Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

EMAIL AND INTERNET ACCEPTABLE USE POLICY

POLICY

Reference	ISP-02		
Approving Body	Information Governance Committee		
Date Approved	19th March 2024		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	X		
Issue Date	Enter the date the document is effective from		
Version	4		
Summary of Changes from Previous Version	Legislation changes following the UKs exit from the EU and the Trust moving from local emails to the national NHSmail platform provided by NHS England		
Supersedes	3		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group Information Governance Committee		
Date of Completion of Equality Impact Assessment	28th January 2024		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	UK General Data Protection Regulation Computer Misuse Act 1990		
Target Audience	All staff		
Review Date	2 years		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Head of Data Security & Protection		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Head of Data Security & Protection, Information Governance Team		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Accessing Encrypted emails Guide for non-NHSmail users Encryption Guide for NHSmail	May 2020 July 2022
Template control	June 2020

CONTENTS

APPENDICIES

Appendix 1	EQUALITY IMPACT ASSESSMENT FORM	
Appendix 2	APPROVAL FOR STAFF MONITORING – AUDIT DATA	
Appendix 3	APPROVAL FOR ACCESS TO BLOCKED INTERNET SITES	
Appendix 4	PROCEDURE FOR INVESTIGATION OF SUSPECTED MISUSE OF THE INTERNET OR EMAIL	

1.0 INTRODUCTION

It is your responsibility to ensure you understand and comply with this policy.

It ensures that:

- You understand your responsibilities and what constitutes abuse of the service.
- Computers and personal data are not put at risk.
- You understand how NHSmail and the use of the internet complies with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 by reading the Transparency Information.

As an NHSmail account holder, you should expect to receive ad-hoc communications about NHSmail from NHS England informing you of changes or important updates to the service that may impact your use.

As many NHS information systems are now electronic, the internet and electronic mail (email) are essential business tools.

All staff are required to use them in a competent, responsible, effective, and lawful manner.

NHSmail accounts are owned by NHS England on behalf of the Secretary of State for Health in England. The Trust (via Nottinghamshire Health Informatics Service) maintains day to day administration responsibility for your NHSmail account. If your use breaches this policy, the Trust has the right to undertake disciplinary procedures in accordance with our HR policy.

Information created or stored within the Trust's NHSmail system constitutes an organisational record; no messages contained within it are considered personal. Emails have the same status as any other form of the Trust's business correspondence or written communication and may be subject to disclosure under UK General Data Protection Regulation and/ or Freedom of Information Act (2000).

Nottinghamshire Health Informatics Service (NHIS) provides and manages the Trust's information technology network services and controls all staff access to the internet and NHSmail under instruction from the Trust.

Staff are granted access to NHSmail and the internet for the Trust's business use and for work-related educational, research purposes and work benefits.

The purpose of this policy is to ensure that all staff understand their personal responsibilities for correctly accessing the internet/NHSmail and understand what the Trust deems to be acceptable use of the internet/NHSmail via the Trust's information technology systems, while on Trust premises, working remotely and when acting in representation of the Trust.

Failure by staff to adhere to this policy and all supporting guidance will be considered gross misconduct and **may result in disciplinary action**.

NHSmail contents are owned by the Trust; however individual users are accountable for the contents of emails sent from Trust accounts.

Do…

✓ Be aware of what information you are sharing, who the information is shared with and how it is shared, as additional controls may need to be applied to make your email secure.

✓ Convey a professional image of the Trust that is consistent with the Trust's Values and Behaviours in email communications.

✓ Bear in mind that the content of emails may be disclosed under UK General Data Protection Regulation and/or Freedom of Information Act.

✓ Report any phishing emails to NHSmail IT Help Desk via spamreports@nhs.net. Further guidance is provided in section 3 under Phishing.

Do not…

X Send confidential information unless you know it is secure (encrypted)[1].

X You must not use NHSmail to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is grounds for immediate dismissal and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending, or receiving material related to paedophilia, pornography, terrorism, incitement to racial harassment, stalking, sexual harassment, and treason. Use of the service for illegal activity will result in the immediate disablement of your NHSmail account and in certain circumstances reporting to the Police, refer to section 9.

X You must not use any of the NHSmail services for commercial gain. This includes, but is not limited to unsolicited marketing, advertising, and selling of goods or services.

X You must not attempt to interfere with the technical components, both hardware and software, of the NHSmail system in any way

1

2.0 POLICY STATEMENT

The Trust will take all reasonable steps to ensure that users of the NHSmail system are aware of policies, protocols, procedures, and legal obligations relating to the use of NHSmail by:

- providing guidance on the categories of emails that should be retained as records (see the Corporate Records Policy[2])
- ensuring its monitoring and auditing procedures comply with legal requirements
- ensuring that the NHSmail system allows for the secure communication of information for the dissemination of confidential information
- providing a system in which saved NHSmail records can be located and retrieved from an electronic folder and reconstructed into their original form with all transactions recorded.

In doing so the Trust aims to reduce the risk of:

- loss of reputation
- unauthorised or inadvertent disclosure of medical, personal, or confidential records and legal liabilities.

3.0 DEFINITIONS/ ABBREVIATIONS

Attachment: a file attached to an NHSmail message, which could contain malicious software and should be opened with care.

Bandwidth: the overall capacity of a network connection/the amount of data that passes through a network connection over time. The greater the capacity, the more likely that better performance will result.

Browser: the Trust uses Microsoft Edge as its standard browser. Nottinghamshire Health Informatics Service will ensure that the recommended version is available on all devices owned by the Trust.

Confidential information can be anything that relates to patients, staff or any other information (such as medical and staff records, contracts, tenders, etc.) held either in paper, disc, computer file or printout, video, photograph or even heard word of mouth. It includes deceased as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' 'special categories' as defined in the UK General Data Protection Regulation. It includes information stored on portable devices such as laptops, mobile telephones and external hard drives/memory sticks).

It can take many forms including patient level health information, employee records, occupational health records etc.

[2] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8635

Health and Social Care Network (HSCN): is a data network for health and care organisations, which replaced N3. It provides the underlying network arrangements to help integrate and transform health and social care services by enabling them to access and share information more reliably, flexibly, and efficiently. Health and care providers will be able to obtain network connectivity from multiple suppliers in a competitive marketplace and in collaboration with other health and social care organisations.

Information asset: broadly, any data, information system, computer, or programme.

Information sharing protocols: written agreements made within the existing legislative framework between the Trust and named organisations to allow sharing of confidential information for health and social care purposes.

Internet (World Wide Web): a global system connecting computers and computer networks. For the purposes of this document, the term internet will also encompass the Trust's intranet.

Intranet: a private network for communicating and sharing information accessible only to authorised staff within an organisation e.g. the Trust's own intranet site or the NHS.net.

Junk mail: unsolicited email messages usually of a commercial nature, chain letters or other unsolicited mass-mailings (see also **spam**).

Local Area Network (LAN) -. The Trust's computer network.

Malicious software/malware: *s*oftware designed to harm a computer or network. Includes but is not limited to:

- **Macros** - Macros are a series of actions that a program such as Microsoft Excel may perform to work out some formulas. Your computer will disable macros by default because they can be programmed to install malware. Always be vigilant; especially when clicking 'enable macros' or 'edit document'. Do you trust the source of the document?

- **Ransomware** - a growing threat in the cyber threat landscape. Usually delivered via phishing email, which use social engineering techniques (i.e. an email made to look like its sent from a person/name known to the victim or disguised to look like it is from your bank, post office, police etc.) to convince a victim to click a link, download or open an attachment. Once the victims computer is infected with ransomware, the malicious code will begin to encrypt files on the device (and network), rendering them inaccessible before demanding payment, often in the form of crypto currency such as bitcoin, in return for the ability to unlock that data with an encryption key. Effectively this tactic denies the victim access to their data unless they pay the ransom or have the ability to restore data from unaffected back-ups.

- **Phishing**: sending an email to staff falsely claiming to be an established legitimate enterprise in an attempt to defraud staff into surrendering confidential information that will be used for identity theft. The email directs staff to visit a website where they are asked to update personal information, such as passwords, credit/debit card numbers and bank account numbers that the legitimate organisation already has. The website, however, is bogus and set up only to steal staff's information (see also **spoofing**).

If you receive a request from a supposed colleague asking for login details, or sensitive, financial, or patient/service user information, you should always double check the request with that colleague over the phone. Equally if you receive an unsolicited email that contains attachments or links you have not asked for, do not open them. Remain vigilant and report the suspicious email to the NHSmail IT Service Desk via spamreports@nhs.net.

Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus and anti-spam software although occasionally, as with any email service, a new virus or spam message may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and inform NHIS. If you receive spam messages you should forward them to spamreports@nhs.net using the process detailed in the Cyber Security Guide. You must not introduce or forward any virus or any other computer programme that may cause damage to NHS or social care computers or systems.

- **Vishing** – phone calls to trick their victims

- **Trojan horses -** malicious, security-breaking programs disguised as something benign such as a screen saver or game.

- **Viruses** - unauthorised computer code attached to a computer programme which secretly copies itself using shared discs or network connections - can destroy information or make a computer inoperable.

- **Worms** - which launch an application that destroys information on a computer and sends a copy of the virus to everyone in the computer's NHSmail Directory.

- **Monitoring** - For the purposes of this document the term includes interception of communications, monitoring of systems, logging, and recording, inspecting, and auditing for the purposes of investigation or further action.

- **NHSmail system** - any computer software application that allows NHSmail - message, image, form, attachment, and data - to be communicated from one computing system to another.

- **Proxy website** - a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.

- **Records** - information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.[3]

- **Social media** - for the purpose of this and other relevant information governance policies the term social media includes, but is not limited to, websites and applications that enable staff to create and share content or to participate in social networking, blogging, tweeting or social engineering.

- **Spam** - unsolicited NHSmail messages, usually of a commercial nature sent to a large number of recipients. Refers also to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

- **Spoofing** - forgery of an NHSmail so that it appears to have been sent by someone other than the sender.

- **UK General Data Protection Regulation -** supersedes the Data Protection Act 1998 and EU General Data Protection Regulation.

- **User** - an individual given access to the Trust's network to access the internet and NHSmail.

- **Wi-Fi** - a mechanism for wirelessly connecting electronic devices through a network access point.

4.0 ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee..

Senior Information Risk Owner (SIRO)

The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated SIRO, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The SIRO also reports annually to the Trust Board on Information Governance performance..

[3] ISO 15489-1:2016 Information and documentation -- Records management -- Part 1: Concepts and principles https://www.iso.org/standard/62542.html

Caldicott Guardian

The Medical Director is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Head of Data Security & Privacy and Data Protection Officer

SFHFT are a public authority and have appointed a Data Protection Officer. The Data Protection Officer reports to the Senior Information Risk Owner and works with the Caldicott Guardian. The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, SFHFT data protection policies, awareness-raising, training, and audits. The SFHFT Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, the Data Protection Officer has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Head of Data Security & Privacy is responsible for periodically monitoring NHSmail use to ensure compliance with this policy and to assist HR in any disciplinary investigations regarding NHSmail use as well as ensuring that risks to secure NHSmail communication are identified with adequate controls applied to ensure the security of Trust data.

Information Asset Owners (IAOs)

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, the advice of the Data Protection Officer is sought, the DPO also monitors the process.

Information Asset Administrators (IAAs)

Information Asset Administrators ensure that IG policies and procedures are followed, recognise actual or potential IG security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

All Managers

All managers are responsible for ensuring that their staff receive relevant training, guidance, and support to understand and adhere to this policy and all supporting guidance.

Staff

All staff (including Medirest, Skanska, agency and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality. You must not attempt to disguise your identity, your sending address or send email from other systems pretending to originate from the NHSmail service. Where there is a need to provide someone else with the ability to send email on your behalf, this should be done via the delegation controls within the service. Where an organisation wishes to send email on behalf of its staff the organisation may request the ability to do this via Impersonation accounts. Individuals being impersonated must always be informed prior to emails being sent.

You must not send any material by email 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 Information Governance.

You must not use the NHSmail service to harass other users or groups by sending persistent emails or instant messages to individuals or distribution lists.

You must not forward chain emails or other frivolous material to individuals or distribution lists.

It is your responsibility to check that you are sending email to the correct recipient, as there may be more than one person with the same name using the service. Please note: if you hover over the individuals names you will see by which organisation they are employed. Always check that you have the correct email address for the person you wish to send to - this can be done by checking their entry in the NHS Directory.

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

You must ensure any application integrating with NHSmail has an in-built error messaging capability to highlight any messages that are not delivered. This is to protect your business process and to ensure any errors are highlighted to the sender in order for the error to be fixed as soon as possible.

All staff must be aware or their individual responsibilities for competent and appropriate use of the Trust's internet and NHSmail systems, in accordance with this policy.

All staff with access to the Trust's NHSmail email service are responsible for:

- Identifying and retaining emails and attachments appropriate for retention as electronic records, because of their business function or content.
- Accurately indexing and electronically filing appropriate emails.
- Managing their email records in a manner that ensures their integrity, availability and safeguards against their inappropriate loss, destruction, or unauthorised disclosure.
- Conveying a professional image of the Trust that is consistent with the Trust's Values and Behaviours.
- Promptly disposing of emails of short-lived value, so that you can manage the size of your mailbox within appropriate limits. Online Archiving is a solution that enables you to store and manage older or legacy emails outside of your primary mailbox – freeing up quota space and improving Outlook performance.

You must ensure your password and answers to your security questions for the NHSmail services are kept confidential and secure at all times. You should notify NHIS if you become aware of any unauthorised access to your NHSmail account. You must **never** input your NHSmail password into any other website other than nhs.net sites. You will never be asked for your NHSmail password. Do not divulge this information to anyone, even if asked.

If you are found to be deliberately responsible for introducing or forwarding a programme that causes any loss of service, NHS England may seek financial reparation from the Trust.

Local Counter Fraud Specialist (LCFS)
The Local Counter Fraud Specialist works with the Trust to investigate any occurrence or allegation of fraud within the Trust and promote awareness of the NHS Counter Fraud Authority amongst staff and patients.

Information Governance Committee
The Committee is responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support its implementation.

The Committee will ensure that the management of NHSmail security and risks associated with the use of Trust systems is part of its assurance process.

5.0 APPROVAL

Policy approval is by the Information Governance Committee.

6.0 USE OF INFORMATION SYSTEMS

6.1 All staff requiring computer access will be allocated a Windows account, NHSmail email address and access to the internet, following authorisation by an appropriate senior manager/line manager.

Having a Windows account allows staff to log onto a Trust device, to access their NHSmail account and access the internet via a web browser. These services are not available without a Windows username and password.

Further information on Trust device access controls are available in the Trust's Information Security Policy.

6.2 Access to the internet through proxy websites or other methods of bypassing security controls or circumventing internet filtering to access content otherwise blocked is **not** permitted. Google, Yahoo, Firefox, and other Search Engines are not a type of proxy website. Staff shall not use external, web-based email services (e.g. hotmail.com) for Trust communications and purposes.

6.3 Any user who requires temporary exemption from any part of this policy to access specific information for legitimate work or research purposes is required to obtain written authorisation from their Line Manager and the Information Governance department.

6.4 All staff shall only be authorised access to information relevant to their work.

6.5 Accessing or attempting to gain access to unauthorised information shall be deemed a disciplinary offence.

6.6 When access to information is authorised, the individual user shall ensure the confidentiality and integrity of the information is upheld, and to observe adequate protection of the information according to NHS policies as well as legal and statutory requirements. This includes the protection of information against access by unauthorised persons.

6.7 All staff should be aware that they have a duty of care to prevent and report any unauthorised access to systems, information, and data. Further information can be found in the Incident Reporting Policy.

6.8 Staff suspected of breaching this policy may have their access rights suspended until an investigation and any disciplinary procedures have been completed.

6.9 Use of NHS information systems for malicious purposes shall be deemed a disciplinary offence. This includes but is not limited to:

- Penetration attempts ("hacking" or "cracking") of external or internal systems.
- Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic.
- Discriminatory (on the grounds of sex, political, religious, or sexual preferences or orientation), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in NHSmail or other electronic communication systems.

- Acquisition or proliferation of pornographic or material identified as offensive or criminal.
- Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software.
- Storage or transmission of large data volumes for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads.

6.12 If identified misuse is considered a criminal offence, criminal charges shall be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.

6.13 All staff should be aware of what constitutes misuse and the potential consequences of any misuse of systems, information, and data.

7.0 PERSONAL USE

7.1 Access to NHSmail and the internet is provided to staff for Trust business purposes and staff work related benefits eg health service discounts and health and wellbeing support..

7.2 Internet access is mainly provided for business purposes. For the purpose of simplifying everyday tasks, limited private use may be accepted. Such use includes access to online banking, public web services and phone web directories. The internet should not be used for personal use during working hours and may lead to disciplinary action. All communication you send through the NHSmail services is assumed to be official correspondence from you acting in your official capacity on behalf of the Trust.

7.3 Staff shall not use internet-based file sharing applications, unless explicitly approved and provided as a service.

7.4 Staff must not upload and download their personal data (e.g. private pictures) to and from the internet.

7.5 Staff must not download copyrighted material such as software, text, images, music, and video from the internet.

7.6 Staff must not use NHS systems or internet access for personal advantages such as business financial transactions or personal business activities.

7.7 Staff must not use their NHSmail account for private purposes such as on social media and discussion forums.

7.8 There is no absolute right for staff to use NHSmail or the internet for personal use.

7.9 The Trust will not be liable for any financial or material loss to an individual user when using NHSmail for personal use.

7.10 The Trust will not be liable for any pecuniary loss to any external supplier of goods and/or services in the event of an individual user failing to honour any financial obligations contracted to that supplier whilst using the Trust NHSmail system for personal use.

8. LARGE FILE TRANSFERS

NHSmail users can securely send large file transfers via the Egress large file transfer web form up to a maximum combined file size of 5GB. This can be used to send to external recipients or other NHSmail users.

It is not possible to send a large file transfer from or to a shared mailbox as shared mailboxes do not have passwords and are not able to login to the web form to send an email or the Egress NHSmail portal to view the sent item. Further guidance is available here[4].

9. MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is an additional way of checking that it is really you when you log in to your account.

Multi-factor authentication will be mandated for all new starters in the Trust from 30th June 2023 and rolled out to all current staff over the next 12 months.

10. MISUES OF THE INTERNET AND EMAIL SYSTEMS

10.1 Misuse of the internet or NHSmail system may make both staff and the Trust liable under law and may impede the function of the Trust's network systems and the efficient functioning of NHSmail.

10.2 Staff must not use the Trust's NHSmail and internet system for:

a) Accessing, composing, or transmitting any material considered to be illegal, racist, homophobic, immoral, offensive, obscene, libellous, defamatory, harassing, or pornographic

Internet – Web Control and Web Protection
Web Control

Web filtering policy decisions are taken on a per category basis. Each individual website is classified by web filtering providers into a category and an action is applied to that category.

[4] https://support.nhs.net/knowledge-base/egress-large-file-transfer-web-form/

As there are millions of websites; and countless websites added to these categories every day, there is not a definitive individual website list, instead the action is applied on the identified category basis – i.e., a sexually explicit website would fall under the category 'Adult or Sexually Explicit'.

All web content falls into one of 56 web categories, the following 20 web categories are **blocked** in our base web filtering policy – based on the following category groups:

Adult/Inappropriate – Blocked by Default

- Adult/Sexually Explicit
- Criminal Activity
- Illegal Drugs
- Intolerance & Hate

Additional Block Content – Inappropriate Business Use

Approved by the Cyber Programme Board, the following categories are blocked based on inappropriate for business use.

- Chat
- Intimate Apparel & Swimwear
- Personals and Dating
- Tasteless & Offensive
- Violence
- Weapons

Additional Block Content – Cyber Threat Protection

Approved by the Cyber Programme Board, the following categories are blocked based on heightened risk and to Cyber Threat protection.

- Downloads
- Games
- Hacking
- Hosting Sites
- Peer-to-Peer
- Phishing & Fraud
- Proxies & Translators
- Ringtones/Mobile Phone Downloads
- Spam URLs
- Spyware

The remaining categories fall into either a 'Warn', where the user must accept a warning to proceed to the web site, or 'Allow' which are allowed by default.

Sophos Web Control: Content type categories

Web Protection

Over and above the Web Control categorisation, web protection is provided as part of the Anti-Virus product and is designed to prevent any threats from reaching the web browser. E.g., web sites detected with virus or malware embedded.

E-Mail

SFH Email is provided from the National NHSMail E-Mail tenant and as such the terms and conditions of its use are detailed in the NHSmail 2 Portal - Acceptable Use Policy. The following are not acceptable for all users.

a) Transmitting material that incites others to criminal, racist, homophobic, or terrorist acts or incites them to contemplate such acts.

b) Creating or transmitting defamatory material (note that common law and statutes pertaining to libel apply to the use of the internet) regarding the Trust, Trust business, service-staff, or staff.

c) Creating or transmitting material designed to or likely to cause annoyance, inconvenience or needless anxiety to service staff, other Trust staff or the general public.

f) Sharing any confidential information or corporate confidential information in contravention of the UK General Data Protection Regulation, Confidentiality: NHS Code of Practice or Caldicott Principles, in any unauthorised way, including social media.

g) Downloading or distributing 'pirated' software, music, or films. Such action is an infringement of the copyright of another person or Trust. The use of proprietary images, home page designs, hypertext links or other such electronic representations may constitute a violation of intellectual property rights of another business or individual. Any copying, modification or misrepresentation of such information is not only unethical but almost certainly illegal.

h) Forwarding chain letters, spam, virus warnings, and junk mail, mass-mailing and unlicensed programmes.

i) Sending unsolicited messages.

j) Transmitting unsolicited commercial or advertising material to other staff, Trusts connected to Health and Social Care Network or Trusts connected to other networks.

k) Deliberate corruption or destruction of other staff' data or work.

l) Accessing and using another user's NHSmail account

m) Sharing of passwords

n) Undertaking activities that deny service to other staff (e.g. overloading of web links with videos or sites using high bandwidth) or switching equipment.

o) Deliberate misuse, including that of other networked resources, such as the introduction of viruses, loading unlicensed software or upgrades.

p) Deliberate wasting of the Trust's time or network resources, including time linked to systems accessible via the internet, and the effort of the Trust or Nottinghamshire Health Informatics Service in support of those systems.

q) Unwarranted sending of large messages or attachments.

r) Downloading entertainment or games and playing games on the internet.

s Downloading any shareware or freeware without authorisation via the NHIS Customer Portal Service.

t) Undertaking activities for personal or commercial financial gain (e.g. sales of personal property, gambling or share dealing) or for political lobbying.

u) Actions that may lead the Trust open to action in breach of copyright or licensing laws when composing or forwarding email and attachments.

v) Forging or attempting to forge NHSmail messages (e.g. spoofing).

w) Streaming of video or audio for personal use.

This list is not exhaustive. The Trust is the final arbiter of what is or is not considered to be misuse of the Trust's internet and NHSmail system.

10.3 If any member of staff has concerns about misuse of the internet or NHSmail by a colleague, they should inform their Line Manager and the Information Governance department immediately.

11. INVESTIGATIONS OF SUSPECTED MISUSE

11.1 Any suspected misuse of the internet or NHSmail system identified through routine monitoring procedures (outlined in section 13 below) will initially be attributed to, and be the responsibility of, the associated logged-in user. Nottinghamshire Health Informatics Service regularly monitor individual activity using web filtering.

11.2 Where inappropriate use is suspected from the results of routine monitoring, the Information Governance department will inform the relevant user's Line Manager and initiate an investigation, in accordance with the procedure set out at Appendix B.

11.3 Where the Information Governance department has concerns about possible fraud and/or corruption in relation to suspected internet or NHSmail misuse, or is in any doubt whether the misuse constitutes fraud or corruption, both the Trust's Senior Information Risk Owner and the Local Counter Fraud Specialist will be informed. Fraud and/or corruption, if proven, may result in criminal action.

11.4 Other inappropriate use of the internet or NHSmail that is in breach of this policy may be referred to the police for investigation.

11.5 The Trust will not support staff to defend any legal action brought about because of internet or NHSmail misuse or other non-compliance with this policy.

11.6 Where any breach of this policy has been established, appropriate action will be taken in accordance with the Trust's disciplinary procedures.

12. TRANSFER OF CONFIDENTIAL INFORMATION

12.1 Consideration must be given to the nature of any information before it is transferred and whether the means of transfer is sufficiently secure. All transfers must comply with the Safe Haven Procedure.

12.2 Confidential information includes data that on its own, or in combination with another piece of data, can identify an individual. This may be factual, such as name[5], address, date of birth, NHS number, but also includes information offered as an opinion, such as a manager's opinion of an employee as the result of a performance appraisal.

12.3 All transfers of confidential information must comply with Data Protection Act and Caldicott Principles. In particular, they should:

- Be an approved lawful data flow agreed by the Information Governance department and/or the Trust's Caldicott Guardian.
- Only be sent on a 'need to know' basis.
- Be supported by a justifiable reason to send the information.
- Be anonymised or pseudonymised, wherever possible.

Further guidance on confidentiality and data protection, including the list of Caldicott Principles, is available in the Trust's Data Protection, Confidentiality and Disclosure Policy.

[5] This excludes the names of staff, their job role and work location, but does apply to their personal data such as home address, date of birth, financial and HR information

12.4 Personal confidential data or Trust commercially sensitive data should only be exchanged electronically when encrypted. emails sent to secure domains is automatically encrypted and complies with the pan-government email standard.

12.5 Secure NHSmail transfers include:

- Sending of emails between email addresses both ending in nhs.net. NHSmail protects emails and their attachments through encryption, but the encryption is only secure if sent from and to NHSmail accounts and other NHSmail systems that are accredited to the ISB 1596 standard. All staff will only use NHSmail accounts and no other email address for work purposes. Please note whilst NHSmail provides a safe path for sending confidential information via email it remains your responsibility to ensure that the recipient is appropriate and able to handle the sensitive data in accordance with Trust Information Governance policies.

- Individual staff must NOT send or forward confidential information or Trust commercially sensitive data to personal email addresses. Examples include but are not limited to Gmail, Hotmail, Yahoo mail, AOL mail, internet or remote storage areas and email services provided by other Internet Service Providers.

- NHSmail also includes an encryption feature that allows users to exchange confidential information securely with users of non-accredited or non-secure email services, for example Gmail, Hotmail etc. Before using the encryption feature, please ensure you read and understand all guidance and instructions to ensure data remains secure. Once a message is sent from NHSmail using the encryption feature, it is encrypted and protected with a digital signature to assure the recipient that the message is authentic and has not been forged or tampered with. Formatting of the message is preserved, and attachments can be included.

- NHSmail users can exchange confidential information securely with other NHSmail users, without needing to use the encryption feature. For example, sending from @nhs.net to @nhs.net. If you are sending confidential information outside of NHSmail, then the encryption feature must be used. The only exception is when sending emails to an organisation that has accredited to the secure email standard, for example NHIS and Nottinghamshire Healthcare NHS Foundation Trust. A list of these accredited domains is available on NHS England's website. NHSmail will identify if a destination domain is secure or not, therefore if there is doubt or uncertainty you should use the NHSmail encryption feature which will encrypt the email if the destination domain is not secure. If sending an email to multiple organisations with some secure and some insecure domains, using the encryption feature means that automatically those that are secure will receive an unencrypted email and those that are not secure will receive an encrypted email.

- NHSmail staff may communicate securely and directly with NHSmail staff on other secure Government domains, including local authorities using the 'Government Connect' NHSmail domains. This is particularly useful for staff wishing to communicate with Social Services or Public Health staff in local authorities or the Home Office nationally. The other secure accredited domains that are secure to send to are:

  For police:
  @pnn.police.uk
  @pnn.gov.uk

  Local Government:
  @nottscc.gov.uk

  Other:
  notts-his.nhs.uk
  nottshc.nhs.uk

  A list of accredited domains which are secure to communicate with without the requirement to include [secure] are here: https://nhs-prod.global.ssl.fastly.net/binaries/content/assets/website-assets/services/nhs-mail/secure-email-standard/dcb1596-accredited-domain.csv.

  If in doubt as to whether the email is being sent by a secure domain use [SECURE] (this must be square brackets) in the NHSmail subject line when sending from NHSmail.

12.6 If there is a requirement to transfer confidential information to other public sector agencies via NHSmail, advice should be sought from the Information Governance department, to ensure that the NHSmail addresses are secure when used in conjunction with an NHSmail address. Alternatively a list of accredited domains which are secure to communicate with: https://nhs-prod.global.ssl.fastly.net/binaries/content/assets/website-assets/services/nhs-mail/secure-email-standard/dcb1596-accredited-domain.csv.

12.7 Password protection is not classed as encryption so if you send an email by a non-secure route (not nhs.net-to-nhs.net OR nhs.net to another secure government domain) password protecting confidential information is not considered secure transfer as password protected documents can easily be accessed. **Password protection of documents is not required.**

12.8 NHSmail is a communication tool to support the secure exchange of information and is not designed as a document management system. Documents, emails, or messages that are required for retention/compliance purposes should be stored within a document management system (ie shared drive) in accordance with the Corporate Records Policy.

It is the mailbox owner's responsibility to ensure the mailbox is kept within quota to avoid restrictions being imposed and impacting business processes. Local archive solutions must be in place to manage the retention of data. NHSmail accounts should not be used to store confidential information. Once the information has been sent or received, it should be deleted or saved in a secure folder on a network drive (not on the C: Drive (desktop). For further guidance see section 14 of this policy - 'NHSmail Retention and Deletion' below.

12.9 Agreed information sharing protocols must be used when sending or forwarding confidential information to individuals in other Trusts. Regular flows of confidential information will need recording on the Data Flow Mapping log. More information on Data flow mapping requirements and information sharing protocols is available from the Information Governance department.

12.10 The principles of confidentiality and data protection should also be applied to the NHSmail transfer of information associated with confidential corporate information.

12.11 While it is recognised that one of the key benefits of NHSmail is that it can be accessed anywhere on any device via the Web option, staff choosing to access their NHSmail Web account on unencrypted, personal, or non-work provided device must do so in line with the policy for Electronic Remote Working.

12.12 While using the NHSmail Outlook Web Access function staff must also abide by the following rules:

a) Ensuring that if NHSmail is being accessed via the Web, staff must not auto save the password on their device.

b) If accessing NHSmail Web on a personal device (such as an iPhone) staff must ensure that a screen saver prompting a mandatory password is kept on the device at all times.

c) Staff must be vigilant of the environment in which they access NHSmail and ensure confidentiality is maintained at all times (e.g. if accessing from a home computer ensure that no friends or family members are able to see emails).

d) Always check you have logged out of NHSmail after use.

e) As the personal device used to access NHSmail via the Web will likely not be encrypted staff must not save any emails outside the secure web portal.

12.13 It is vital that line managers ensure ALL NHSmail accounts areclosed when staff leave regardless of whether they are joining another NHS organisation

13. USE OF SOCIAL MEDIA

13.1 All Trust employees and appointees are reminded of the confidentiality statement included in their contract of employment and all staff are reminded of their duty to comply with all information security requirements in the Trust's information governance policies located on the intranet and internet.

13.2 Staff must not disclose any Trust information that is or may be confidential information, or that is subject to a non-disclosure contract or agreement. Please refer to the Trust's Social Media and Recordings for non-clinical Purposes Policy[6].

14. CYBER SECURITY

14.1 All computer equipment within the Trust is virus protected, and incoming messages are virus checked. However, staff should report any unusual occurrences relating to the performance of their computer to the NHIS Service Desk.

14.2 NHSmail is protected by anti-virus and anti-spam software although occasionally, as with any email service, a new virus or spam message may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and inform NHIS. Care should be taken, or NHIS advice should be sought before opening any suspicious or unexpected NHSmail attachments or links.

If you receive spam messages you should forward them to spamreports@nhs.net using the process detailed in the Cyber Security Guide. You must not introduce or forward any virus or any other computer programme that may cause damage to NHS or social care computers or systems.

14.3 The deliberate introduction of viruses or similarly harmful programs will be considered as an act of gross misconduct and action will be taken in accordance with the Trust's disciplinary procedures. Further guidance on protection against computer viruses is available in the Trust's Information Security Policy.

15. EMAIL RETENTION AND DELETION

15.1 To support effective information management, all staff are expected to comply with the following principles of good practice for the retention and deletion of emails:

- Regularly review stored emails, deleting those that are no longer needed

[6] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/governance/?id=8444

- Retain or delete emails in accordance with the Records Management Code of Practice 2021[7] and NHSmail: Data Retention and Information Management Policy[8]. This guidance applies to all records, regardless of the media on which they are held
- Keep the contents of mailboxes to a minimum
- Never use the NHSmail system as a document filing system or for long-term storage of business-critical information
- Save messages and/or attachments in your personal network drive, a shared work area, or a shared drive as appropriate (not the C: Drive (desktop)
- Use the 'Auto Archive' function for old messages - this will delete messages after a certain period and is useful for sent messages
- Consider setting your NHSmail account to remove deleted messages when exiting your account

15.2 Attachments should be saved to an appropriate directory - either on staff's personal or shared network drives and deleted from their mail folder. Information must not be saved onto the C: Drive/desktop unless this is on an encrypted laptop and access to the network is temporarily unavailable. Further details can be found in the Trust's Corporate Records Policy.

15.3 Emails and their content are requestable under the Freedom of Information Act (2000) and UK General Data Protection Regulation. This applies to all retained emails (including those held in 'deleted Items'), regardless of their content, sender, whether they relate to the business of the Trust, service staff, members of the public, or have been generated by staff for purposes not directly relevant to the Trust's business. Further details can be found in the Trust's Freedom of Information Act Policy and Data Protection, Confidentiality and Disclosure Policy.

Further information on the retention and deletion of emails is provided by NHS England[9].

16. MONITORING OF INTERNET AND EMAIL USAGE

16.1 The Trust will establish with Nottinghamshire Health Informatics Service suitable mechanisms for the routine monitoring of internet and NHSmail usage, this will include consideration of the 'Top Sites by Bandwidth.'

16.2 Monitoring records will be maintained, audited periodically and only communicated to those with a valid need to know.

[7] https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/#appendix-ii-retention-schedule
[8] https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/NHS+Digital+Policy+Docs/NHSmail+Data+Retention+and+Information+Management+Policy.pdf
[9] https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/NHS+Digital+Policy+Docs/NHSmail+Data+Retention+and+Information+Management+Policy.pdf

16.3 Records of activity undertaken through staff's login cannot be created, amended, altered, deleted, or destroyed by staff or any member of Nottinghamshire Health Informatics Service.

16.4 If staff inadvertently access a site to which they believe access should be prevented they should immediately inform their Line Manager and the Nottinghamshire Health Informatics Service Desk.

17.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored **(WHAT – element of compliance or effectiveness within the document will be monitored)**	**Responsible Individual** **(WHO – is going to monitor this element)**	**Process for Monitoring e.g. Audit** **(HOW – will this element be monitored (method used))**	**Frequency of Monitoring** **(WHEN – will this element be monitored (frequency/ how often))**	**Responsible Individual or Committee/ Group for Review of Results** **(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g. verbal, formal report etc) and by who)**
Audit activity and performance	Information Security Officer	Analysis of requests and responses	Monthly	Head of Data Security & Privacy
IG toolkit validation	360 Assurance	Audit	Annually	IG Working Group/Head of Data Security & Privacy /Audit and Assurance Committee/IG Committee
Adherence to IG policies and procedures in nominated Division	360 Assurance	Audit	Annually	IG Working Group/Head of Data Security & Privacy /Audit and Assurance Committee/IG Committee
IAO report to the SIRO	IAO	Self-assessment return	Annually	Head of Data Security & Privacy /SIRO/IG Committee

18.0 TRAINING AND IMPLEMENTATION

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[10] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[11]

The requirements identified in this document will be subject to regular monitoring with random audits conducted by Internal/External auditors, to ensure compliance and identified breaches/non-compliance will be dealt with accordingly.

19.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document is not subject to an Environmental Impact Assessment.

20.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Computer Misuse Act (1990) https://www.legislation.gov.uk/ukpga/1990/18/contents
- Copyright Designs & Patents Act (1988) https://www.legislation.gov.uk/ukpga/1988/48/contents
- Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Electronic Communications Act 2000 https://www.legislation.gov.uk/ukpga/2000/7/contents
- Freedom of Information Act (2000) https://www.legislation.gov.uk/ukpga/2000/36/contents
- Health and Safety at Work Act 1974 https://www.hse.gov.uk/legislation/hswa.htm
- Health and Social Care Act 2012 http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted
- Human Rights Act (1998) https://www.legislation.gov.uk/ukpga/1998/42/contents

[10] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[11] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

- Information Commissioner (2003), The Employment Practices Data Protection Code: Part 3: Monitoring at Work: Supplementary Guidance https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf
- ISO/IEC 27001:2013 https://www.iso.org/standard/27001
- ISO/IEC 27002:2013 https://www.iso.org/standard/54533.html
- Limitation Act 1980 https://www.legislation.gov.uk/ukpga/1980/58
- NHS England - IG standards for systems and development of guidance for NHS and partner organisations
- NHS England Secure email Standard https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb1596-secure-email
- Records Management Code of Practice 2021 https://transform.england.nhs.uk/information-governance/guidance/records-management-code/
- Regulation of Investigatory Powers Act 2000 https://www.legislation.gov.uk/ukpga/2000/23/contents
- The Environmental Information Regulations 2004 https://www.legislation.gov.uk/uksi/2004/3391/contents/made
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 https://www.legislation.gov.uk/uksi/2003/2426/contents/made
- The Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000 https://www.legislation.gov.uk/uksi/2000/2699/contents/made
- UK General Data Protection Regulation https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685632/2018-03-05_Keeling_Schedule.pdf.

Related SFHFT Documents:

- Accessing Encrypted Emails Guide for non-NHSmail users https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8637
- Confidentiality Audit Policy https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8634
- Data Protection, Confidentiality and Disclosure Policy https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8636
- Data Protection, Confidentiality and Disclosure Procedure https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8636
- Encryption Guide for NHSmail https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8637
- Information Governance Policy https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8639
- Information Security Policy https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8640

- Remote Working Policy https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8645
- Safe Haven Procedure https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8648

21.0 KEYWORDS

Safe Haven, encrypted, secure, confidential information, confidential information, unsecure

22.0 APPENDICES

- Please refer to the contents table

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Email and Internet Acceptable Use Policy			
New or existing service/policy/procedure: existing			
Date of Assessment: 6th July 2021			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None

Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None
Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None

What data or information did you use in support of this EqIA?

- Trust guidance for completion of the Equality Impact Assessments

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

- None

Level of impact

Low Level of Impact

Name of Responsible Person undertaking this assessment: Gina Robinson

Signature: G. H. Robinson

Date: January 2024

APPENDIX 2: APPROVAL FOR STAFF MONITORING – AUDIT DATA

Name & Job Title of Requester	
Date of Request	
Name & Job Title of the employee	
Detail the information that is required (e.g. require all websites accessed between May and June this year) Access to what systems	
What is the justification for requesting audit data? E.g. required as part of an investigation by HR.	
Are you the lead investigator?	
Is this part of an HR investigation?	
Is this a breach of Health & Safety that could jeopardise other workers	
Why do you require the information and how will the information be used and for what purpose	
Is this in relation to Criminal Activity at work or gross misconduct (please indicate severity)	
What is the timescale for the data to be provided?	
Has the member of staff been informed where the audit data may have privacy implications for the individual concerned (e.g. if emails are to be searched in the absence of the employee)? If no, then explain why.	

Signature/email authorisation of service lead/ Deputy Director of People Directorate:

IG Authorise or Decline:

Reason for decision:

Date:

Please Note: The information produced as part of this investigation monitoring may be required to be retained on the staff file.

APPENDIX 3 – APPROVAL FOR ACCESS TO BLOCKED INTERNET SITES

Website Unblocking

Web filtering plays a key role in protecting our network by categorising web sites and blocking access to those deemed high risk such as those associated with spam, hacking, phishing, and fraud. The filter also makes the web appropriate for business use by blocking any material considered to be illegal, racist, homophobic, immoral, obscene, offensive, or pornographic. If however you need access to a blocked website for work purposes follow the instructions below.

How to request unblocking of a website

1. Visit the NHIS Customer Portal https://customerportal.notts-his.nhs.uk/
2. Log in
3. Select: Security tab > **Unlock a Website > Fill in your details >**

Requests will be reviewed by Information Governance and the NHIS Cyber Security team to ensure the site does not pose a threat and, if approved.

APPENDIX 4 – PROCEDURE FOR INVESTIGATION OF SUSPECTED MISUSE OF THE INTERNET OR EMAIL

Suspected misuse of the Trust's internet or NHSmail systems may be identified (but not exclusively) by:

- Routine monitoring.
- Eyewitness accounts.
- Personal experience.
- Actual evidence (e.g. examples of inappropriate emails).
- Evidence of poor performance or time-wasting.
- External complaints or queries received.

The relevant line manager should initially discuss the suspected abuse with the Information Governance department to determine what action should be taken and where required an investigation will be carried out in accordance with the Trust's Disciplinary Procedure.

Suspicions or allegations of fraud and/or corruption in connection with the use of the internet and/or NHSmail system must be referred immediately to the Senior Information Risk Owner and the Trust's Local Counter Fraud Specialist. Where there is any doubt as to whether an allegation or suspicion relates to fraud and/or corruption, the Local Counter Fraud Specialist must be contacted for advice.

No discussions should be entered into with the suspected individual by their Line Manager or any other member of staff without agreement and guidance from the Local Counter Fraud Specialist (or /HR in the event of a Local Counter Fraud Specialist or criminal investigation being closed).

Where suspicion or allegation involves illegal activity that does not constitute fraud and/or corruption (following advice from the Local Counter Fraud Specialist where appropriate), the Information Governance department should refer the matter to the Police and contact the IT Service Desk to isolate the IT equipment as soon as possible

There are four options available that you can choose from to authenticate your account: Microsoft Authenticator App (available on all Trust devices), text message, phone call, FIDO2 token or NHS smartcard. Guidance on how to set up MFA is available here: Getting Started with MFA – NHSmail Support[12].

How to set up multi-factor authentication

4. Self-enrol - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Getting+Started+with+MFA_Steps+for+Self-Enrolment.pdf
5. Microsoft Authenticator App - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Setting+Up+MFA_Steps+for+Mobile+App.pdf

[12] https://support.nhs.net/knowledge-base/getting-started-with-mfa/#mobile-app-method-enrolment

6. Text message - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Setting+Up+MFA_Steps+for+Text+Message.pdf
7. Call - https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/Setting+Up+MFA_Steps+for+Phone+Call.pdf