North East Ambulance Service NHS
NHS Foundation Trust

Email Usage Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-12
Version Number	V04
Document Author	IM&T Systems Manager
Lead Executive Director Sponsor	Director of Finance & Resources
Ratifying Committee	Finance Committee
Date Ratified	22 December 2017
Date Policy Effective From	22 December 2017
Next Review Date	22 December 2020
Keywords	NHS mail; NHS.net; Encryption; Internet; Webmail; Hotmail; Gmail Outlook; Exchange; Domain

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
0000.1	All	Initial Draft	Assistant IM&T Manager	Dec 2009
0001.0	All	Final	Assistant IM&T Manager	Dec 2009
0003.1	All	Renamed 'Email and Internet Policy' from 'Email Usage Policy' Full content review under all sections **Note: Version number change as a result of combined policy**	Assistant IM&T Manager / IG Officer (Steven Pratt / Rahima Hoque)	Sep 2011
0003.2	All	After discussion, agreed Email Usage Policy should indeed be separate from Internet Policy	Assistant IM&T Manager / IG Officer (Steven Pratt / Rahima Hoque)	Oct 2011
0003.3	Appendices	Alterations to Appendix A & B	Assistant IM&T Manager / IG Officer (Steven Pratt / Rahima Hoque)	Nov 2011
0003.4	Minor alterations to format and appendices	- Following comments from Policy Review Group: • Formatting changed from 1.5 line spacing to 1. • Trust logo updated • 9 updated • Appendix A only relevant to office based staff. Appendix B includes standard email footer	Assistant IM&T Manager / IG Officer (Steven Pratt / Rahima Hoque)	Nov 2011
0004	All	Final (Ratified by Governance and Risk Committee)	Assistant IM&T Manager / IG Officer (Steven Pratt / Rahima Hoque)	Jan 2012
0004.1	All	Full review of content and transfer of content into new template (2014)	IM&T Systems Manager, Steven Pratt	May 2014
0004.2	All	Modifications made. Appendix B & C removed	IM&T Systems Manager, Steven Pratt	July 2014
0004.2 *(Q-Pulse v.3)*	All	Transferred from old template onto new with a full review of content.	IM&T Systems Manager, Steven Pratt	22nd September 2017

Table of Contents

1. Introduction

Email is used widely by staff within North East Ambulance Service (NEAS). It is important that staff use email professionally and efficiently to maximise benefits to the organisation.

The Trust is legally obliged to ensure all staff are protected against viewing or accessing inappropriate materials. It is mandatory that employees, when communicating by email, adhere to this policy. Failure to follow this policy may lead to disciplinary action being taken.

2. Purpose

The purpose of this document is to present a policy for the acceptable use of email whilst also ensuring that the Trust is not exposed to any additional security risk or threat. It sets out the expectations of domain[1] users for the proper use of its email systems and compliments other Information Governance policies.

3. Scope

This document scope covers the appropriate and effective use of email by:

- Setting out the rules governing the creation, sending, receiving, storing and access of email.
- Promote adherence to current legal requirements and any applicable NHS standard.

The policy applies to all employees, agents and contractors (including sub-contractors), in any capacity, working for or supplying services to the organisation.

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives.

4.2 Chief Executive

The Chief Executive is ultimately responsible for email usage within NEASFT and compliance with the policy is delegated to the Director of Finance and Resources who

[1] Domain Account Policy POL – F – IMT - 5

is also the Senior Information Risk Owner.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is also the Senior Information Risk Officer (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

4.4 Information Asset Owner

The Information Asset Owner (IAO) is responsible for Risk Management of Email Services. The information asset Owner is the Assistant Director of IM&T.

4.5 Information Technology Systems Manager

Has responsibility for:

- Developing, maintaining and implementing this policy
- Monitor email usage and report to managers where breaches are identified as per policy
- Work with line managers and risk management leads in the investigation of potential breaches of this policy
- Report any risks related to email usage to the SIRO and IAO

4.6Line Managers

Have a responsibility to ensure all current, new and temporary staff/users are instructed in their responsibilities in relation to email usage and work in a manner consistent with this policy.

4.6 All Users

All users are personally responsible for ensuring they are aware of and compliant with this policy. By signing up to a Domain Account, users will agree to this policy and its guidelines and should be aware that a breach of this policy may be regarded as serious misconduct which could lead to disciplinary action in accordance with disciplinary procedures. Users should also be aware that email usage will be monitored and any unacceptable usage will be acted upon.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
NHS Mail / NHS Mail 2	The email and directory service specifically designed with an

Term	Description
	aim to meet the needs of NHS staff which allows email to be sent in an encrypted form. This service is accredited to the SCCI 1596 standard. A trust MUST use an email service accredited to this standard
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific key or password
Spam	The use of mailing lists to blanket forum groups or email boxes with indiscriminate, unsolicited messages of promotional (potentially manipulative / corrupt) nature.
SCCI 1596 **(Standardisation Committee for Care Information)**	Information standard. Defines requirements for a secure email service, covering storage and transmission of email, including where email is used for the sharing of 'sensitive' data (including patient identifiable information or PII).
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Article 4 GDPR)
Defamation & libel	A published statement that affects the reputation of a person (person can be an individual or an organisation) and exposes them to hatred, ridicule, contempt, discredited etc. If the statement is not true then it is considered slanderous or libelous.
Harassment	Conduct which is unwanted by the recipient; is considered objectionable by the recipient; causes humiliation, offence or distress. Non-Verbal – offensive literature in an email context.
Pornography	The description or depiction of sexual acts or naked people that are designed to be sexually exciting. NEASFT will not tolerate its facilities being used for this type of material and would consider such behaviour to constitute a serious disciplinary offence.
Copyright	Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the

Term	Description
	work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. The symbol does not have to be displayed under British Law.
GDPR	General Data Protection Regulation. New legal framework (EU) (Data Protection)
Domain	A domain contains a group of computers that can be accessed and administered with a common set of rules.

6. Policy Content

Email is an important means of communicating quickly and easily to support the business needs of the organisation. The email application must be used in accordance with requirements of the Data Protection Act (DPA) 1998, EU General Data Protection Regulation (GDPR) 2016 and Freedom of Information Act (FOIA) 2000. Any email, sent or received, may have to be disclosed in litigation or in an internal or external investigation. Email however can be used inappropriately, either deliberately or otherwise.

The FOIA enables people to have access to much more information held by public bodies than previously. Communications sent via e-mail may relate to decisions made that might have been sent in letters and memos a few years ago. Like their paper counterparts, these e-mail records must be saved, filed and managed in a manner that will allow easy access in future.

E-mail is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Consideration should also be given to the DPA and GDPR.

The following rules are to be strictly adhered to:

- Do not send or forward emails with any libelous, defamatory, offensive, harassing, racist or any discriminatory language homophobic, obscene or pornographic remarks or depictions. If you receive an email of this nature, you must notify your manager and/or report this as an incident.
- Do not forward confidential information without acquiring permission from the sender first.
- Do not knowingly send an email that contains a virus.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's email account.
- Do not knowingly breach copyright or licensing laws when composing or forwarding emails and email attachments.

By following the guidelines in this policy, the e-mail user can minimise the legal risks involved in the use of e-mail. If any user disregards the rules set out in this policy, they may be subject to action by the Trust in accordance with the Trust's Disciplinary Policy.

NHS Mail is only secure when emails are sent between two NHS Mail accounts or between NHS Mail and organisations which are certified as secure. Details of which organisations are certified is available directly from NHS Mail support.

Outside of the approved recipient list all transfers of personal identifiable information MUST be encrypted to the approved standard or sent by secure file transfer. See appendices B & C.

6.1 Access To and Use of Email System

6.1.1 The internal Electronic Mail (email) system (Microsoft Exchange / Outlook) is provided by the NEASFT to support staff in undertaking their duties. The internal email system can be used for all email communications that are not deemed **sensitive**. Access to the external national NHS Mail 2 service is also provided and this service should always be used for **sensitive** email communications. Further information is available in Appendix A through to C.

6.1.2 The Trust has provided email for business purposes. It is recognised that emails are occasionally used for non-work purposes. This should be limited and should only be carried out in your own time whilst remembering that content of any email may be disclosable as part of a subject access request or FOI request. This includes live, archived and deleted emails. The NEASFT reserves the right to monitor and record all email communications sent or received via the Trust's network or computer equipment for violations of this policy, in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and ICO Employment Practices Code.

6.1.3 Email must not be used for personal financial gain or other secondary employment.

6.1.4 Email users may not attempt to make any alterations to the configuration of the email software but a user may customise their own email view and grant proxy rights to other staff. Please contact the IM&T Service Desk for any further advice.

6.2 Key Principles and Standards

6.2.1 Email is a communication tool and not a records management system. Where the content of email or attachments forms part of a record it is the responsibility of the user to ensure it is added to, and becomes part of, that record.

6.2.3 Always consider whether email is the most appropriate means of communicating and whether other forms of communication may be more appropriate. Email is a form of communication it is not designed to replace others.

6.2.4 Any email sent from a personal email account, e.g. john.smith@google.com , containing business information cannot be classified as an official business communication.

6.2.5 Email sent from NEAS must contain a suitable and appropriate disclaimer and statement of confidentiality. At present the disclaimer is sent automatically. Email containing personal views must be clearly labelled as being representative only of the view of the sender, not of NEAS, and is not authorised or sent on behalf of NEAS.

6.2.6 It is the sender's responsibility to ensure sensitive emails are sent via the appropriate medium, and in this case it must be sent via NHS Mail.

6.2.7 Many employees will have private external email accounts that are provided by Internet Service Providers (ISP) which may be accessible via the web, e.g. Hotmail, Gmail etc. under no circumstances must they be used to transfer or forward sensitive Trust information or for the transfer of personal or patient identifiable information. The Trust strictly prohibits the automatic forwarding of any work emails to personal accounts without prior consent.

6.2.8 The Trust does not dictate what types of business communication can or cannot be performed via email, other than the guidance around sensitive content see Appendix A; the Trust does not need to hold email for a defined period of time however backups keep 12 months' worth of data. Staff need to be aware of retention policies and / or legislation that dictate how long any data of a certain category needs to be kept for and then to manage the record in line with the Records Management Policy. Staff are asked to take a decision on appropriateness of sending the detail via email in these circumstances.

6.2.9 Do not use the email facility to send out attachments to a large group of staff. When arranging a meeting only add attachments when it is absolutely necessary. Where information needs to be communicated in this manner please ensure you contact the Communications team who will advise you on how best to disseminate, e.g. the document is posted on the Intranet, Internet and a suitable hyperlink sent to recipients; for meeting requests ensure either your content is included on the meeting request directly or a hyperlink is contained within the meeting request to the document library.

6.3 Out of Office

An "out of office" message must be set up when absent from the Trust for one day or more. If away for a significant period of time (e.g. maternity leave or long-term sick leave) you should contact the IT Service Desk so that your account can be temporarily suspended.

6.4 Delegate Access

Where appropriate, access to a delegate can be admistered by the account holder. However, if it is necessary to check the e-mail accounts of workers in their absence for business continuity purposes, make sure that they are aware that this will happen by seeking consent of the account holder. If this is not possible in an emergency situation, the access should be authorised by the Senior Information Risk Owner (SIRO).

6.5 Access for Investigation Purposes

Further information is provided in the Domain Account Policy.

6.6 Email Classification

All email accounts and email content maintained on the Trust email systems are the property of the Trust. All emails including personal emails are monitored for viruses. All email traffic (incoming and outgoing) is logged. These logs are audited periodically. The content of emails is not routinely monitored. The Trust reserves the right to inspect, monitor and retain message content as required to meet legal, statutory and business obligations.

Further information around classification of categories and examples of such will be made available in 2018 (currently under review).

7. Training Required for Compliance with this Policy

7.1 Microsoft Outlook e-Learning Training

Microsoft Outlook is an email client used to manage mail, calendar and contacts. To learn how to use this application the following e-Learning courses is available:

- Outlook for the Workplace

The content includes:

- Introducing email
- Using email
- Organising messages
- Appointments and meetings
- Using contacts

This course is accessible via the IT Skills Pathway Programme and available via this link, click here.

7.2 Email Best Practice e-Learning Training

To take control of emails, gain 30 minutes per day, cut inbox size by 33%, reduce stress and increase productivity the following course is available:

- Effective Email

The course content includes:

- The medium of email
- Achieving Impact with email
- Critiquing an email
- Subject lines

- Replying and copying
- The hazards of email
- Managing overload
- Email package tools

Please note: there are limited logins available for this course, so it is recommended for frequent email users or those who may have a large mailbox.

This course is accessible via the Oracle Learning Management (OLM) system and available via this link, click here.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

At present compliance relies on staff adhering to policy without the ability to **pro-actively** monitor other than reviews of quarantined email.

Reactive monitoring can occur when IM&T departments are asked to help any incident investigation and that can include someone reporting non-compliance with policy, potentially via whistleblowing for example.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Incident Reporting	Number of incidents involving incorrect email usage (trend)	Action to be assigned to IM&T Service Desk as a result of an official investigation or root cause analysis. When an investigating an incident it may become apparent non-compliance with policy / Reports to IM&T of non-compliance of email / pro-active awareness	Any investigating officer to raise; IM&T Service Desk to examine any record and / or usage information	All incidents raised to be reported to the IGWG (Information Governance Working Group)	When applicable	To be determined as a result of the specific findings from each investigation / incident.
Monitoring and reporting on policy compliance	Number of incidents involving incorrect email usage (trend)	Via Sophos Email Quarantine Monitoring Tool and alerts	IM&T Service Desk / IM&T Systems Manager	All incidents raised to be reported to the IGWG (Information Governance Working Group)	Bi-monthly	Monitor via action plans (IGWG)

10. Consultation and Review of this Policy

The original policy was consulted with members of the Compliance and Risk Committee and the Information Working Group in 2009 with a number of modifications / revisions since, the last being made in 2014.

This policy has been reviewed in consultation with members of the Information Governance Working Group; the Education and Development Officer and members of the IM&T Department.

The policy will be reviewed every three years unless there are significant revisions to be made.

11. Implementation of this Policy

This Policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings and will also be included as part of the effective use of email training.

12. References

This document refers to the following guidance, including national and international standards:

- Data Protection Act 1998
- EU
- Freedom of Information Act 2000
- Computer Misuse Act 1998
- SCCI (Standardisation Committee for Care Information) 1596 Email Compliance
- Copyright Design and Patents Act 1988
- Regulatory of Investigatory Power Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

13. Associated Documentation

Domain Account Policy POL – F – IMT – 5

Internet Policy POL – F – IMT - 9

14. Appendices

Appendix A Sharing Sensitive Information for NHS Mail

Appendix B Encryption Guide for Senders

Appendix C Encryption Guide for Receivers

14.1 Appendix A - Sharing Sensitive Information for NHSMail

Embedded document

sharingsensitiveinformationguide.pdf

Hyperlink to official webpage (note links can change – notify policy holder)

Sharing sensitive information guide for NHSMail

The NHS Mail service is a secure service. NHS Mail is authorised for sending sensitive information, such as clinical data between NHS Mail and:

- NHSmail addresses (i.e. from an '*.nhs.net' or '.hscic.gov.uk' account to an '*.nhs.net' or '.hscic.gov.uk' account)
- Government secure email domains (between *.nhs.net and *.gsi.gov.uk, *.gse.gov.uk and *.gsx.gov.uk)
- Police National Network/Criminal Justice Services secure email domains (between *.nhs.net and *.pnn.police.uk, *.cjsm.net)
- Ministry of Defence secure email domains (*.mod.uk and *.mod.gov.uk).
- Local Government/Social Services secure email domains (*.nhs.net and *.gcsx.gov.uk)

14.2 Appendix B - Encryption Guide for Senders

Embedded Document


encryptionguide.pdf

Hyperlink to official webpage (note links can change – notify policy holder)

Encryption guide for senders

14.3 Appendix C Encryption Guide for Receivers

Embedded document

accessingencrypted emailsguide.pdf

Hyperlink to official webpage (note links can change – notify policy holder)

Encryption guide for recipients