Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

EMAIL AND INTERNET ACCEPTABLE USE POLICY

POLICY

Reference	ISP-02		
Approving Body	Information Governance Committee		
Date Approved	30th July 2021		
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	August 2021		
Version	3		
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 Digital		
Supersedes	2		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group Information Governance Committee		
Date of Completion of Equality Impact Assessment	6th July 2021		
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	30th July 2023 ***Extended to 29/01/2024***		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Information Security Officer		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Information Security Officer		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Not applicable	

CONTENTS

APPENDICIES

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) by reading the Transparency Information.

As an NHSmail account holder, you should expect to receive ad-hoc communications about NHSmail from NHS Digital 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 Digital 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 Trusts business use and for work-related educational and research purposes. Access for limited and appropriate personal use in his or her own time is allowed.

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.

Don't…

X Send personal confidential data 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.

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

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

[1] https://www.sfh-tr.nhs.uk/media/7278/isp-021-encryption-guide-for-nhsmail-version-7.pdf

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 Management Policy)
- 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 personal confidential data
- 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.

Browser: the Trust uses Microsoft Internet Explorer as its standard browser. Nottinghamshire Health Informatics Service will ensure that the current recommended version is available on all desktop PCs.

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.

UK General Data Protection Regulation: supersedes the Data Protection Act 1998, 2018 and EU General Data Protection Regulation.

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

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 personal confidential data 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**).

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

Malicious software/Malware: software designed to harm a computer or network. Includes but is not limited to:

- **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.
- **Trojan horses -** malicious, security-breaking programs disguised as something benign such as a screen saver or game,
- **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).
- **Ransomware** - a growing threat in the cyber threat landscape. Usually delivered via phishing Emails, 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's 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.
- **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?

- **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.

Personal Confidential Data (PCD): this term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this policy 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include 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.

Phishing: sending an Email to staff falsely claiming to be an established legitimate enterprise in an attempt to defraud staff into surrendering private 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.

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

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.

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

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.[2]

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

4.0 ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive is responsible for ensuring that the Trust complies with the statutory and good practice requirements governing internet and NHSmail use outlined in this policy and is supported by the delegated management responsibilities outlined below.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner has lead responsibility for the security and confidentiality of the Trust's information, ensuring that information risk is properly identified and managed.

Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient information processed by the Trust and enabling appropriate information sharing.

Information Governance Manager and Data Protection Officer

At an operational level, the information governance agenda is led by the Senior Information Risk Owner, supported by the Information Governance Manager. They are responsible for the effective management of all aspects of Information Governance, including ensuring that systems and processes are in place to support compliance with this policy.

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

The Information Governance Manager 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.

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

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 which organisation they are employed by. 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 Digital 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.

6.10 Staff accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other person without a legal basis or prior authorisation from senior management is strictly forbidden and shall be deemed a disciplinary offence. Staff access to systems and audit trails are monitored in the Trust systems to show what users are accessing.

6.11 Use of NHS information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and shall be deemed a disciplinary offence.

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, but it is accepted that they may be accessed for purposes not directly relevant to the Trust's business. This should only take place outside an individual's normal working hours or during authorised rest periods, and where this does not interfere with the normal work duties of the individual or others. Excessive personal use of the internet during working hours shall not be tolerated 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. Should you need to, by exception, send communication of a personal

nature you must clearly state that your message is a personal message and not sent in your official capacity.

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. Personal Emails must be kept separately from work Emails and deleted regularly.

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

7.4 Staff must not upload and download private 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 private 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. Personal NHSmail and internet use must adhere to the terms of this policy.

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. USER RESPONSIBILITITES INCLUDING CLEAR DESK PROCEDURES

The following should be read in conjunction with the ‘Misuse of the Internet and NHSmail Systems’ section 9 below.

8.1 Staff must lock their terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete or Windows + L function or other applicable method) when left unattended, even for a short period. Computer screens must be angled away from the view of unauthorised persons.

8.2 Staff must not install unapproved or privately owned software on Trust equipment. Only authorised IT personnel shall be allowed to reconfigure or change system settings on the IT equipment.

8.3 Laptops and mobile devices (including storage media) shall:

- Only be used by the NHS or third-party employee who has signed and taken personal responsibility for the device.
- Have the corporate standard encryption software installed, rendering the information on the laptop inaccessible if the device is stolen or lost.
- Have the corporate standard anti-virus, anti-spyware, and personal firewall software installed.
- Have the corporate standard remote access installed.

8.4 If configured according to the specifications above the laptop/mobile device may be connected to wired or wireless access points.

8.5 NHS laptops shall never be (via cable or wireless) directly connected to other non-NHS IT equipment or systems. The use of home printers or using devices to print information off site is not permitted.

8.6 Staff must not use privately owned storage devices or storage devices owned by third parties for transfers of NHS data without permission and undertaking a security risk assessment. Further guidance is available on the NHIS Customer Portal

8.7 Any device lost or stolen shall be reported immediately to your line manager, Nottinghamshire Health Informatics Service Customer Portal https://customerportal.notts-his.nhs.uk/, or NHIS.ServiceDesk@nnotts.nhs.uk or call 01623 410310 and the police if advised to do so.

8.8 Staff using the internet and NHSmail must conduct themselves in accordance with their terms and conditions of employment or appointment.

8.9 Staff must not broadcast personal messages, advertisements, or other non-business-related information via NHSmail.

8.10 Staff must only use the Windows Internet Explorer, Google Chrome and Firefox Web browsers supplied and maintained by Nottinghamshire Health Informatics Service. Staff must

not load other browsers or ISP (Internet Service Provider) software, later versions / patches or upgrades from CD-ROM, floppy disk or from the internet (including Windows updates).

8.11 Staff who intend to make information available over the internet about the Trust's facilities and services must ensure that they liaise with the Trust's Communications Team and the Branding and Design Guidelines.

8.12 Staff must not continue to use an item of networking software or hardware, following a request from Nottinghamshire Health Informatics Service or a Trust manager to cease doing so on the grounds of causing disruption to the correct functioning of the Trust's information systems. Internet monitoring software is in use, which prevents access to certain sites. Where staff has a legitimate business, clinical or research need to access a restricted site they should complete the online process using the NHIS Customer Portal. The process is detailed in Appendix 3.

8.13 It is recognised that in the course of their work or associated research, some staff may have a requirement to access, transmit or receive material that may be defined as offensive, obscene, indecent, or similar. Any such requirement should be logged with the Information Governance department. In most cases, such internet sites will be blocked as standard and will require unblocking using the online process using the NHIS Customer Portal. Access to pornographic images is deemed misuse. Staff shall not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic, or obscene.

8.14 Engaging in any illegal activities via NHSmail or the internet is prohibited. Discovery of such material shall, if deemed as being of a criminal nature, be handed over to the police.
Staff shall not distribute statements of a political or religious nature, or other information of a personal nature.

8.15 Downloaded files become the property of the Trust and it is staff's responsibility to obey any licensing terms that may apply.

8.16 Downloading images, MP3 files and streaming video or audio can have a significant impact on the performance of the network and must be restricted to authorised clinical and research needs only. It is accepted that webinar and conferences are now attended remotely, and this usage is permitted.

8.17 Staff are expected to use the same personal and professional courtesy in Emails as they would in any other forms of communication. NHSmail messages are written documents and may be used as such in a court of law. They may also be disclosed to the public as the result of a UK General Data Protection Regulation and/or Freedom of Information Act request. Therefore, staff are advised to create all Email messages with a view to them being public correspondence.

8.18 In using NHSmail to communicate externally, staff must not give the impression that their comments represent the views of the Trust unless specifically authorised to do so.

8.19 The use of NHSmail for critical correspondence should not be relied upon without independent verification of receipt. Further guidance on the correct usage of NHSmail for corporate correspondence can be found in section 14 of this policy - 'NHSmail Retention and Deletion'.

8.20 NHSmail addresses are traceable and identifiable to the Trust.

8.21 Staff using work issued devices or accessing the web version of NHSmail from personal or unencrypted devices must also refer to the Electronic Remote Working Policy and the Information Security Policy available on the Trust's website.

8.22 Further guidance on the correct use of Trust devices is available in the Trust's Information Security Policy.

9. MISUES OF THE INTERNET AND EMAIL SYSTEMS

9.1 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.

9.2 All staff are responsible for complying with the 'Personal Use' and 'User Responsibilities' sections above and for ensuring that they do 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 (other than for lawful and properly supervised purposes – see section 7.7 above).

b) Accessing or transmitting pornographic images falling into the following categories:

- Level 1: Indicative (non-erotic/sexualised pictures)
- Level 2: Nudist (naked or semi-naked in legitimate settings/sources)
- Level 3: Erotica (surreptitious photographs showing underwear/nakedness)
- Level 4: Posing (deliberate posing suggesting sexual content)
- Level 5: Erotic Posing (deliberate sexual or provocative poses)
- Level 6: Explicit Erotic Posing (emphasis on genital areas)
- Level 7: Explicit Sexual Activity (explicit activity, but not involving an adult)
- Level 8: Assault (sexual assault involving adult)
- Level 9: Gross Assault (penetrative assault involving adult)
- Level 10: Sadistic/Bestiality (sexual images involving pain or animal).

Instances of misuse falling into Level 3 will be reported immediately to the Police.

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

d) 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.

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

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

o) 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.

p) Any deliberate attempt to disable, defeat or circumvent the Trust's internet firewall and other security measures in place to protect the network.

q) Failing to comply with this policy when a Virtual Private Network (VPN) system is used to access the Trust's network.

r) Any attempt to disrupt, corrupt or otherwise negatively affect the Trust's information assets.

s) Unwarranted sending of large messages or attachments.

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

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

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

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

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

y) 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.

9.3 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.

10. INVESTIGATIONS OF SUSPECTED MISUSE

10.1 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.

10.2 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.

10.3 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.

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

10.5 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.

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

11. TRANSFER OF PERSONAL CONFIDENTIAL DATA AND CONFIDENTIAL CORPORATE INFORMATION

11.1 Transfer of any information must give due consideration to the nature of the information that is being transferred and whether the means of transfer is sufficiently secure. All transfers must comply with the Secure Transfer of Information/Safe Haven Policy.

11.2 Personal confidential data (PCD) 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[3], 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.

11.3 All transfers of personal confidential data must comply with Data Protection 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.

[3] 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

11.4 All staff must comply with the following agreed methods for the internal and external transfer of personal confidential data by NHSmail. Failure to comply is a breach of this policy and contravenes requirements of the UK General Data Protection Regulation and the Confidentiality: NHS Code of Conduct.

11.5 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.

11.6 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 personal confidential data 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 personal confidential data 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 personal confidential data 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 personal confidential data 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 personal confidential data 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 Digital'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

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.

11.7 If there is a requirement to transfer personal confidential data 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.

11.8 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 personal confidential data is not considered secure transfer as password protected documents can easily be accessed. **Password protection of documents is not required.**

11.9 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 personal

confidential data. 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.

11.10 Instant Messaging services i.e. WhatsApp, Messenger are not secure and must not be used to process personal confidential data.

11.11 Agreed information sharing protocols must be used when sending or forwarding personal confidential data to individuals in other Trusts. Regular flows of personal confidential data 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.

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

11.13 Please note 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. Access under these circumstances is permitted for View Only purposes - please contact Information Governance if further guidance is required.

11.14 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, access is permitted to merely view Emails, contacts, and calendar.

11.15 It is vital that line managers ensure ALL NHSmail accounts are marked as leavers, by Nottinghamshire Health Informatics Service once the staff member has left the Trust to ensure Web access is closed. Guidance is available in the Leavers and Joiners Guide.

11.16 When moving roles between health and care organisations, it is your responsibility to ensure any data stored in the NHSmail account relating to your current/previous role is archived appropriately and/or deleted. It must not be transferred to your new employing organisation without consent of the organisation you're leaving. Guidance is available in the Leavers and Joiners Guide. The Local Administrator (NHIS) has the right to empty the users OneDrive at any time without the consent of the user with permission from the Trust.

12. USE OF SOCIAL MEDIA

12.1 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.

12.2 Staff must not disclose any Trust information that is or may be personal confidential data, or that is subject to a non-disclosure contract or agreement. Please refer to the Trust's Social Media Policy.

13. CYBER SECURITY

13.1 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.

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

13.3 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.

14. EMAIL RETENTION AND DELETION

14.1 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.
- Retain or delete Emails in accordance with the Records Management Code of Practice (2020) and NHSmail: Data Retention and Information Management Policy 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.
- If you plan to be away from work for an extended period, ensure that a colleague has delegated access to your NHSmail account at an appropriate level. Further guidance is here: Giving delegate access to your mailbox – NHSmail Support.

14.2 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 g Corporate Records Policy.

14.3 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 Digital.

15. MONITORING OF INTERNET AND EMAIL USAGE

15.1 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'.

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

15.3 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.

15.4 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.

16.0 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	Information Governance Committee/ Information Governance Manager/Data Protection Officer

17.0 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[4] 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.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation
A copy of this policy and relating guidelines and procedures will be posted on the Information Governance section of the Trust's website and Intranet.

The Communications Team will ensure Trust-wide communication of the Policy.

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.

Resources
No additional resources are required.

18.0 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.

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

Evidence Base:
- Computer Misuse Act (1990)
- Copyright Designs & Patents Act (19988)

[4] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)

- Data Protection Act 2018
- Environmental Information Regulations 2004
- Freedom of Information Act (2000)
- EU General Data Protection Regulation 2016
- Health and Safety at Work Act 1974
- Health and Social Care Act 2012
- Information Commissioner (2003), The Employment Practices Data Protection Code: Part 3: Monitoring at Work: Supplementary Guidance
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- NHS Digital - IG standards for systems and development of guidance for NHS and partner organisations
- NHS Digital Secure Email Standard https://digital.nhs.uk/media/322/ISB-1596-conformance-statement-for-NHSmail/pdf/ISB_1596_Conformance_Statement_for_NHSmail_August_2016
- The Electronic Communications Act 2000
- The Human Rights Act (1998)
- The Limitation Act 1980
- Records Management Code of Practice (2020)
- The Privacy and Electronic Communications Act (EC Directive) Regulations 2003
- The Regulation of Investigatory Powers Act (2000)
- The Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations
- UK General Data Protection Regulation.

Related SFHFT Documents:

- Accessing Encrypted Emails Guide
- Confidentiality Audit Procedure
- Data Protection, Confidentiality and Disclosure Policy
- Data Protection, Confidentiality and Disclosure Procedure
- Electronic Remote Working Policy
- Email Guidance
- Information Governance Policy
- Information Security Policy
- Safe Haven Procedure

20.0 KEYWORDS

Safe Haven, encrypted, secure, personal confidential data, unsecure

21.0 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: 6th July 2021

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 of service lead/ Deputy Director of HR:

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 an important 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, the site will be unblocked for the requester only.

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