absence of inappropriate, discriminatory or otherwise harmful content before distribution.

For further information on Generative AI framework for HM Government see **appendix 17**

For Trust approved AI engines see **appendix 18**

3.41. Breach of Policy and Enforcement

3.41.1. Any breach of this policy will be investigated fully and may result in disciplinary action being taken in line with the Trust disciplinary HR01 Disciplinary Policy on the Trust Connect pages under Policies & Procedures.

3.41.2. Staff should be aware of the Trust Anti-fraud, Bribery and Corruption policy (CG22) section 2.7 which refers to Computer Misuse (under the Computer Misuse Act 1990)

The Computer Misuse Act 1990 includes such offences as:

- Unauthorised access to computer material, which includes ID and password misuse, to alter, copy delete or move a program or data or simply to output a program or data, laying a trap to obtain a password.
- Unauthorised access to a computer with intent, this includes gaining access to financial or administrative records.
- Unauthorised modification of computer material including destroying another's files creation of a virus, introduction of a virus and any deliberate action to cause a system malfunction.
- Any examples of the above must be reported to the Head of Information Security and the CFS. (Counter Fraud Service)

4: Responsibilities

Defined responsibilities relevant to the policy:

Post(s)	Responsibilities	Ref
All Staff	To be aware and put in practice their Information Governance responsibilities in regard on information Security. Information Security awareness Training is undertaken. Passwords must never be divulged and meet password construction Standards.	**3.4.4** **3.20.1, 3.25.2** **3.13, 3.14 3.15, 3.16.2**

	It is your responsibility to check that you are sending E-mail to the correct recipient, as there may be more than one person with the same name using the service. Always check that you have the correct E-mail address for the person you wish to send to. This can be done by checking their entry in the BSMHFT Directory.	
	All staff should comply with all UK legislation relating to Information security. see appendix 7.	
	Should follow E-mail usage guidelines. See appendix 11	
	Staff are responsible for the security of their Trust device.	**3.18.2**
Service, Clinical and Corporate Directors	For ensuring that their staff is aware of their responsibilities and for ensuring the physical and logical security of in the environment in which their teamwork.	**3.6**
Information Governance Team	Support Information Asset Owners, and ensure that information assets are registered	
Information Asset Owners	Information Asset Owners ensuring the information security of their system.	**3.4.3, 3.9.1, 3.20.1**
Policy Lead	Ensuring this policy is up to date and reviewed appropriately.	
Executive Director	The Senior Information Risk Officer (SIRO) is responsible for assuring the governance of Information security.	**3.20.1, 3.6.1**
Others	HR will ensure all staff have a contract of employment with a confidentiality clause.	**3.8**

5: Development and Consultation Process

Consultation summary	
Date policy issued for consultation	November 2024
Number of versions produced for consultation	1

Committees / meetings where policy formally discussed	Date(s) ICT managers meeting 17th Oct, ISAG meeting 13th Nov
Information Security Assurance Group	Monthly – second Thursday of the month.

Where received	Summary of feedback	Actions / Response

6: Reference documents

- Trust documentation

Link	Description
All forms for these services can be found at the following link on the Trust Intranet: **ICT Forms (sharepoint.com)**	Disposal of ICT Equipment
	ICT Access Form
	ICT Purchasing
	ICT Request for Change
Learning and Development Portal (sharepoint.com)	Statutory and mandatory training
http://connect/corporate/governance/riskmanagement/Pages/default.aspx	Risk Management

- **The General Medical Council (GMC) Good Medical Practice**
- **NHSmail**

7: Bibliography

None

8: Glossary

Acronyms	Description
ARD	Azure Remote Desktop
BSMHFT / 'The Trust'	Birmingham and Solihull Mental Health Foundation Trust

CAB	The Change Advisory Body consists of representatives of the ICT Management team and, where necessary, invited Information Asset Owners. The function of the CAB is to ensure all changes to IT services and systems are managed to minimise the impact of the change and assess business need. The CAB has final sanction on whether a request for change can progress.
HSCIC	Health & Social Care Information Centre
DoH	Department of Health
FTP	Fixed Transfer Protocol
IG	Information Governance
IGSG	Information Governance Steering Group
IAR	Information Asset Register
IAO	Information Asset Owner
IAA	Information Asset Administrator
ICT	Information, Communication and Technology
ICTP	ICT Policy
ITAP	Information Technology Access Form
RA	Registration Authority
RFC	ICT Request for Change. For further information on the Trust's RFC please visit the ICT pages on Connect.
MFA	Multi Factor Authentication
SIRO	Senior Information Risk Owner
WEEE	Waste Electrical and Electronic Equipment
E-Mail	Electronic mail

9: Audit and assurance:

Element to be monitored	Lead	Tool	Frequency	Reporting Arrangements
Number of Security Breaches	Head of ICT	ICT Service Delivery System	Monthly	ISAG Meeting
System Reports	Azur Remote Desktop and Direct Access (DA) Lead	Azure Remote Desktop Reports DA System Reports	Monthly	Service Delivery Team Meeting

10. Appendices

Appendix 1 - Equality Analysis

Equality Analysis Screening Form

A word version of this document can be found on the HR support pages on Connect
http://connect/corporate/humanresources/managementsupport/Pages/default.aspx

Title of Policy	**ICT Policy**		
Person Completing this policy	XXXX	**Role or title**	ICT Operations Manager
Division	Corporate	**Service Area**	ICT
Date Started	10/10/24	**Date completed**	11/10/24
Main purpose and aims of the policy and how it fits in with the wider strategic aims and objectives of the organisation.			
Main purpose and aims of the ICT policy and how it fits in with the wider strategic aims and objectives of the organisation.			
Who will benefit from the policy?			
All Trust staff and 3rd parties accessing the Trust ICT network			
Does the policy affect service users, employees or the wider community? ***Add any data you have on the groups affected split by Protected characteristic in the boxes below. Highlight how you have used the data to reduce any noted inequalities going forward***			
BSMHFT and 3rd party staff who access the ICT network			
Does the policy significantly affect service delivery, business processes or policy? *How will these reduce inequality?*			
No			
Does it involve a significant commitment of resources? *How will these reduce inequality?*			

No

Does the policy relate to an area where there are known inequalities? (e.g. seclusion, accessibility, recruitment & progression)				
No				
Impacts on different Personal Protected Characteristics – *Helpful Questions:*				
Does this policy promote equality of opportunity? *Eliminate discrimination?* *Eliminate harassment?* *Eliminate victimisation?*				*Promote good community relations?* *Promote positive attitudes towards disabled people?* *Consider more favourable treatment of disabled people?* *Promote involvement and consultation?* *Protect and promote human rights?*
Please click in the relevant impact box and include relevant data				
Personal Protected Characteristic	**No/Minimum Impact**	**Negative Impact**	**Positive Impact**	**Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.**
Age	x			It is anticipated that age will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their age.
Including children and people over 65 Is it easy for someone of any age to find out about your service or access your policy? Are you able to justify the legal or lawful reasons when your service excludes certain age groups				
Disability	x			It is anticipated that disability will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their disability.

Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families?				
Gender	x			It is anticipated that Gender will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their gender.
This can include male and female or someone who has completed the gender reassignment process from one sex to another Do you have flexible working arrangements for either sex? Is it easier for either men or women to access your policy?				
Marriage or Civil Partnerships	x			It is anticipated that marriage or civil partnerships will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their marriage or civil partnership.
People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?				
Pregnancy or Maternity	x			It is anticipated that pregnancy or maternity will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their pregnancy or maternity.
This includes women having a baby and women just after they have had a baby Does your service accommodate the needs of expectant and post natal mothers both as staff and service users? Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity?				

Race or Ethnicity	x			It is anticipated that race or ethnicity will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their race or ethnicity.
Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees What training does staff have to respond to the cultural needs of different ethnic groups? What arrangements are in place to communicate with people who do not have English as a first language?				

Religion or Belief	x			It is anticipated that religion or belief will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their religion or belief.
Including humanists and non-believers Is there easy access to a prayer or quiet room to your service delivery area? When organising events – Do you take necessary steps to make sure that spiritual requirements are met?				
Sexual Orientation	x			It is anticipated that sexual orientation will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their sexual orientation.
Including gay men, lesbians and bisexual people Does your service use visual images that could be people from any background or are the images mainly heterosexual couples? Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea?				
Transgender or Gender Reassignment	x			It is anticipated that transgender or gender reassignment will not have an impact in terms of discrimination as this policy ensures that all affected by this should be treated in a fair, reasonable and consistent manner irrespective of their transgender or gender reassignment.

This will include people who are in the process of or in a care pathway changing from one gender to another Have you considered the possible needs of transgender staff and service users in the development of your policy or service?				
Human Rights	x			This policy is written to promote remove any discrimination to ensure that everyone can fulfil their full potential within a Trust that is inclusive, compassionate, and committed. This is keeping in line with our Trust values, the NHS People's Plan commitment to equality, diversity and inclusion and reflects the provisions of the Equality Act 2010.

				This policy applies to **all**, including applicants applying for a job, staff including agency, bank and volunteers,
Affecting someone's right to Life, Dignity and Respect? Caring for other people or protecting them from danger? The detention of an individual inadvertently or placing someone in a humiliating situation or position?				
If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)				
		No		
What do you consider the level of negative impact to be?	**High Impact**	**Medium Impact**	**Low Impact**	**No Impact**
				x

If the impact could be discriminatory in law, please contact the **Equality and Diversity Lead** immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required. If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the **Equality and Diversity Lead** before proceeding. If the policy does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the **Equality and Diversity Lead.**
Action Planning:
How could you minimise or remove any negative impact identified even if this is of low significance?
Leads will work to reduce any reported of detrimental impact experienced
How will any impact or planned actions be monitored and reviewed?
Feedback from reports of concern, Regular audits and policy updates and communications to ICT managers through meeting and committees
How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.
The Policy will be promoted in ways accessible to all staff
Please save and keep one copy and then send a copy with a copy of the policy to the Senior Equality and Diversity Lead at bsmhft.edi.queries@nhs.net. The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis

Appendix 2 - ICT Access Form (IAF)

ICT Access Form (IAF)

Appendix 3 – Third Party IT Access Form

Third Party ICT Access form

Appendix 4 – Request for Change (RFC) Form

A system change request can be made via ICT Self-Service Portal

Further information can be found on the **Request for Change** page on Connect.

Appendix 5 – Secure E-mail Paths

When sending email from NHSmail to another secure service you do not need to A any action.

You will know if you have an NHSmail email address because it will end in nhs.net.

Please note that nhs.uk systems that have not met the accreditation standards are not considered secure.

The table below is a summary of email addresses that are known/not known to be secure:

Recipient email address ends	Secure	Additional actions required
*.nhs.uk (listed **here as** accredited to the DCB1596 secure email standard).	Yes	Secure
All email domains that are accredited to the DCB1596 secure email standard, listed in **the secure email standard**	Yes	Secure
*.nhs.uk (not accredited to the DCB1596 secure email standard)	Unknown	Use [secure] in the subject line
*.gov.uk	Yes	Secure
*.cjsm.net	Yes	Secure

*.police.uk	Yes	Secure

Recipient email address ends	Secure	Additional actions required
*.mod.gov.uk	Yes	Secure
*.parliament.uk	Yes	Secure
Any other email address (not listed in **the secure email standard** as accredited to the DCB1596 secure email standard)	Unknown	Use [secure] in the subject line

Link **Guidance for sending secure email (including to patients) - NHS Digital**

Information on sending a secure e-mail can be found here:
http://connect/corporate/ICT/servicedelivery/SitePages/Info%20-%20Sending%20Secure%20E-mail.aspx

Appendix 6 – Passphrase Construction:

Passwords are a critical part of information security. They serve to protect systems and the information stored upon them.

The purpose of these guidelines is to set a standard for creating, protecting and changing passwords. All Trust staff should take appropriate steps to ensure that they create strong (complex), secure passwords and safeguard them at all times. Poorly chosen passwords, if compromised, could put the information stored on the Trust's systems at risk.

Password Construction:

Choosing passwords can sometimes present a dilemma. Ideally, a password should be complex and as hard as possible for somebody to guess, but at the same time be simple enough for you to remember. A simple strategy for creating a memorable but difficult-to-crack password is to **use a passphrase**.

A passphrase is a sequence of words and characters strung together. The difference is that a passphrase is typically longer and uses a combination of words and/or characters that only make sense to you and is easy to remember. Creating a strong passphrase is easy, see examples below:

- mydogfido’IS7
- Yellowcat”baseball
- MyVacation2paris
- soexcitedtoFinish!

Notice how each of these is a fairly simple phrase. By stringing together a couple of words we’ve created passphrases that are random and more complex. Including a

few symbols, numbers, or uppercase letters somewhere in the passphrase will also increases its strength.

A well-chosen phrase is difficult to crack.

Further information can be found on the ICT Cyber Security Connect Pages **Password Guidelines**

Appendix 7 - Legislation

- The Data Protection (Monetary Penalties) Regulations 2010 (SI 2010/31 and SI 2010/910)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2008
- Access to Health Records Act 1990
- The Data Protection Act2018 (DPA, UK GDPR)
- The Defamation Act of 2013
- Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
- The Environmental Information Regulations 2004 (SI 2004/3391)
- Criminal Justice and Immigration Act 2008
- The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208).
- Protection of Freedoms Act 2012

Appendix 8 – Defamation

E-mail Defamation

E-mail has become the modern tool for sending messages whether it is for personal or business use, you are constantly connected with everyone from around the world. It easy to forget that E-mails are not always kept private and confidential. You should be cautious when it comes to sending content. You should refrain from attacking people privately or stating things you would not say or do in person or over the phone. Defamatory E-mails can be forwarded to various sources either by mistake or on purpose creating a complicated matter from an unintentional consequence.
Defamation requires publication such as an E-mail from a verified E-mail account. This means when you are writing a defamatory statement about someone, you are authorising publication of that E-mail. All E-mails thereafter

are considered a new publication and any other person who forwards or shares that E-mail may be implicated in any resulting cases.

E-mails should be treated as any other channel of information and nothing should be written in an E-mail you would not want to be shared publicly. What you may write as a joke, may be considered offensive to others. E-mails can be forwarded and passed around very quickly so please think twice before presuming your content is confidential.

Deleting or retracting an E-mail does not protect you from defamation as messages are stored on the server of the company and can be recalled from the archive by the IT department or IT specialist.

Definitions of defamation

1. You should be on guard against making statements which could be defamatory.

   A defamatory statement is one which injures the reputation of another person: it "tends to lower him in the estimation of right-thinking members of society generally[1]".

2. Such a statement constitutes a "libel" if it is:

published (publication for these purposes, is simply the communication of the defamatory matter to a third person)

- in writing, print or some other permanent form.

3. A statement will amount to a "slander" if it is
   - published; and
   - made orally or in some other transient form.

4. An action for defamation can be brought by:
   - an individual.
   - a company, in respect of statements that damage its business reputation.

5. An action for defamation cannot be brought by a Local Authority nor by any other public authority.

6. Section 1(1) of the 2013 Defamation Act introduced a new test which provides that a statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant. This is qualified by s 1(2) in that for the purposes of the section, harm to

the reputation of a body that trades for profit is not "serious harm" unless it has caused or is likely to cause the body serious financial loss.

Appendix 9 – Guide for sending sensitive data

1. You should make sure that any exchange of sensitive 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.
2. Caldicott and local Information Governance principles should apply whenever sensitive information is exchanged.
3. As with printed information, care should be taken that sensitive or personal information is not left anywhere it can be accessed by other people, e.g. on a public computer without password protection.
4. When you are sending sensitive information, you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time-sensitive information such as referrals.
5. If you accidentally share sensitive or patient data with an incorrect recipient, it is your responsibility to report this in line with your local information governance policies and processes. This is a local data breach and should be treated accordingly.
6. If personal identifiable information is visible to other people, it is your responsibility to make sure those people have a valid relationship with the person.
7. You must always be sure you have the correct contact details for the person (or group) that you are sending the information to. If in doubt, you should check the contact details in the BSMHFT directory or NHS Directory.
8. If it is likely you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.
9. Remember that personal information is accessible to the data subject i.e. the patient, under General Data Protection Regulation (GDPR) legislation.

Appendix 10 – Approved list for sending emails from NHSmail

Link to NHS mail Secure email standards including current accredited organisations:

The secure email standard - NHS Digital

Approved list for sending emails from NHSmail (June 2023)

Organisation Name	Domain name
NHS	nhs.net
UK Government	gov.uk
Ministry of Justice	cjsm.net
Police	pnn.police.uk
Ministry of Defence	mod.uk
Parliament	parliament.uk
Ambulance Radio Programme	arp.nhs.uk
Berkshire Healthcare NHS Foundation Trust	berkshire.nhs.uk
Blind Veterans UK	blindveterans.org.uk
BMI Healthcare	bmihealthcare.co.uk
BMI Healthcare	bmichoice.co.uk
BMI Healthcare	bmidecontamination.co.uk
BMI Healthcare	ghg.co.uk
BMI Healthcare	circlerehabservices.co.uk
BMI Healthcare	circlehealthgroup.co.uk
BMI Healthcare	bmihd.co.uk
Bolton NHS Foundation Trust	boltonft.nhs.uk
Bradford District Care NHS Foundation Trust	bdct.nhs.uk
Bradford Teaching Hospitals NHS Foundation Trust	bthft.nhs.uk
Bradford Teaching Hospitals NHS Foundation Trust	yhhiec.nhs.uk
Bradford Teaching Hospitals NHS Foundation Trust	yhia.nhs.uk
Bupa	bupa.com

Bupa	richmond-villages.com
Cambridgeshire and Peterborough NHS Foundation Trust	cpft.nhs.uk
Caring Homes Group	caringhomes.org
Caring Homes Group	consensussupport.com
Cumbria, Northumberland, Tyne & Wear NHS Foundation Trust	cntw.nhs.uk
Dorset County Hospital NHS Foundation Trust	dchft.nhs.uk
Earl Mountbatten Hospice	mountbatten.org.uk
East Midlands Medical Services	emmshealthcare.uk
East of England Ambulance Service NHS Trust	eastamb.nhs.uk
Four Seasons Health Care Group	fshc.co.uk
Four Seasons Health Care Group	brighterkind.com
Four Seasons Health Care Group	huntercombe.com
Four Seasons Health Care Group	fshcgroup.com
Genomics England	genomicsengland.co.uk
Gloucestershire Health and Care NHS Foundation Trust	glos-care.nhs.uk
Gloucestershire Health and Care NHS Foundation Trust	ghc.nhs.uk
Greater Manchester Mental Health NHS Foundation Trust	gmmh.nhs.uk
Health Education England	hee.nhs.uk
James Paget University Hospitals NHS Foundation Trust	jpaget.nhs.uk
Maria Mallaband Care Group	cwch.com
Maria Mallaband Care Group	mmcg.co.uk
Maria Mallaband Care Group	kingsmanorcarehome.co.uk
Maria Mallaband Care Group	windsorcourtcarehome.co.uk
Methodist Homes	mha.org.uk
Mid Cheshire Hospitals NHS Foundation Trust	mcht.nhs.uk
Millbrook Healthcare	Millbrookhealthcare.co.uk
Millbrook Healthcare	Ultimatehealthcare.co.uk
Milton Keynes University Hospital NHS Foundation Trust	mkuh.nhs.uk
NHS England & Improvement	cmu.nhs.uk
NHS England & Improvement	england.nhs.uk
NHS England & Improvement	improvement.nhs.uk
NHSmail	nhs.net

NHSX	nhsx.nhs.uk
Norfolk and Suffolk NHS Foundation Trust	nsft.nhs.uk
Norfolk Community Health and Care NHS Trust	nchc.nhs.uk
North Bristol Trust	nbt.nhs.uk
North East London NHS Foundation Trust	nelft.nhs.uk
Northumbria Healthcare NHS Foundation Trust	northumbria-healthcare.nhs.uk
Northumbria Healthcare NHS Foundation Trust	nhct.nhs.uk
Northumbria Healthcare NHS Foundation Trust	northumbria.nhs.uk
Northumbria Healthcare NHS Foundation Trust	nepssg.nhs.uk
Nottinghamshire Health Informatics Service	notts-his.nhs.uk
Nottinghamshire Healthcare NHS Foundation Trust	nottshc.nhs.uk
Nuffield Health	nuffieldhealth.com
Nuffield Health	nuffieldhealthpartners.com
Oxford Health NHS Foundation Trust	oxfordhealth.nhs.uk
Quanta Dialysis Technologies	quantadt.com
Somerset NHS Foundation Trust	somersetft.nhs.uk
Southern Health NHS Foundation Trust	southernhealth.nhs.uk
South West London and St George's Mental Health NHS Trust	swlstg.nhs.uk
South West London and St George's Mental Health NHS Trust	swlstg-tr.nhs.uk
Staffordshire and Shropshire Health Informatics Service	sshis.nhs.uk
Stockport NHS Foundation Trust	stockport.nhs.uk
Sunrise Senior Living	sunrise-care.co.uk
Sunrise Senior Living (Gracewell)	gracewell.co.uk
Surrey and Borders Partnership NHS Foundation Trust	sabp.nhs.uk
Sussex Partnership NHS Foundation Trust	sussexpartnership.nhs.uk
Sussex Partnership NHS Foundation Trust	spft.nhs.uk
Tameside and Glossop Integrated Care NHS Foundation Trust	tgh.nhs.uk
University Hospitals of Leicester NHS Trust	uhl-tr.nhs.uk
WCS Care	wcs-care.co.uk
Weldricks Ltd	weldricks.co.uk
West Midlands Ambulance Service University NHS Foundation Trust	wmas.nhs.uk
West Suffolk NHS Foundation Trust	wsh.nhs.uk

Appendix 11 – E-mail guidelines

Information Governance Email Guidance v1.01

Appendix 12 – ICT Training

Training Course Information

Appendix 13 - Multi Factor Authentication (MFA)

Resources using MFA:

- Azure Remote desktop
- NHS Mail for Local administrator account
- Trust Social media accounts

Appendix 14 - NHSmail Policy and guidance web links

- NHS Mail Policy homepage: **Policy – NHSmail Support**
- Information Acceptable Use Policy AUP: **Acceptable Use Policy – NHSmail Support**

Appendix 15 - M365 web links for further information

- **https://portal.nhs.net/Home/AcceptablePolicy - Your responsibilities**
- Data Retention and Information Management Policy – Office 365 – NHSmail Support

Appendix 16 – Shared mailbox guide for NHS mail

- **Shared Mailbox Guide for NHSmail – NHSmail Support**

Appendix 17 – Generative AI framework for HM Government

- **Generative AI framework for UK Government**

Appendix 18 Approved AI engines

- ChatGPT
- Co Pilot
- Gemini