Tees, Esk and Wear Valleys
NHS Foundation Trust

Email Policy

Ref IT-0006-v6

Status: Ratified
Document type: Policy

Contents

1 Introduction

This policy sets out the rules and provides guidance on what the Trust deems as acceptable and unacceptable use of email, including what email system should be used.

The Trust's email system is NHS mail – this is a secure national email service which enables the safe and secure exchange of sensitive and personable identifiable (PI) information within the NHS and other local/central government agencies.

2 Why we need this policy

Email is an essential business tool used for communication and sharing information and this policy sets out the rules and provides guidance on what the Trust deems as acceptable and unacceptable use of email.

2.1 Purpose

Adhering to this policy will ensure that the Trust:

- Ensure staff have a clear understanding of the use of email
- Complies with legislation
- Minimises' the risk of damage to Trust data and computer by virus infection.
- State what email system must be used to conduct Trust business

2.2 Objectives

The objectives of this document are to:

- Explain the policy that governs the use of email within the Trust
- Set out what is deemed as acceptable and unacceptable use
- Ensure staff are aware of their responsibilities when using email, including our trust's values and behaviours

3 Scope

3.1 Who this policy applies to

- This policy applies to all employees of the Trust, non-executive directors, contractors and third parties (including agency staff), students, trainees, secondees, staff on placement with the Trust, and staff of partner organisations with approved access; and all email systems supported by the Trust.

- This policy also applies to the use of Trust-provided mobile devices including but not limited to: phones, tablets, laptops, and any other portable device on which email can be used.

3.2 Roles and responsibilities

Role	Responsibility
Staff, Students, contractors	• Use NHSmail for all business communication • Accept and comply with the NHSmail Acceptable use policy • Complete network training prior to using the Trust's email system. • Be aware of the Trust's associated policies as set out in section 9 • If accessing NHSmail from a non trust device, do so only using the web browser and not an email client. • Ensure nondisclosure of personal information outside of the Trust's policies and procedures • Follow the Corporate Records Guidance as emails are classed in law as legal documents and can be a corporate record. • Ensure that email content does not damage the professional reputation of the Trust • Consider the content of email messages, as email is admissible as evidence in court. • Be aware that misuse of the Trust's email system will lead to disciplinary action and is strictly prohibited. In addition some types of use may attract criminal liability or breach of an agreed contract. • If sensitive information is received by the wrong recipient, whether internal to the Trust or not, it is reported via the Trust's Incident Reporting System as an information security incident and will be investigated. • Ensure that the content of the mailbox is managed appropriately so that it does not exceed the size provided, see Email Procedure for more details.
Managers	• Report all breaches, near misses or suspected breaches of this policy in line with the Trust's incident reporting process. • Inform the service desk of starters and leavers within the department
System Owner	• Produce all required system specific policies, procedures and guidance documentation • Carry out audits on the system

The Chief Executive	• The Chief Executive is ultimately responsible for ensuring the Trust complies with this policy

4 Policy

4.1 Acceptable Use

- Use email as a business communication tool in a responsible, effective and lawful way to support Trust business processes.

- Use associated with professional memberships or bodies, approved academic pursuits; trade union, industrial and staff relation activities; initiatives by the Trust.

- Do not automatically assume that the responsibility for an action has been passed to someone by sending them an email.

- Use an NHSmail account to transfer Person Identifiable Information (PII) or business sensitive information to another secure email account when there is a legitimate business need.

- Use an NHSmail account to transfer PII or business sensitive information to a non-accredited or non-secure email service using the NHSmail encryption feature when there is a legitimate business need.

- Use a signature to convey job title, location and contact details using the default font settings (arial 10, black) and a white background.

- Limit the size of attachments where possible to less than 10Mb

- Send sound or video files only where they related to an approved Trust process.

- Limited personal use, however such use should preferably be restricted to outside or normal working hours and during breaks and should not:

    - Consume Trust resources i.e. consumables such as printer paper and toner.
    - Interfere with staff productivity or system performance
    - Involves cost to the Trust
    - Detrimentally affect the Trust's business interests, reputation or cause loss of goodwill to the Trust
    - Pose any risks to the integrity, security and confidentiality of the Trust's corporate and clinical systems.

- Use web-based email services e.g. Hotmail, Yahoo and Gmail etc. for limited personal use from Trust devices. These types of email services MUST NOT be used for business use.

4.2 Unacceptable Use

- Anything which detrimentally affects the Trust's business interests, reputation or causes loss of goodwill to the Trust.
- Sending PII or business sensitive information to personal or unsecure accounts without using the NHSmail encryption feature (See Email Procedure for more details).
- Sending PII or business sensitive information from an a non NHSmail account
- Sending or forwarding emails containing pornography, libelous, defamatory, offensive, racist or obscene remarks.
- Forging or attempting to forge email messages.
- Altering, misrepresenting, obscuring or suppressing your identity on any communication.
- Sending an email from another users account.
- Accessing the email system using another user's login credentials.
- Posing any risk to the integrity, security and confidentiality of the Trust's corporate or clinical systems.
- Excessive personal use.
- Using the email system to engage in communications that violate the law, Trust policies or the rights of others.
- Replying to the sender of suspicious messages
- Sending messages containing: computer executable files, worms, Trojans or any other types of malicious code
- Sending or circulating spam such as unsolicited email, junk email, joke emails and chain emails.

4.3 Monitoring

The Trust retains the right to access and employee's email messages if it has reasonable grounds to do so. The contents of email will not be accessed or disclosed other than for security purposes, as part of an investigation, or as required by law, by application of the appropriate legal status.

Extended monitoring of individual mailboxes will only occur when there is a legitimate requirement to do so and only for as long as required; for example where there is evidence of email misuse. Staff will not have any indication that mailboxes are being monitored unless informed.

All email will be automatically scanned for viruses, inappropriate content and unauthorised attachment.

5 Definitions

Term	Definition
Email	Messages distributed by electronic means from one computer user to one or more recipients via a computer network:
Email Client	A computer programme that is installed on a personal computer or mobile device and is used to read and send email.
Web Email	Where email is accessed via a web browser rather than an email client.
Web Browser	Software that is used for retrieving, presenting and traversing information resources from the World Wide Web (WWW)
Record	A record (clinical or corporate) is information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transit of business (BS ISO 15489-1)
Personal Identifiable Information (PII)	Is information that can be used to uniquely identify, contract or locate a single person or can be used with other sources to uniquely identify a single individual
Computer Virus	A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made.
Pornography	This can take many forms e.g. textual descriptions, still and moving images, cartoons, sound files. Some pornography is illegal in the UK and some legal. Pornography considered legal in the UK may be illegal elsewhere. Because of the global nature or the internet and email, these issues must be taken into consideration. Therefore the Trust defines pornography as the

	description or depiction of sexual acts or naked people that are designed to be sexually exciting. The Trust will not tolerate it's facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

6 How this policy will be implemented

• This policy will be published on the Trust's intranet and external website.
• Line managers will disseminate this policy to all Trust employees through a line management briefing
• The Policy is referenced in the Trust's network training that all staff must undertake prior to being issued with a network account and email address.
• All line managers will ensure this policy is included in local induction for all email users.

7 How this policy will be audited

The information department will conduct checks on the use of email to ensure compliance with this policy. This will include but is not limited to:

- Checking reports from NHS Net
- Reviewing Anti-Virus Software for malicious code detection
- Use of Proxy servers and filtering software for inappropriate content
- Only granted access to the Trust email system upon completion of the Trust's network training.

The Trust will also employ auditors to regularly review this policy and associated procedures.

8 References

- Our values and behaviours
- Information Security and Risk Policy
- Network Security Policy
- Email Procedure
- Access to Information Systems Policy
- Telephone Usage Policy
- HSCIC Statement of Compliance

9 Document control

Date of approval:	24 July 2019	
Next review date:	31 December 2024	
This document replaces:	Email Policy Ref IT-0006-v5	
Lead:	Name	Title
	Keith I'Anson	Desktop Product Manager
Members of working party:	Name	Title
	Jane Dennis	Technology Development Manager
This document has been agreed and accepted by: (Director)	Name	Title
	Patrick McGahon	Finance and Information Director
This document was approved by:	Name of committee/group	Date
	Digital Transformation and Safety Board	10 July 2019
This document was ratified by:	Name of committee/group	Date
	Executive Management Team	24 July 2019
An equality analysis was completed on this document on:	June 2019	

Change record

Version	Date	Amendment details	Status
V5	4th Aug 15	Put into new format, definitions updated, section on personal use added, statement on smartphones added	
V5	21st Sept 15	Some changes to acceptable use, based on feedback from ISTAAG	
V5	17th November	Spelling checked from ISGG and policy ratified with minor changes	
V5	09/01/2019	Document under review, review date extended to allow review work to be done.	
V6	5/4/2019	Deleted "other than as an account for accessing the Google Play store relating ot Trust Smart Phones" this no longer applies	
V6	19/6/2019	3.2 – hypelink email client to Glossary 3.2 – refrenced email procedure for mailbox management 4.1 removed bullet point "Use email content and	

		speedy response to connvey a professional image and good customer service” 4.2 – linked NHS Mail encryption feature to reference Emal Procedure 4.2 Remove examples of excessive personal use, as covered in 4.1 4.3 – added coment that excesive monitoring will not be known by the user, unless informed.	
V6	24/07/2019	Reference to trust values and behaviours added at request of EMT	Published
V6	Jul 2020	Review date extended 6 months	Published
V6	Jan 2022	Review date extended to 24 July 2023	Published
V6	May 2023	Review date extended to 31 December 2023	Published
V6	May 2024	Review date extended to 31 December 2024	Published

Tees, Esk and Wear Valleys
NHS Foundation Trust

Appendix 1 - Equality Analysis Screening Form

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc.	Information Department					
Name of responsible person and job title	Keith I'Anson – Head of Information Technology					
Name of working party, to include any other individuals, agencies or groups involved in this analysis	Technical Services					
Policy (document/service) name	Email Policy					
Is the area being assessed a…	Policy/Strategy	X	Service/Business plan		Project	
	Procedure/Guidance				Code of practice	
	Other – Please state					
Geographical area covered	Trust wide					
Aims and objectives	The email policy sets out the rules and provides guidance on what the Trust deems as acceptable and unacceptable use of email, including what email system should be used. The Trust's email system is NHS mail – this is a secure national email service which enables the safe and secure exchange of sensitive and personable identifiable (PI) information within the NHS and other local/central government agencies.					
Start date of Equality Analysis Screening	10 June 2019					

End date of Equality Analysis Screening	10 June 2019

You must contact the EDHR team if you identify a negative impact. Please ring Sarah Jay 0191 3336267

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?

   All individuals whose personal information is shared via email.

2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?

Race (including Gypsy and Traveller)	No	**Disability** (includes physical, learning, mental health, sensory and medical disabilities)	No	**Sex** (Men, women and gender neutral etc.)	No
Gender reassignment (Transgender and gender identity)	No	**Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.)	No	**Age** (includes, young people, older people – people of all ages)	No
Religion or Belief (includes faith groups, atheism and philosophical belief's)	No	**Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave)	No	**Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners)	No

Yes – Please describe anticipated negative impact/s

No – Please describe any positive impacts/s

Following this policy will ensure that all users of email do so appropriately and reduce risk to personal information

3. Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.? **If 'No', why not?**	**Yes**	**X**		

Sources of Information may include: • Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc. • Investigation findings • Trust Strategic Direction • Data collection/analysis • National Guidance/Reports		• Staff grievances • Media • Community Consultation/Consultation Groups • Internal Consultation • Research • Other (Please state below)

4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Gender, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership
Yes – Please describe the engagement and involvement that has taken place
The email policy has undergone Trust-wide consultation. Trust staff comprise all protected characteristics.
No – Please describe future plans that you may have to engage and involve people from different groups

5. As part of this equality analysis have any training needs/service needs been identified?					
No					
A training need has been identified for;					
Trust staff	No	Service users	No	Contractors or other outside agencies	No
Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so					
The completed EA has been signed off by: You the Policy owner/manager: Type name: Keith I'Anson				Date: 15/07/2019	
Your reporting (line) manager: Type name: Richard Yaldren				Date: 15/07/2019	
If you need further advice or information on equality analysis, the EDHR team host surgeries to support you in this process, to book on and find out more please call: 0191 3336267/3046					

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	No	Explanation given in equality assessment
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	NA	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
Signature:			