Northamptonshire Healthcare NHS
NHS Foundation Trust

Email - Acceptable Use Procedure

IMTr004

Table of Contents

Why we need this Procedure

This procedure sets the standards for the use and management of e-mail, states the position of Northamptonshire Healthcare NHS Foundation Trust (NHFT) and sets out the obligations that all members of staff have when dealing with e-mail messages. This procedure is designed to ensure NHFT are complying with legislation and best practice standards.

What the Procedure is trying to do

This e-mail procedure applies to all e-mails in use within NHFT. It sets out the obligations that all members of staff have when dealing with e-mail. It covers the sending, receiving, forwarding and storing of all e-mail messages, whether internal or external. This procedure also details the IM&T responsibilities for the management of mailboxes.

This procedure applies to all NHFT staff, (including Non-Executive Directors, trainees, temporary staff, researchers, trainers, and consultants provided with authorised access to NHFT computer systems). It also includes those staff not directly employed by NHFT but who have access to NHFT e-mail systems.

Which stakeholders have been involved in the creation of this Procedure

- IM&T Programme Board
- Office365 Board

Any required definitions/explanations

NHFT: Northamptonshire Healthcare NHS Foundation Trust

Disaster recovery: specific steps taken to resume operations in the aftermath of a catastrophic disaster or failure, for example through duplicating computer operations, routine off-site backups, and procedures for activating critical information systems in a new location.

Data Backups: the activity of copying files or databases so that they will be preserved in case of equipment failure.

Distribution Lists: a group of mail recipients that is addressed as a single recipient.

E-mail / electronic mail: the transmission of messages over the IT networks, most commonly using software such as Microsoft Outlook.

E-mail encryption: the conversion of an email into a code which cannot be understood by unauthorised people.

Information security: protection of the confidentiality, integrity and availability of data and information. In other words: (i) restricting information to those with a need to know (Confidentiality); (ii) Information is accurate and complete (Integrity); (iii) Information and services are available when needed (Availability).

NHSmail 2: the national email service available to NHS staff in England and Scotland. This is different to the Trusts own nhft.nhs.uk email system. NHSmail 2 encrypts data between NHSmail 2 accounts, to standards approved by the NHS.

Office 365 all email mailboxes are located in the cloud Microsoft Office365 cloud. The security arrangements for this solution comply with SCCI1596.

Phishing: an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather sensitive personal and financial information from recipients, for example by sending users to fake, but legitimate looking websites.

Spam: also known as junk email or unsolicited bulk email – involves nearly identical messages sent to numerous recipients by email – generally e-mail advertising for some product sent to a mailing list or newsgroup

Virus: A virus is a malicious program that has the ability to reproduce itself and infect other programs or storage devices. Typically a virus will not show itself immediately, but will add itself to programs and disks to spread widely on many computers before it is triggered into its destructive phase.

Key duties

E-mail is a business communication tool and ALL staff must use this tool in a responsible, effective and lawful manner. All e-mail accounts maintained on the e-mail system are the property of NHFT.

Overall accountability:

Ultimate responsibility rests with the Chief Executive and delegated senior managers of NHFT who are personally accountable for the implementation and compliance of all NHFT policies.

Senior Information Risk Owner (SIRO)

To oversee and direct IM&T in the management and delivery of this procedure including providing access to ESR to enable effective management of the starters and leavers process.

The SIRO has overall responsibility for information governance and information security incident management and reporting.

The IM&T Directorate accountability:

-to ensure that only authorised users of NHFT computer can access and use e-mail facilities

- Systems are maintained and managed to provide secure and effective communications solutions at all times

- The global address list is maintained and up to date. (Please note that this relies specifically on line-managers completing the Starters and Leavers protocol.)

- All complaints and breaches of procedure concerning the unacceptable use of e-mail on NHFT systems are investigated appropriately.

- E-mail systems are used effectively and efficiently through the provision of awareness programmes and the formulation of this procedure

- Monitoring the implementation of this procedure.

To remove mailbox accounts when notified of leavers (mailboxes are automatically destroyed 30 days after an account being removed)

To interrogate active mailboxes Trust Wide if required to do so under legal request.

To interrogate active mailboxes upon request from a HR Business Partner where linked to a disciplinary investigation.

Department heads, Service and Line Managers accountability:

- Implement and monitor the operation of this procedure within their functional areas.

- Ensure that staff follow and adhere to this procedure at all times.

- Ensure that staff complete their annual Information Governance Training.

- Ensure the correct usage of the Starters and Leavers protocol within NHFT.

Staff accountability:

Every user of e-mail has the responsibility to ensure that they practice appropriate and proper use of the e-mail system, that they understand their responsibilities, and do not bring NHFT into disrepute.

- Are responsible in law for any e-mails they create or amend.

- Understand when use of e-mail is strictly prohibited.

- Must be aware that any e-mails they create are not their personal property, but belong to NHFT, and may be subject to public disclosure.

- Take due care and attention when sending, receiving, amending and storing all e-mail transactions.

- Should comply with good housekeeping routines, to manage their mailboxes appropriately, ensuring that e-mails are actioned, deleted or stored for reference purposes.

- Should understand their responsibilities under the law.

- Share e-mails and the information they contain only in accordance with professional standards, local policy and information sharing protocols. Staff must not share passwords with anyone. All staff are personally liable for any e-mail misuse logged under their username and password

Staff must log any incidents relating to email misuse on Datix following Trust Incident Policy CRM002.

The use of NHFT e-mail facilities by individual members of staff assumes and implies compliance with this procedure, without exception.

Procedure detail

Legal Framework

Although e-mails seem to be less formal than other written communication, their legal status is the same. Anything sent by e-mail is just as likely to form a legally binding contract and be admissible in court proceedings, as if it were a written document sent by post or fax. Therefore e-mail messages should be treated with the same level of attention given to drafting and managing formal letters, reports and memos.

As part of the written corporate record of the Trust they are subject to legislation such as the Public Records Act (1958 & 1967) the General Data Protections Regulations (2018), the Freedom of Information Act (2000) and the European Convention on Human Rights . As such e-mails may be released in part or whole to a wider audience or used as evidence in legal proceedings.

This means that care should be taken with regards to ensuring that users do not:

- Send messages or attachments that could be deemed libellous, defamatory, harassing or pornographic
- Breach the Data Protection Act 2018
- Breach the Common Law Duty of Confidentiality
- Send information in breach of Copyright legislation

E-mail is capable of forming or varying a contract in just the same way as a written letter. Such capability gives rise to the danger of employees inadvertently forming contracts on behalf of NHFT or varying contractual terms in which NHFT then becomes bound.

NHFT will be held liable for any representations made or contractual arrangements entered into by its employees if it is reasonable to assume that such employees were acting with the employer's authority.

All employees should therefore take due care when drafting the words of an e-mail so that they cannot be construed as forming or varying a contract when this is not the intention.

Prohibited Use of E-mail Facilities

NHFT encourages and supports the use of e-mail as an appropriate business tool for internal and external communications. However it is vital that e-mail is used effectively and appropriately at all times by all staff.

Whilst there are times when the use of e-mail is not the best option for communications or information sharing there are other types of e-mail use that are **expressly prohibited.**

This includes any behaviour or comments that are not acceptable in the spoken or paper environment as these are also not acceptable within the e-mail environment.

This also includes the transmission (i.e. sending, receiving or forwarding) of any material that:-

- Brings the NHS or NHFT into disrepute.
- Is abusive or threatening to others.
- Discriminates or encourages discrimination on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, and disability, political or religious beliefs.
- Contains offensive, obscene or indecent images, data or other material.
- Contains unsolicited commercial or advertising materials, chain letters, jokes and executables or junk mail of any kind.
- Infringes copyright of another person including intellectual property rights.
- Wastes staff effort or networked resources.
- Corrupts or destroys other user's data or disrupts the work of other users.
- Violates the privacy of others.
- Attempts to disguise the identity of the sender, is anonymous or is deliberately forged.

In addition it is important to understand that e-mail messages containing inaccurate information about an individual or organisation, may result in legal action being taken against the person sending the e-mail message and anyone forwarding the e-mail message on to others.

The transmission of e-mails that include any of the above could result in formal disciplinary proceedings being taken against the person sending the message and anyone forwarding the email message to others.

Framework and Controls

Core Principles

- NHFT staff will be provided with a mailbox licence with an 'nhft.nhs.uk' e-mail account.

- Leaver's mailbox licences will be removed and email content will be securely destroyed after 30 days of their leave date.
- Safeguards will be established to protect the security, integrity and availability of NHFT systems.

IT Controls

There are a number of safeguards and controls built into the e-mail system to protect the system from overload. These safeguards and controls are also dependent on good user practices and housekeeping measures. It is the user's responsibility to ensure that the e-mail system is not used to store non-work related material and that work related e-mails are actioned, deleted or transferred into a more appropriate filing location.

Microsoft is responsible for disaster recovery and data storage within the secure Azure environment.

Control Measures

Mail Box Limits

Each user is allocated a base mailbox size. When this limit is reached, the user will receive a warning message as they approach their mailbox size limit. When the limit has been reached the user receives a prohibited send message and is not able to send further emails until the mailbox has had enough emails deleted to meet the size limit requirements. The third warning is reached on exceeding the mailbox and stops both sending and receiving. Senders of emails to a full mailbox will receive a non-delivery report message. It is the user's responsibility to ensure they manage their mailbox and transfer to the appropriate network files emails that require permanent preservation.

Any emails relating to clinical care must be stored in the clinical record in line with Health Records Management Policy IGP107.

Distribution Lists

IM&T can create NHFT e-mail distribution lists/groups for specific communication purposes. The lists/groups are set to have a file size limit. This is to prevent large attachments being sent to many users.

- Alternative methods must always be considered such as the Staff Room/e-Brief for mass mailing announcements or publishing your documents on NHFT Intranet. Files are unusually large if graphics and pictures are used within. These should be removed if unnecessary.
- Inappropriate use of email distribution lists waste both network resources and staff time, for this reason they are to be used solely for distributing information which is relevant to everyone on the list and cannot be communicated effectively by any other method.
- IM&T can created distribution lists/groups and provide access to specific staff and groups.

Security Controls

NHFT emails are stored within the Microsoft environment. Microsoft is responsible for scanning of all inbound and outgoing messages to identify security threats including Viruses, Malware, Malicious URL's, SPAM, Phishing and suspect attachments. NHFT staff must continue to be vigilant. In the event that a user suspects a virus or hoax alert, they must stop using their machine and contact the IM&T Service Desk immediately logging the call as urgent.

Business Continuity/Disaster Recovery

NHFT emails are stored within Microsoft data centres and are subject to Microsoft's business continuity and disaster recovery policies and procedures. Customer data is stored in a redundant environment with robust data protection capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are implemented, ranging from redundant disks to guard against local disk failure to continuous, full data replication to a geographically diverse data centre. More information is available via the Microsoft Office365 website (https://technet.microsoft.com/en-us/library/office-365-service-health.aspx).

- IM&T will not recover accidental deletion of email related items due to the time and processes involved. This includes the restore of accounts that have been deleted after an individual has left the organisation.

Disclaimer

This following disclaimer will be automatically added to the bottom of every outgoing e-mail by the IM&T Directorate.

This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Any views or opinions expressed are those of the author and do not represent the views of the Trust unless explicitly stated.

The information contained in this email may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this email and your reply cannot be guaranteed.

Staff must not use their own versions of disclaimer notices.

Personal Use

Limited personal use of email is currently permitted provided that full compliance with this policy is maintained. Staff must not use their NHFT email address to register with external sites, unless this is pursuant to work related activities, e.g. Trade union or professional memberships, or unless it is to be used for limited and exceptional circumstances, e.g. as an 'emergency contact' address with known external agencies, such as your child's school.

Staff should be aware that use of e-mail may be subject to monitoring, and disclosure to others. Therefore in order to respect and protect the privacy of individuals in compliance with the European Convention on Human Rights it is strongly advised that all personal/private e-mails: -

- Are not stored in Mailboxes or Personal Folders but are actioned and deleted immediately from all mailboxes

REMEMBER THAT THE MAILBOX IS A WORKING BUSINESS COMMUNICATIONS TOOL – NOT A PERSONAL TOOL.AND ANY EMAILS COULD BE SUBJECT TO DISCLOSURE UNDER LAW.

Access to Individual Mailboxes

All e-mail accounts maintained on the e-mail system are the property of NHFT. There are occasions when it is necessary for the Trust to access e-mail messages from an individual's mailbox and when e-mail messages sent or received may be seen by others e.g. when a person is away from the office for an extended unplanned period, to meet a legislative request, has left the organisation or simply in the interests of business continuity.

The Process for accessing an individual's mailbox is as follows:

- Gain written authorisation from the relevant Director or delegated appropriate Head of Department, (not simply line manager). The need for access must be justified and in keeping with the Data Protection Act 2018, the Convention on Human Rights and the Information Commissioners Office: Employment Practices Code Part 3 Monitoring at Work 2005. If in any doubt contact the Information Governance Lead for clarification.
- Submit a Request for Access to the Service Desk.
- A record should be made of the reasons for accessing the mailbox.

Home working

Trust emails, including those containing confidential and/or sensitive information or data, must not be sent to personal / home email accounts, unless specific authorisation has been given. Any confidential and/or sensitive information that is copied or removed from the workplace should be subject to approved procedures designated to minimise the risk of loss or disclosure.

Alternative solutions exist to enable access to email (and certain other NHFT IM&T services) to support home working. Specifically this is the use of laptop and VPN software, connected via a secure personal broadband account. Users should contact the IM&T Service Desk to request this.

Sensitive and Personal Information

Staff must ensure that all information of a sensitive nature that is sent via e-mail is treated with care in terms of drafting and addressing. Sensitive information sent via e-mail that is incorrect might provide a case for initiating legal proceedings against the person sending the information and/or

NHFT. Sensitive information can include commercial information, information about specific individuals or groups and Service user information. Confidentiality can be compromised especially when using external Internet-based e-mail systems and the privacy and confidentiality of messages sent via e-mail cannot be guaranteed. It is the responsibility of all members of staff to exercise their judgement about the appropriateness of using e-mail when dealing with sensitive or confidential subjects.

Sending emails securely

NHFT have adopted Office 365 for use by all staff within the Trust as its secure email solution as recommended by NHS Digital. The NHFT email solution meets the standards detailed within the NHS Digital *Office 365: Secure Email Configuration* (September 2017) document.

Sending emails within NHFT: nhft.nhs.uk to nhft.nhs.uk addresses

Where it is essential to send personally identifiable information by email within NHFT, please observe the following best practice protocol:

- Check the recipients email address is correct.

- Do not include identifiable or sensitive corporate information in the subject header of the email.

- Be aware that emails could be forwarded on outside of your control.

- Understand that emails relating to an individual may be disclosable under the Data Protection Act 2018.

- E-mail messages containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message, for example an e-mail message containing comments about the performance of a specific staff member or a group of staff. This should decrease the likelihood of the message being forwarded to unintended recipients.

Sending emails to public sector non nhft.nhs.uk addresses

There is encrypted transit in place for emails sent from nhft.nhs.uk to the following email domains:

- Gov.uk
- Secure.nhs.uk
- nhs.net
- cjsm.net
- pnn.police.uk
- mod.uk
- parliament.uk

Sending emails to other external email addresses

Put [Secure] in the subject line if sending personal confidential data or sensitive data to:

- Nhs.uk (not nhft.nhs.uk or secure.nhs.uk)
- Any other email address

This method of encryption allows the recipient to respond to the message sent and will secure the email conversation.

Recipients will receive email notification of a secure message having been sent and will be asked to follow the on screen instructions to access the email. If there are issues experienced by the recipient the sender of the email is responsible for supporting the recipient to receive the information securely via other means.

Staff are permitted to reply directly to Northamptonshire County Council emails that have been sent to NHFT via Egress Switch.

Sending secure emails from NHSmail

The functionality exists within NHSmail to enable users to send encrypted emails to addresses outside of the Government Secure Framework.

When sending emails outside of NHSmail, use [secure] at the start of the email subject. [Secure] is not case sensitive. The NHSmail service will assess whether encryption is required.
• If the domain the email is being sent to is accredited, the email will be sent securely and no further encryption is required.
• If the domain the email is being sent to is not accredited, and therefore insecure, the NHSmail service will programmatically enforce the use of the encryption tool to protect the email data. The recipient will need to log into the Trend Encryption Micro portal to unencrypt the email before it can be read.

Please follow the instruction on the below link to use this function:

https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/encryptionguide.pdfCommunications with Service Users: Ensuring Compliance with the Data Protection Act 2018.

Sending emails to Service users

You should not normally use email to establish a Service users-clinician relationship. Rather, email should add to and follow other, more personal, encounters, when the Service user has given permission for you to communicate with them by email.

Only use email with service users who have given their informed consent for using email to communicate with them. This consent should be clearly recorded in the care record.

Even when using secure email, privacy and confidentiality can be broken, usually as a result of human error. Service users should have the opportunity to accept this risk before you send any confidential or sensitive information, this should form part of the consent discussion.

Use of email is not always appropriate, for example when the email relates to mental-health treatment or sexual-health diagnoses. Please check with your manager or the Information

Governance team if you are unsure. Email communications with service users must always be saved on the clinical record.

Training requirements associated with this Policy

Information Governance training has been integrated into NHFT's induction programme for all new staff. For existing staff, an ongoing programme of training will be delivered as part of NHFT's Information Governance training programme. Additional campaigns and awareness raising will be undertaken as appropriate.

Specific Training

It is the responsibility of all managers to ensure attendance at induction and training programmes and to obtain feedback from staff regarding the knowledge and understanding they have obtained.

Individuals have an obligation to seek training, advice and support where uncertain in order to improve Freedom of Information practices appropriately.

Ad hoc training sessions based on an individual's training needs as defined within their annual appraisal or job description.

How this Policy will be monitored for compliance and effectiveness

Aspect of compliance or effectiveness being monitored	**Method of monitoring**	**Individual responsible for the monitoring**	**Monitoring frequency**	**Group or committee who receive the findings or report**	**Group or committee or individual responsible for completing any actions**
Duties			To be addressed by the monitoring activities below.		
Adherence to email procedure.	Monitoring of Incident log and audit	Head of Clinical Systems & Governance	Updates to be included as required in IG monthly Highlight Reports.	IM&T Programme Board.	IM&T Programme Board
Where a lack of compliance is found, the identified group, committee or individual will identify required actions, allocate responsible leads, target completion dates and ensure an assurance report is represented showing how any gaps have been addressed.					

For further information

Compliance with all NHFT policies is a condition of employment and a breach of policy may result in disciplinary action. This policy is complementary to other NHFT policies and protocols and should be used in conjunction with them, but especially with:

- IGIS01 - Use of Information and Communications Technology Policy
- IGP107 Health Record Management Policy
- IGP113 – Systems Data Quality Policy

Equality considerations

The Trust has a duty under the Equality Act and the Public Sector Equality Duty to assess the impact of Policy changes for different groups within the community. In particular, the Trust is required to assess the impact (both positive and negative) for a number of 'protected characteristics' including:

- Age;
- Disability;
- Gender reassignment;
- Marriage and civil partnership;
- Race;
- Religion or belief;
- Sexual orientation;
- Pregnancy and maternity; and
- Other excluded groups and/or those with multiple and social deprivation (for example carers, transient communities, ex-offenders, asylum seekers, sex-workers and homeless people).

The author has considered the impact on these groups of the adoption of this Policy and does not believe that there are any specific equality considerations that need to be taken into account.

Reference Guide

Faster, better, safer communications using email in health and social care for patients and healthcare professionals, March 2015, PRSB.

Microsoft Office 365 Service Health and Continuity
https://technet.microsoft.com/en-us/library/office-365-service-health.aspx

Office 365: Secure Email Configuration, September 2017, NHS Digital.

Document control details

Author:	The Information Governance Team
Approved by and date:	IM&T Programme Board – 05.02.2019
Any other linked Policies:	None
Policy number:	IMTr004
Version control:	Version 3:

Version No.	Date Ratified/ Amended	Date of Implementation	Next Review Date	Reason for Change (eg. full rewrite, amendment to reflect new legislation, updated flowchart, minor amendments, etc.)
1.0	04.11.2014	05.11.2014	04.11.2016	Inclusion of service user guidance and update to national email guidance
2.0	04.11.2014	05.11.2014	31.03.2018	Update as a result of Office 365
3.0	25.06.2019	26.06.2019	25.06.2022	Updated as a result of encryption methods