Bridgewater
Community Healthcare
NHS Foundation Trust

Information Technology (IT) Acceptable Use Policy (AUP)

Policy Number	**IT/Pol/003**
Target Audience	**All Bridgewater Staff and Contractors**
Lead Executive Director	**Director of finance/senior information risk owner**
Recommending Committee/Group	**Digital Information Governance and Information Technology**
Approving Committee(s)	**Corporate Clinical Policy Group**
Ratifying Committee	**Corporate Clinical Policy Group**
Date First Approved	**December 2015**
Last Full Review Date	**November 2023**
Next Full Review Date	**November 2026**
Extension approved until	**N/A**
Lead Author(s)	**Information Governance Manager, Head of IT**
Version Number	**4.0**

Applicable Statutory, Legal or National Best Practice Requirements	ISO/IEC 27001, Code of Practice for Information Security Management Computer Misuse Act (1990) Freedom of Information Act (2000) Regulation of Investigatory Powers Act (2000) Human Rights Act (1998) Equality Act (2010) UK GDPR and Data Protection Act (2018) Regulation of Investigatory Powers Act (2000)

The Trust is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust’s intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Document retention – lifetime of the Trust or 20 year review
Document owner –Information Governance Manager, Head of IT

Version Control Sheet

Version	Date	Reviewed By	Comment
3.0	Nov 2020 Nov 2020 Dec 2020 Dec 2020 Dec 2020	J. Hogan DIGIT Corporate Clinical Policy Group James Hogan S. Arkwright	Reviewed Sign-off agreed Approved subject to minor amendments and final chair approval Minor amendments completed Approved by chair action
3.1	October 2022	S Ormesher on behalf of DIGIT	11.1 Pando app is the preferred method of communications. WhatsApp is not to be used to PID.
3.2	November 2022	Jimmy Cheung	Approved by chair action
3.3	Sept 2023	Information Governance Manager	Full review
3.4	Sept 2023	M. Corkery	Reviewed, comments made
3.5	3/10/23	DIGIT	Appoved
3.6	October 23	M. Corkery	Further comments
4.0	November 23	Corporate Clinical Policy Group	Approved

Equality impact assessment
Consider if this document impacts/potentially impacts:

- Staff
- Patients
- Family members
- Carers
- Communities

Yes □ **complete box A**	**No** ☒ **complete box B**
Box A Contact the Trust's equality & inclusion manager at: **Email: ruth.besford@nhs.net** **Date contacted:**	**Box B** Complete details below: **Name: Policy author** **Email: bchft.ig.nhs.uk** **Date: 5.10.23**

Education & Professional Development Question

In order to ensure that any training requirements are discussed, and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements.
Please answer the following question by entering a cross in the box below:

	Yes	**No**
Does this document have any additional training requirements or implications?		X

If you have answered **YES** you must forward a copy of this document to Education & Professional Development **before** submitting to the Policy Officer.
Date submitted to Educations & Professional Development: ……………………………
No further action is required if you have answered NO.

This table below must be completed in full for audit and governance purposes. Please note documents will be returned if section 1 in the table below is not completed fully. This will result in a delay in listing the document for approval.

Name of document	IT Acceptable Use Policy (AUP)
Document number	IT/Pol/003
Document author	Sharon Ormesher
Section 1 - actions required by author	**Authors response**
Date proposal form submitted to policy officer (new documents)	n/a
Date proposal form presented to CCPG (new documents)	n/a
Date proposal approved by CCPG (new documents)	n/a
Date literature search/reference review requested	n/a
Date EqIA considered	Yes See date above
Date additional training requirements considered	Yes See date above
Date fraud-proofed by the Anti-Fraud Specialist (AFS) if applicable	Sent as part of consulation, no response
Date template accessed on the Hub Add 'OFFICIALSENSITIVE: COMMERCIAL' to front cover if the document can be shared on the internet Add 'OFFICIALSENSITIVE: PERSONAL' to appendices if they include or will include personally identifiable information (PID)	Add date
Date literature review completed (check references are formatted correctly, and hyperlinks working)	N/A
Date first draft submitted to policy officer for initial review	04/09/23
Date returned by policy officer following initial review	15/09/23
Date submitted to key individuals/groups/subject matter experts for comments (add names and designations of responders to consultation table)	Sept 23
For clinical documents, date document submitted to consultation group for sign-off i.e., IPC, Medicines Management (this applies if the document contains medication or medical gases - update version control sheet to confirm sign-off)	N/A
Name of Recommending Committee/group	DIGIT
Date sent to Recommending Committee/group for sign-off	3/10/23
Date signed-off by the Recommending Committee/group (upda version control sheet once signed-off)	03/10/2
Date submitted to policy officer for listing at CCPG	06/10/23
Section 2 – for completion by the policy officer	
Date approved by CCPG	13th November 2023
The following policies require Board approval and must be submitted to Board following CCPG approval: • Risk Management Framework Policy • Health & Safety Policy • Policy and procedure for the production, approval and ratification of Trust-wide policies and procedures ("Policy for Policies") Date submitted for Board approval: Date approved by Board:	N/a

Contents

1 Introduction 6

2 Definitions 7

3 Abbreviations 8

4 Other relevant procedural documents 8

5 Roles and responsibilities 9

6 Equipment 12

7 Acceptable use 13

8 Managing and protecting information 13

8.1 Users' musts "do" 13

8.2 Users must not "don'ts" 14

9 User ID's and passwords 14

9.1 Users' musts "do" 14

9.2 Users must not "don'ts": 15

10 IT equipment including mobile phones/telephones 15

10.1 Users' musts "do" 15

10.2 Users must not "don'ts" 16

11 Software and applications (Apps) 17

11.1 Users' musts "do" 17

11.2 Users must not "don'ts" 17

12 Acceptable use of electronic communication 17

13 NHSmail 18

13.1 Users' musts "do" 18

13.2 Users must not "don'ts" 19

14 The Internet 19

14.1 Users' musts "do" 20

14.2 Users must not "don'ts" 20

15 Consultation 21

16 Dissemination and Implementation 21

17 Process for monitoring compliance and effectiveness 22

18 Standards/key performance indicators 22

19 References 22

1 Introduction

This policy outlines the obligations on the part of staff and other contractors regarding the acceptable use of the Trusts owned or contracted computer equipment and/or information asset (IAs)/systems.

Bridgewater Community Healthcare NHS Trust (hereafter the Trust) is committed to ensuring that information technology (IT) and communications facilities are used sensibly, professionally, lawfully, consistently with the duties of the role, with respect for colleagues and in accordance with this policy.

The Trust support its staff in meeting the Trusts and their legal requirements. Legal requirements directly related to this policy is the Computer Misuse Act 1990, Data Protection legislation (Data Protection Act 2018), Confidentiality: NHS Code of Practice (Department of Health and Social Care (2003), and the Caldicott Principles (National Data Guardian (2020).

Adherence to this policy will support staff in not only accessing secure IT and subsequent programs but will secure theirs and that of their clients information.

Under legislation the Trust has to have in in place processes to ensure it meets its legal obligations to secure information. Where there suspected fraudulent activities, the matter will be referred to the Trust's Anti-Fraud Specialist (AFS) and/or the police. Any evidence of system misuse may result in system or service access withdrawal and result in subsequent disciplinary action.

In exceptional circumstances The Regulation of Investigatory Powers (RIPA) Act 2000 permits monitoring and recording of employee's 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 legislation. In addition, communications may be monitored for the purpose of checking whether those communications are relevant to the purpose of the Trusts business, and the employee's position within the Trust. Any communication can be subject to a Freedom of information (FOI) or as subject access request (SAR).

1.1 Objective

The aim of the policy is to ensure that all staff are given the relevant support to ensure they are aware of what is acceptable use of any IT or computer equipment and/or information system owned or operated by the Trust and therefore can apply procedures accordingly.

1.2 Scope

This policy applies to all Trust staff, whether permanent, part-time, or temporary with responsibilities listed within section 5. It also applies to contractors granted access to Trust information and information systems. This includes staff from other organisations working on the Trust infrastructure are required to understand and abide by this policy.

2 Definitions

The definitions applicable to this policy are as follows:

Infrastructure	The system of hardware, software, facilities and service components that support the delivery of business systems and IT-enabled processes.
Computer equipment	This means electronic data processing hardware and related peripheral equipment. This includes, but is not limited to, laptops, monitors and display screens, "media," keyboards, printers, modems and permanently installed wiring associated with such equipment.
Information asset (IA)/system	An integrated set of components for collecting, storing, and processing data
Users	A users is a someone who uses a product, machine, information systems or application.
Multifactorial authentication (MFA)	An authentication method that requires the user to provide two or more verification factors to gain access to a resource or application.
Electronic communication	any information sent between particular parties over a phone line or internet connection.
Freedom of information (FOI)	The FOIA 2000 provides public access to information held by public authorities.
Subject access request (SAR)	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
Privalaged user	A user that is authorised (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Full details of privalaged user roles is set out in the Information Asset and System Audit Policy

Smartcard	A smartcard is a authentication token based on position. Acceptable use of smartcards and clinical systems links to a separate Smartcard terms and conditions (NHS Digital) which links to the NHS Confidentiality Code of Practice (Department of Health and Social Care, 2023)

3 Abbreviations

The abbreviations applicable to this policy are as follows:

AFS	Anti-Fraud Specialist
CABIT	Change Advisory Board and Information Technology Group
DSPT	Data Security and Protection Toolkit
FOI	Freedom of information
FOIA	Freedom of information Act
HSCN	Health and Social Care Network
IAO	Information asset owners
IT	Information Technology
IG	Information Goverannce
ID	Identification
IA	Information Asset
MFA	Multifactorial authentication
RA	Registration Authority
SIRO	Senior information risk owner
SAR	Subject Access Request

4 Other relevant procedural documents

This policy should be read in conjunction with the following documents:

Information Governance Framework Policy

Information Security Policy

Information Asset and System Audit Policy

Registration Authority (RA) Policy

Mandatory Training and Induction Policy

Home Based Working Policy & Procedures

Risk Management Framework

Incident Reporting Policy

Leavers Policy

Disciplinary Policy and Procedures

Dignity and Respect at Work Policy

Social Media Policy

Data Protection and Confidentiality Policy

Mandatory Training and Induction Policy

Anti-Fraud, Bribery & Corruption Policy

Access Control Policy

Freedom of Information and Environment Information Regulations Policy

Subject Access / Access to Health Records Policy

Video Consultation Procedure

PANDO Messaging Application for use in Trust Services Guideline

5 Roles and responsibilities

5.1 Senior information risk owner

The senior information risk owner (SIRO) is the Board member who has overall responsibility for information risk management in the Trust including health, staff, finance, and business critical information and computer assets. The responsibilities of the SIRO are to:

- ➢ Take overall ownership of the Trust's information risks including any risks associated with this policy

- ➢ Receive written assurance from information asset owners (IAOs) on the required standards within this policy

- ➢ Understand how the strategic business goals and how other NHS organisation's business goals may be impacted by information risks, and how those risks may be managed

- Sign off and take accountability for risk-based decisions and reviews in regard to the processing of personal data within the Trusts registered IAs

- Advise the Board on the effectiveness of information risk management across the Trust.

The SIRO will report to the Finance and Performance Committee on information risks and through the statement of internal controls following assurance from the IAOs.

The SIRO is the director of finance. The deputy SIRO is the assistant director for IT.

5.2 Assistant director of IT/deputy senior information risk owner

The asistant director of IT/SIRO supported by their teams, is overall responsible for developing, implementing, and enforcing suitable and relevant information security procedures and protocols on Trust systems and infrastructure.

They are responsible for ensuring all the Trusts IT and associated assets including third party systems, have adequate security measures to comply with data protection and data security legislation and regulations. This in turn will support the staff in meeting their obligations set out in this policy.

5.3 Head of information Technology

The head of IT supported by the Change Advisory Board and Information Technology Group (CABIT) is responsible for:

- Liaising with the appropriate person or team regarding a breach of this policy. This includes the Trust's AFS where there is a suspicion that Trust IT is being used for fraudulent purposes in accordance with the Computer Misuse Act 1990

- Ensuring users are suspended or remove where an investigation identifies that it is appropriate to do so

- Establishing secure systems, maintain the confidentiality, integrity and authenticity of information held within managed electronic systems

- Adhering to standards and establishing operational IT procedures to support this policy ensuring that all regulatory, contractual, and legal requirements are complied with

- Providing support, advice, and guidance to enable users to adequately protect devices and information

- Ensuring compliance with the core components of the standards in the data security and protection toolkit (DSPT) to protect IAs to deliver confidential, accurate and timely information to support patient care and associated support operations

- Ensuring all managed systems are controlled and protected against unauthorised access

- Ensuring IT assets purchased are identified, classified, and protected as required

- Establishing and maintaining business continuity planning processes to ensure that serviceability and the integrity of information are maintained

- Supporting the IAOs in fulfilling their responsibilities related to this policy.

5.4 Change Advisory Board and Information Technology group

The Change Advisory Board and Information Technology (CABIT) group will monitor the compliance of this policy on behalf of the Trust and will report and escalate any areas of concern to the Digital Information Governance and Information Technology (DIGIT) group.

5.5 Digital Information Governance and Information Technology Group

The DIGIT group will seek assurance on compliance with this policy on behalf of the Trust and will report on the management and accountability arrangement and provide assurance to the Board through the Trusts sub committees.

5.6 All managers/information asset owners and administrators

This policy applies to all staff those who manage staff or have been given the responsibilities of owning or managing and information systems have additional responsibilities for the following relating to this policy:

- Producing any supporting documentation to support this policy to help their staff

- Ensuring their staff are appropriately trained to use the IT computer equipment and IAs/systems used

- Understanding and addressing risks associated with this policy

- Undertaking and/or supporting any investigations or audit related to this policy

- Ensuring any learning outcomes related to an incident is shared with staff for which they are responsible

- Ensuring appropriate access to systems is followed, by notifying IT services of any staff leavers or changes in access.

5.7 Data protection officer

The data protection officer (DPO) for the Trust is held by the Trust secretary.

The DPO reports directly to the Board about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

With the support of the Information Governance Team, they will:

- Provide advice to the Trust and its employees on compliance obligations with data protection law (DPA, 2018)

- Advise on when data protection impact assessments are required

- Monitor compliance with data protection law and organisational policies in relation to data protection law (DPA, 2018)

- Co-operate with, and be the first point of contact for the Information Commissioner

- Be the first point of contact within the Trust for all data protection matters

- Be available to be contacted directly by data subjects

- Take into account information risk when performing the above.

5.8 All staff

All staff that use any Trust IT and communications facilities must:

- Use them sensibly, professionally, lawfully, consistently with the duties of the role, with respect for colleagues and in accordance with this policy

- Undertake education and awareness on security and using information and technology, including the mandatory annual security e-learning, in order to support the understanding of recognising and reporting threats, risks, vulnerabilities and incidents

- Follow and understand the specific dos and don'ts are outlined in this policy

- Be aware that any IT computer and IAs and systems have automatic logs of activity including user's interactions. This allows the Trust to undertake audits and investigations.

- Be aware that electronic and manual audits will be undertaken to ensure this policy is followed. This will ensure that both patients, staff and the Trust are always protected

- Immediately report any breach of this policy to their manager and to the relevant team and comply with official procedures when a breach of the policy is suspected or reported

- Complete an online inicident form using the risk management reporting system (Ulysses).

6 Equipment

All IT computer equipment, IAs and systems accessed or used by users.

7 Acceptable use

IT access is provided on the basis of business need. Use of any equipment provided for business purposes is acceptable only where such use falls within the normal day to day remit of the individual.

Staff are the users of the Trust IT equipment and systems which allows them to them to work efficiently and effectively within their role.

Equipment and systems access are provided for users' business purposes. Personal use should be kept to a minimal as it increases the Trust's information security risk exposure. Usage should at all times be within the constraints of Trust policies and procedures.

Users who use the Trust IT equipment for personal use, need to be aware that their personal information like banking details can be captured by the security software used by the Trust.

It is unacceptable to view, process or store illicit, pornographic, or racist material. This includes using Trust equipment to duplicate copyrighted materials such as software or music.

The appropriate use of Trust IT equipment and systems supports staff ie the users with their legal responsibilities to protect personal and sensitive information.

The policy is sectioned to ease of reading each section has a "must or must not" or "dos and don'ts" for users. The sections are:

- Managing and protecting information
- User identification (ID) and passwords
- IT equipment including telephones.
- Software/applications (apps)
- Electronic communications including emails
- Internet/Intranet
- Remote access.

8 Managing and protecting information

To ensure that patient, staff and corporate information is processed appropriately the following apply to all staff and users.

8.1 Users' musts "do"

- Ensure that all information is created, used, shared, and disposed of in line with business need and in compliance with Information Governance and Records Management policies.

- Apply the security classification appropriately to documents to ensure information is stored and process appropriately.

- Always protect and secure patient and staff information.

- Limit using Trust equipment for personal use, as their details and information can be retained.

8.2 Users must not "don'ts"

- Misuse their official position to further private interests or those of others.

- Attempt to access anyone's personal data unless there is a legitimate business need that is appropriate to their job role.

- Under any circumstances, knowingly access, or attempt to access, their own records or the records of friends, family members, ex-partners, relatives, or anyone else they know.

- Attempt to access, amend, damage, delete or disseminate another person's files, emails, communications, or data without the appropriate authority.

- Attempt to compromise or gain unauthorised access to IT, telephony or content, or prevent legitimate access to it.

9 User identification (ID) and passwords

Everyone has a unique ID with additional measures for Information Assets/systems to safe guard the information. Those with access to NHS Spine compliant clinical systems (except for Mobile Working Applications including SystmOne Brigid) are to be accessed via a smartcard.

9.1 Users' musts "do"

- Protect usernames, staff numbers, smart cards, dongles, and passwords appropriately.

- Create secure passwords following the standard domain user passphrase security document (if not automatically applied).

- When using a password manager, ensure that their master password is stored securely within the Trust domain.

- Remove their network access smart card or dongle and/or lock the screen when temporarily leaving devices that are in use.

- Log out of all computer devices connected to Trusts internal network during nonworking hours, i.e., at the end of the working day.

- Where temporary passwords are issued to any individual, for any reason, then they should be changed at first logon to a permanent password.

- Adopt multifactorial authentication (MFA) where possible.

- Use your assigned smart card on NHS Spine compliant Clinical Systems (except for Mobile Working Applications including SystmOne Brigid)

9.2 Users must not “don’ts”:

- Share or store passwords in shared folders (including paper folders/documents).
- log on to any Trust system using another user’s credentials.
- Share smart card log in details.
- Share passwords or log in details with anyone.

10 IT equipment including mobile phones/telephones

To ensure that personal and sensitive information is always secure it is unacceptable, regardless of the purpose for family or friends, to use or access Trust computers or IAs/systems.

On termination of employment, resignation or transfer, staff must return all equipment to their manager. Staff must also provide details of all of their system logons so that they can be disabled.

10.1 Users’ musts “do”

- When travelling by car, if staff have to leave the car unattended, equipment should be kept locked in the boot and out of sight when it is not possible to take the equipment with them.
- Adhere to the terms and conditions of all license agreements relating to IT systems which they use. This includes software, equipment.
- Ensure they start and terminate each session of use of IT systems in accordance with published instructions.
- Take every precaution to avoid damage to equipment caused by smoking, eating, or drinking in its vicinity. In particular, eating or drinking in IT system rooms is forbidden
- Respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT systems.
- Ensure their workstation is locked whenever it is not in use.
- Reboot their computer or laptop on a minimum weekly basis to allow for security updates.
- Only store Trust information including patient information on a trusted Trust IA/system or a secure server.
- Inform IT if an encrypted pen drives or CD/DVD are being used.
- Inform their manager and IT services if wishing to take Trust devices outside the country for official business.

- Ensure screen displays are not in direct view of the general public.

- Ensure screens are locked before moving away from the computer, at any time.

10.2 Users must not “don’ts”

- In any way, cause damage to the Trust’s IT systems.

- Modify any Trust equipment or IT systems.

- Deliberately introduce any virus, for example worm, trojan horse or other harmful or nuisance program or file, onto any IT systems, nor take deliberate action to circumvent any precautions taken or prescribed by the Trust.

- Delete or amend the data or data structures of other users without their permission.

- Exceed the terms of their registration. In particular they must not connect to any other computing IT systems without the permission of the designated authority.

- Interfere with the use by others of the IT systems; they must not remove or interfere with output belonging to another user

- Create, display or circulation of offensive material in any form.

- Share login details and passwords with any other user or write them down where they could be viewed and by another person and used to gain system access.

- Trade or canvass support for any organisation on IT equipment, whether it is for personal gain from any type of transaction or on behalf of external bodies.

- Take equipment outside the United Kingdom unless approved and required for official business.

- Provide a Trust telephone number as a contact point in personal advertisements in the press, on the internet etc.

- Use/call premium rate phone numbers such as those associated with competition lines, racing lines, chat rooms etc.

- Transmit offensive material in either voice, text or image format from Trust supplied mobile phones.

- Use of Trust telephony for personal use outside of business hours.

- Use the service to impersonate someone else.

11 Software and applications (Apps)

Users must not install personal software on Trust equipment regardless of its nature. Only software, which supports Trust business, is to be installed and in all instances, this must be approved and undertaken by IT service.

The installed security software that is recommended by the Trust is to utilised and not turned off.

11.1 Users' musts "do"

- Log a call with IT services for installation of any software or application which is deemed business beneficial.
- Understand that where software or an application processes personal information the legally required Data Protection Impact Assessment needs to be completed.
- Adhere to the terms and conditions of all license agreements relating to IT systems.
- Allow the software to install the latest security updates.
- Understand that any software can be accessed or seen by privileged users when they are auditing or updating the systems.

11.2 Users must not "don'ts"

- Deliberately introduce any virus, for example worm, trojan horse or other harmful or nuisance program or file.
- Violate copyright or use in breach of a licence agreement.
- Use any type of applications and/or devices to circumvent management or security controls or damage, destroy, or deny availability of service.

12 Acceptable use of electronic communication

Pando is the Trust approved application for processing information relating to patient and staff and is supported by this guidance: PANDO Messaging Application for use in Trust Services Guideline. Applications like Whatsapp or Messenger must not be used for processing personal information.

Under no circumstances should patient identifiable information (PID) be transmitted by non-authorised or non-secure electronic communication or un-encrypted media/devices.

The content of all messages including emails are owned by the Trust, users should not have an expectation of privacy in anything they create, store, send or receive on their computer.

The Trust has the capability and right to monitor electronic communications including emails if there are suspicions of inappropriate or non-acceptable use in alignment to this or any other Trust policy. Misuse of email or any other Trust system may be dealt with by way of the Disciplinary Policy and Procedure.

As commercial internet mail accounts such as, Yahoo, Hotmail and Google are particularly insecure these have been blocked by IT. Staff must not access them from any Trust devices.

13 NHSmail

The Trust, like all other NHS organisations, has subscribed to the NHS directory service. As part of this, NHSMail accounts are established for all staff. NHSmail is a secure internet mail, calendar, and directory service within which every employee has an "address for life" which is always @nhs.net and does not change as they move NHS organisations.

It is also available directly from the internet allowing users to access their mail from any location. The NHSmail Acceptable Use Policy (AUP) (NHS Digital, 2021) needs to be accepted by all users, and staff need to be made aware of their responsibilities in this document. NHSmail accounts can access all of Office 365 products there is a **N365 Acceptable user policy** to support users regarding the wider Office 365 products.

13.1 Users' musts "do"

- Think carefully when composing emails, the nature of email is that it is often less formal than letters etc. This informality can cause differences in interpretation amongst recipients.
- Use distribution lists appropriately. Distribution lists need to reviewed and updated on a regular basis.
- Check that you have the right recipient ahead of pressing send.
- Manage their mailbox. Check emails regularly, and respond to requests promptly.
- Advise people when you are not available by setting 'out of office auto-reply' on the system.
- Be selective about who receives emails, especially when using 'Reply to All.'
- Remember that a message from a Trust email account reflects on the Trust. It is also admissible in a court of law and may require disclosure under the FOIA 2000.
- Keep passwords secure.
- Mark emails as private or confidential, where appropriate.

- Emails is a communication tool and should be used as a repository. Any information that needs to be retained should be filed in a different location.

13.2 Users must not "don'ts"

- Use their work email for non-Trust purposes.
- Send PID outside the Trust without encryption i.e., add [secure] in the subject line.
- Send offensive, pornographic, or illegal messages or material.
- Use the email accounts of others except where proxy rights have been granted.
- Send global messages, except for alerts.
- Send messages to those whom they are aware do not wish to receive the mail.
- Use the account of another individual without official access to that account.
- Use the email system for personal gain.
- Forward junk mail, spam, or chain mail.
- Send attachments in excess of 20Mb.
- Open mail where they do not recognise the sender, or the contents appears to be dubious – it may be a virus.
- Open attachments with exe, vbs, ps1, psm1 and psd1 extensions.
- Be caught out by the speed of email. Think carefully, is your first reaction really the one that you want the recipient to receive.

14 The Internet

The Internet is a valuable tool for research and distribution of information. However, the risk associated with connection to, and use of, the internet is extreme and requires significant management and control.

The Trust provides internet access to all staff via a managed Health and Social Care Network this is called the HSCN (N3) connection (NHS Digital), which is a secured service, which aims to protect the NHS from many of the risks associated with the Internet.

The Trust users' electronic protocols with block users from high risk sites, this is to protect the user and the Trust. A user must not install or configure any connections to commercial Internet service providers. Such connections are insecure and may, in certain circumstances, represent a breach that will be investigated.

Access to a blocked site can be granted upon request to the IT Service desk. If the request is deemed against policy, it must be supported by their manager who will outline the business justification along with any required risk assessment.

Staff who use streaming services that are not for work purposes or cause network disadvantages to other staff will be blocked from the network.

Users should also note that internet usage is tracked, and logs are retained that can be produced as evidence in the event of any accusations of misuse.

There is a Social Media Policy that covers the use of social media websites by staff in either a personal or professional capacity.

Users who access websites using the Trust IT equipment for personal use, need to be aware that their personal information like banking details can be captured by the security software used by the Trust.

14.1 Users' musts "do"

- ➢ Only use streaming services such as "YouTube" for work purposes, as streaming can cause high congestion on the network. I.e., makes the systems to run slow for everyone.
- ➢ Always be professional and courteous to other users.
- ➢ Only access approved websites.

14.2 Users must not "don'ts"

Staff must not:

- ➢ Use Trust equipment for non-Trust related ventures like that of a private business.
- ➢ Access, download, or transmit any obscene, indecent, or pornographic images, data, or other materia
- ➢ Access, download, or transmit any defamatory, sexist, racist or otherwise offensive images, data, or other material
- ➢ Access, download, or transmit any copyrighted material in a manner that violates that copyright
- ➢ Access, download, or transmit any material that is designed or likely to annoy, harass, bully or inconvenience other people
- ➢ Access, download, or transmit material created for the purpose of corrupting or destroying the data of other users
- ➢ Allow non-Trust persons access to systems

- Enter their Trust email or ID into any non-work related internet site.

15 Consultation

Key individuals/groups involved in the development of the policy to ensure it is fit for purpose once approved.

Name	Designation
Lucy Brierley	Information Governance Officer.
Sandra Alderson	Programme Manager Digital and Clinical Systems Team
Paul Dwerryhouse	Service Delivery Manager IT Services
Mary Corkery	Policy Officer
Caroline Rigby	RA and Training Manager
DIGIT	Digital Information governance and IT group

16 Dissemination and implementation

16.1 Dissemination

The IG manager will disseminate this policy to all staff via the team brief. The policy will be made available on the Trust intranet and published in the bulletin. This will enable those listed in the roles and responsibilities to fulfil their obligations regarding dissemination.

16.2 Implementation

Managers are responsible for implementing this policy and ensuring all staff adhere to it.

The policy will be implemented via the mandatory data security awareness level one is for all staff and Trust Induction.

Training will be be periodically updated via mandatory IG training, staff bulletins, desktop messages and global messages.

17 Process for monitoring compliance and effectiveness

Process for reviewing compliance and effectiveness i.e., audit, review, survey, incident reporting	Responsible	Frequency of monitoring	Assurance group
Corporate Incidents relating to aspects of this policy	IG team	Quarterly reports	DIGIT

18 Standards/key performance indicators

Standards set in the DSPT which are reviewed yearly and reported to DIGIT then published.

19 References

Computer Misuse Act 1990, c.18 [online]. Available at: http://www.legislation.gov.uk/ukpga/1990/18/contents

Data Protection Act 2018, c.12 [online]. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents

Department of Health and Social Care (2023) Confidentiality: NHS Code of Practice Guidance [online]. Available at: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Equality Act 2010, c. 15 [online]. Available at: http://www.legislation.gov.uk/ukpga/2010/15/contents

Freedom of Information Act 2000, c.36 [online]. Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents

Human Rights Act 1998, c. 42 [online]. Available at: http://www.legislation.gov.uk/ukpga/1998/42/contents

International Organization for Standardization (2022) ISO/IEC 27001, Code of Practice for Information Security Management [online]. Available at: https://www.iso.org/isoiec-27001-information-security.html

NHS Digital [webpage] Health and Social Care Network (HSCN) Available at: https://digital.nhs.uk/services/health-and-social-care-network

Regulation of Investigatory Powers Act 2000, c.23 [online]. Available at: http://www.legislation.gov.uk/ukpga/2000/23