Policy Document Control Page

Title

Title: Electronic Mail Policy

Version: 7

Reference Number: CO6

Keywords:
(please enter tags/words that are associated to this policy)
Email

Supersedes
Supersedes: Version 6
Description of Amendment(s):

- **Updated to add detail around the NHSmail acceptable use policy in relation to personal use by exception and also the local stipulation to remove work contact details if sending in a personal capacity , and New links to NHSMail2 guidance documents.**

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Jenny Spiers

Designation: Information Governance Manager

Equality Impact Assessment (EIA) Process
Equality Relevance Assessment Undertaken by: Jonathan Mayes
ERA undertaken on: 24th February 2012
ERA approved by EIA Work group on: 24th February 2012

Where policy deemed relevant to equality- N/A
EIA undertaken by N/A
EIA undertaken on N/A
EIA approved by EIA work group on N/A

Integrated Governance Group

Referred for approval by: Information Governance Manager

Date of Referral: 1st March 2017

Approved by: Information Governance Assurance Group

Approval Date: 1st March 2017

Date Ratified by Executive Directors: 20th March 2017

Executive Director Lead: Director of Service Development and Sustainability

Circulation

Issue Date: 22nd March 2017

Circulated by: Information Department

Issued to: An e-copy of this policy is sent to all wards and departments

Policy to be uploaded to the Trust's External Website? YES

Review

Review Date: May 2018

Responsibility of: Jenny Spiers

Designation: Information Governance Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 22nd March 2017

Contents

1. INTRODUCTION

1.1 This document defines the Email policy for Pennine Care NHS Foundation Trust and:

- Sets out the Trust policy for the protection of the confidentiality, integrity and availability of the email system.
- Establishes organisational and user responsibilities for the email system.
- Provides reference to guidance relevant to this policy.

1.2 The NHS mail service has been provided to aid the provision of health and social care and this should be the main use of the service.

1.3 The Trust utilises the NHSmail service provided through the Health and Social Care Information Centre.

1.4 Compliance with Trust policies is a condition of employment and breach of a policy may result in disciplinary action.

2. OBJECTIVE

2.1 The objective of this policy is to explain to users of the NHS mail service, accessed via the Trust network, how the service should be used.

2.2 The purpose is to ensure the proper use of the Trust's email system and make users aware of what the Trust deems as acceptable and unacceptable use of its email system.

3. SCOPE

3.1 This policy applies to all users accessing the NHSmail service via the Trust network.

3.2 This policy applies to all information sent or received via the NHSmail service via the Trust network.

4. LEGAL RISKS

4.1 Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature, email seems to be less formal than other written communication, the same laws apply. Misuse of email may contravene one or more of the following:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Law of Copyright
- The Electronic Communications Act 2000

Therefore, it is important that users are aware of the legal risks of email.

4.2 If you send or forward emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the Trust can be held liable.

4.3 If you unlawfully forward confidential information, you and the Trust can be held liable.

4.4 If you send an attachment that contains a virus, you and the Trust can be held liable.

5. USER RESPONSIBILITIES

Users **must not**:

5.1 use the NHSmail service to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is usually grounds for 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, terrorism, incitement to racial harassment, stalking and sexual harassment and treason. Use of the service for illegal activity will result in the immediate suspension of the user's NHSmail account.

5.2 use NHSmail accounts for regular personal use. A personal email account should be set up with an internet provider (see Section 19 for further guidance on personal use).

All communication you send through the NHSmail service is assumed to be official correspondence from you acting in your official capacity on behalf of the organisation. Should you need to, by exception, send a communication of a personal nature you must clearly state in the subject field that your message is a personal message and not sent in your official capacity and remove any details from your email signature i.e. job title, work location and contact details.

5.3 use the NHSmail service for commercial gain.

5.4 use the NHSmail service to disable or overload any computer system or network.

5.5 use the NHSmail service to harass other users or groups.

5.6 attempt to interfere with technical components, both hardware and software, of the NHSmail system in any way.

5.7 attempt to disguise your identity or your sending address.

5.8 send any material by email that could cause distress or offence to another user.

5.9 forward frivolous material e.g. chain emails, or use 'reply all' when informing the sender that they feel an email was not meant for themselves.

Users **must:**

5.10 When a user sets up an NHSmail account, they must identify themselves honestly, accurately and completely.

5.11 E-mail is to be used for the purposes of the organisation to enable information to be passed across the organisation or from one organisation to another. E-mail should be viewed with the same status as any letter or memorandum and must meet the standards of business etiquette.

5.12 Sign off with your name, organisation and telephone number (see Section 7).

5.13 Use the subject field with a few short descriptive words to indicate the contents when sending e-mails. This will assist the recipient in prioritising and aids future retrieval. Confidential identifiable information should not be used in the subject field

5.14 Type your message in lower case. Using capital letters can be considered aggressive.

5.15 Be careful about the content - make sure it adheres to this policy.

5.16 Maintain the conventions normally used in sending a letter by post. If you usually address someone as “Dr Smith”, do the same in e-mail. E-mail carries the same etiquette as traditional communication and also the authority of the sender.

5.17 Users must ensure that their password and answers to their security questions for the NHSmail system are kept confidential and secure at all times. Users should immediately notify the ICT Helpdesk on 0161 716 1234 or ICTServiceDesk.PennineCare@nhs.net if they become aware of any unauthorised access to their NHSmail account.

5.18 Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus software although occasionally, as with any email service, a new virus may not be immediately detected. If a user is unsure of the source of an email or attachment it should be left unopened and the ICT Service desk informed.

5.19 Users must familiarise themselves with the NHSmail guidance pages which include important policy guidelines, information about known issues with the service and user/administration guides. These are all available within NHSmail:

https://web.nhs.net/public/?a=s

5.20 It is possible for email to be read and sent (in the user’s name) from an unattended PC. It is the responsibility of the user to ensure that, when leaving their PC unattended, they either:

- Shut down the PC; or

- Use the “lock computer” utility by pressing control, alt, delete together and then clicking on Lock computer.

6. SENDING EMAILS

6.1 It is the user’s responsibility to check that they are sending email to the right recipient, as there may be more than one person with the same name or a similar name using the service. 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. Where the intended recipient does not have an NHSmail account, their email address can be verified by contacting them directly or the organisation they work for via the phone.

6.2 No confidential or person identifiable information should routinely be sent from an NHSmail account to an unsecure account (this includes all commercially available emails such as Hotmail and yahoo, and some public and private sector organisation email addresses (see section 8.4)) (refer to section 8 for further details)

6.3 All outgoing email will automatically contain an appended disclaimer stating the following:

> This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful.
> Thank you for your co-operation.
>
> NHSmail is the secure email and directory service available for all NHS staff in England and Scotland
> NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and GSi recipients. NHSmail provides an email address for your career in the NHS and can be accessed anywhere

7. EMAIL SIGNATURES

7.1 Providing your contact details within an email will help to ensure that individuals are aware of your most up to date contact details. NHSmail has a facility that enables a ‘signature’ to be automatically applied to each email. The following layout should be adopted:

Your Name
Your Job Title
Pennine Care NHS Foundation Trust
Your work location and address
Telephone no.
Mobile no. (if applicable)
Email: e.g. your.name@nhs.net
Fax no.
Web: **www.penninecare.nhs.uk**

7.2 The sign off is in Arial 10 point, and laid out as shown in the example below:

Jenny Spiers
Information Governance Manager
Pennine Care NHS Foundation Trust
225 Old Street
Ashton-under-Lyne OL6 7SR
Telephone: 0161 716 3145
Mobile: 07826 531949
Email: jenny.spiers@nhs.net
Fax: 0161 716 3389
Website: **www.penninecare.nhs.uk**

7.3 Within NHSmail, you can set up your signature by clicking on options, scroll down to Email signatures, type in your email address using the above format, tick the box 'Automatically include on outgoing messages' then click save.

7.4 Within Microsoft Outlook (2003), you can set up your signature by clicking on tools, options, mail format, signatures, new, give a name to your signature e.g. formal or informal, next, type in your email address using the above format (you can change the font etc.), click on finish, ok, select the signature for new messages and replies then click on ok.

7.5 Within Microsoft Outlook (2010), you can set up your signature by clicking on New E-mail, then go to 'Signature', click on the down arrow to 'Signatures' and type in your contact details.

Nb. You may need to set up your signature again if you access a different pc.

7.6 **GENERIC EMAIL ACCOUNTS:** Advice should be sought from the Information Governance Department regarding the use of Generic Email Accounts.

8. SHARING SENSITIVE/PATIENT IDENTIFIABLE INFORMATION BY EMAIL

8.1 **No** unencrypted personal confidential data should be transferred by email unless there is a legal and justifiable purpose for doing so, appropriate authority, and the sending and receiving email addresses are secure, sa described in the following paragraphs.

8.2 NHSmail (*.nhs.net)

NHSmail is a secure national email service which enables the safe and secure exchange of sensitive and patient identifiable information within the NHS and with local/central government.

8.3 Across the NHS

Between NHSmail addresses:

.nhs.net to .nhs.net is secure

.nhs.net to nhs.uk is not secure

8.4 Using NHSmail to email central and local government

Email sent to the communities below will be securely routed by NHSmail over the Government Secure Intranet Convergence Framework (GCF) if it is sent to one of the formally accredited secure email services listed below. Content does not need to be encrypted.

Secure email domains in Central Government

Between .nhs.net and

- .gsi.gov.uk
- .gse.gov.uk
- .gsx.gov.uk

Nb. An email that ends just in .gov.uk is not secure. You will need to contact the person and ask if they have a .gsi.gov.uk, gse.gov.uk or gsx.gov.uk for it to be a secure address.

Secure email domains in the Ministry of Defence

Between .nhs.net and

- .mod.uk

The Police National Network/Criminal Justice Services secure email domains

Between .nhs.net and

- .pnn.police.uk
- .scn.gov.uk
- .cjsm.net

Secure email domains in Local Government/Social Services

Between .nhs.net and .gcsx.gov.uk

If the intended recipient does not have a secure email account with one of the above domains, the new nhsmail encryption can be used (see 9.5 below)

The latest guidance for using NHS mail and secure addresses can be accessed via clicking on the following Link:

https://portal.nhs.net/Help/policyandguidance

Please Note: The list is reviewed and updated as changes occur and staff should regularly refer back to the NHSmail portal to ensure their lists remain accurate. The Information Governance Team will provide updates via the monthly IG Bulletins as and when required.

8.5 New NHSmail encryption feature

The new encryption feature does not change the way you send e-mails to the secure e-mail addresses above and staff should always check if there is a secure email address to send personal/sensitive information to before using the guidance below.

However, you can now send secure e-mails from NHS Mail (nhs.net) to insecure e-mail service domains. (e.g. gov.uk, nhs.uk, Hotmail, googlemail, etc.).

If you have a contact that uses an insecure email and you need to exchange personal/sensitive information you need to send an initial encrypted email that they can open, read and reply to securely. Full instructions can be found in the document available via:

visiting www.nhs.net, select '*Get help*' then select '*Policy and guidance' then 'sharing sensitive information guidance' then ' Accessing Encrypted Email'.*

The following steps must be followed to send encrypted emails to insecure domains:

- Send recipient the 'Encryption Guidance for Recipients', document which can be found at the link below:

visiting www.nhs.net, select '*Get help*' then select '*Policy and guidance' then 'sharing sensitive information guidance' then 'Encryption Guide'.*

- Send an initial encrypted email to recipient but do not include any sensitive/personal information (follow steps below). Once the recipient has registered for the encryption service and confirmed to the sender that this has been done (by responding to your initial email), personal/sensitive information can be sent in an email or as an attachment to this contact. Registration only needs to be carried out once for each recipient – subsequent emails are much easier for them to access.

To send an encrypted email:

- Create a new mail message in the normal way
- Ensure the recipient's email address is correct
- In the subject field, enter the word **[secure]**, before the subject of the message. The word **[secure]** must be surrounded by square brackets for the message to be encrypted. **If the square brackets are not used, your message will not be encrypted and will be recorded as an incident and treated as a confidentiality breach. [secure] is not case sensitive so [secure] or [SECURE] can be used.**
- Compose the message, adding any attachments

- Click to send the message. An unencrypted copy will be saved to your **Sent items** folder

The full guidance for using the new NHSmail encryption feature can be accessed by visiting www.nhs.net, select '*Get help*' then select '*Policy and guidance' then 'sharing sensitive information guidance'.* There is a link within this section.

8.6 You must always use the following guidelines when sending sensitive information:

- You should make sure that any exchange of sensitive information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated

- Caldicott principles should apply whenever sensitive information is exchanged i.e.

1. Justify the purpose(s) of using confidential information.
2. Do not use patient-identifiable information unless it is absolutely necessary.
3. Use the minimum necessary patient-identifiable information that is required.
4. Access to patient-identifiable information should be on a strict need-to-know basis.
5. Everyone with access to patient-identifiable information should be aware of their responsibilities.
6. Understand and comply with the law.
7. The duty to share information <u>can be</u> as important as the duty to Protect patient confidentiality

8.7 Caldicott Guardians are senior staff in the NHS and social services appointed to protect patient information. The Caldicott Guardian for the Trust is the Medical Director.

- As with printed information, care should be taken that sensitive information is not left anywhere that it can be accessed by other people e.g. on a public computer without password protection.

- When you are sending sensitive information, you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time sensitive information such as referrals.

- You must not hold patient identifiable data in your calendar if your calendar may be accessed by other people who are not involved in the care of that patient.

- If patient identifiable information is visible to other people, it is your responsibility to ensure that those people have a valid relationship with the patient.

- You must always be sure that you have the correct contact details for the person (group) that you are sending the information to. If in doubt, you should check the contact details in the NHS Directory or by telephone.

- If it is likely that you may be sent patient and/or sensitive information, you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected. Unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

9. EMAILS SENT / RECEIVED IN ERROR

9.1 If you receive an incorrectly addressed email, you should return it to the sender immediately, unless it contains confidential information, in which case you should remove this information before returning it.

9.2 Where the confidential information relates to the personal information of a client or staff member of the Trust, you must complete an incident form.

9.3 Where the email reasonably appears to be spam, it should be deleted without being opened or forwarded.

10. USE OF THE 'OUT OF OFFICE' ASSISTANT

10.1 Use the Out of Office Assistant whenever you are unable to respond to e-mail for an extended time.

10.2 Within NHSmail to access the Out of Office Assistant click on options, then out of office assistant on the left-hand panel.

10.3 Within Microsoft Outlook (2003), click on tools, Out of Office Assistant, type in the 'Auto reply only once to each sender with the following text' box the message you require to be seen. Click on 'I am currently out of the office' if you require the message to be seen with immediate effect.

10.4 Within Microsoft Outlook (2010), click on File in the top left and then click on the box headed 'Automatic Replies (Out of Office)'

11. LOGGING ON TO NHSMAIL ON A PUBLIC COMPUTER

11.1 One of the key advantages of NHSmail is the ability to access your email wherever you are. However, if you access your NHSmail from a public computer, it is essential you take certain precautions in order to safeguard your login details and the sensitive data in your NHSmail mailbox.

- Make sure no one watches you type your username and password when you log in; and

- Never select an option that allows you to save your password for later use. Always type your password, even if you plan to use the same computer for several days

- If you are logging onto NHSMail via a smartphone or similar device, ensure you are familiar with how your phone handles NHSmail, for example ensuring that if you open an attachment, the attachment isn't downloaded onto your device. If this does happen, you should find and delete the download as soon as you have finished your session on the email.

11.2 Guidelines for opening an attachment

Follow these guidelines when you open an attachment:

- Open attachments only from people you know and trust.

- If you are using a public computer, click the **Open as Web Page** link next to the attachment name. This protects you from potential virus attacks and prevents a copy of the attachment from being created and stored in the temporary files on the computer.

- If you want to open an attachment directly rather than as a Web page, save it to a secure folder or a location that you can easily find and then open it from that location. It is not possible to open an attachment directly if you are using a public computer. Do not save documents to computer hard drives (usually known as C drives), particular when you are using non Trust issued equipment.

12. LEGAL ADMISSIBILITY

12.1 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 Freedom of Information Act 2000 (contact the Trust Information Governance Team for more information about the FOI Act). Emails should be treated like any other communication and care should be taken to ensure that content is accurate and the tone is appropriate.

12.2 Emails may also be requested as part of a Subject Access Request. Subject to Data Protection rules regarding disclosure, we cannot refuse to release emails on the basis that we don't think what was said in them was appropriate. If it's recorded, it has to be considered for disclosure.

13. THE NHS DIRECTORY

13.1 It is the user's responsibility to make sure their details in the NHS Directory are correct and up to date.

13.2 A user must not use the NHS Directory to identify individuals or groups of individuals to target for commercial gain, either on the user's behalf or that of a third party.

14. COMMUNICATING WITH CLIENTS/CARERS/RELATIVES VIA EMAIL

14.1 On occasion, it may be appropriate to communicate with clients or relatives/carers via email as this may be the preferred method that is agreed between the two parties i.e. clinician/staff member and patient/relative. This should be via a team email account rather than to an individual staff member.

14.2 If a request to communicate via email is received and the recipient of that request does not consider it is an appropriate method of communication, the reason behind that decision must be shared with the person making the request. There is no obligation on any member of staff to communicate with clients or carers/relatives via email. However, Trust staff must ensure there is an alternative method to allow appropriate communication to take place.

14.3 Communication via email to clients or carers/relatives will not usually be secure, unless using the new NHSmail encryption feature, the person with whom you are communicating with should be advised of this process and agree that email communication can continue or whether they would prefer to be contacted by mail/telephone.

14.4 When communicating with relatives/carers, explicit consent of the client must be in place (see the Confidentiality Policy (CO04) and Information Sharing Policy (CO13) for further advice on consent).

14.5 The Information Governance Team MUST be consulted before email correspondence of this nature takes place. The IG Team will provide an appropriate clause as part of the consent process.

14.6 Any correspondence communicated by email should follow the same rules as with any other format i.e. verbal/letter, in terms of the use of appropriate content and language. The communication should be printed and retained in the appropriate record or filed electronically.

14.7 Procedures must be put in place to ensure that, where the communication via email has been agreed, during periods of staff absence, there is an appropriate method of ensuring that emails are not left unanswered. This may be via the use of a team email account rather than to a named member of staff.

15. GLOBAL EMAILS

15.1 High priority corporate messages/briefings to all Trust staff

Only critical or high priority messages will be circulated by global email to all staff.

15.2 Borough-wide or service-wide messages
Staff are encouraged to develop their own local email distribution lists so that emails can be more accurately targeted. The ICT Department will be able to offer support on setting up these lists, where required and has created borough-wide and service-wide email distribution lists. However, these lists will only be made available to designated staff.

15.3 Non-urgent messages that are relevant to all staff
For any non-urgent messages to all staff, the relevant template should be completed (appropriately approved) and returned to the Communications Department. Messages will be uploaded to the 'Announcements' area of the intranet within around two working days.

15.4 Use of BCC
There are 2 ways to copy other users into an email; you can use **CC (carbon copy)** and **BCC (blind carbon copy). CC** allows all recipients of the email to see other email addresses. IF you want to copy other users in privately use the **BCC** field. Any recipients on the BCC line of an email are not visible to others on the email.

For security and privacy reasons it is best to use the BCC feature when sending an email message to a large number of people. When you place email addresses in the BCC field of a message those addresses are invisible to the recipients of the email.

16. MANAGEMENT/RETENTION OF EMAIL MESSAGES AS A RECORD

16.1 To manage email messages appropriately, members of staff need to identify email messages that are records of their business activities as opposed to routine email messages. Emails regarding clients should be printed and filed in the health record if a paper record is in use.

16.2 It is important that email messages and their attachments which are records are moved from personal mailboxes and managed with and in the same way as other records. They should be saved to the relevant folder in the shared drive unless the information is in draft or is confidential, in which case staff should save it in their personal area on a network drive.

16.3 All email sub-folders count towards the amount of space you are taking up, not just the mail in your inbox. It is good practice to regularly check the size of your mailbox. Look at the folders that are taking up the most space and decide whether you really need to keep all the messages in them.

- Remember that you have primary responsibility for the emails you generate.

- Emails are another form of a 'record' and are, therefore, subject to Records Management legislation and local policy i.e. the Records Management Policy (CO20).

- You must never delete email (or any other type of record) if you know it is subject to a Freedom of Information Act or Data Protection Act request that has been received by the Trust. This act would constitute not only Trust policy breach but also breaking the law.

17. MONITORING AND DISCLOSURE OF EMAIL

17.1 As outlined in the Regulation of Investigatory Powers Act (RIPA), the Trust reserves the right to access and disclose the contents of electronic communications without the explicit consent of the user (only to the extent that it will not contradict relevant clauses in the Human Rights Act). The Trust will do so when it believes it has a legitimate business need and only after explicit authorisation from an Executive Director.

17.2 Reasons for monitoring and disclosure may include but are not limited to:

- Provide evidence of sales orders, invoices or other business communications.

- Absence (e.g. due to sickness, holiday or business commitment) where there is a need to access messages in order to carry out the normal functions of the Trust.

- To further an investigation triggered by indications of misconduct or unauthorised use: or, upon production of evidence, to ascertain whether the law has been broken

17.3 You should have no expectation of privacy for any personal email that you send or receive via the NHSmail service.

18. PERMITTED USE OF THE TRUST INTERNET FOR PERSONAL EMAIL USE

18.1 Use of the Trust internet is permitted to enable users to send personal emails provided that the user sets up their own personal account with an internet provider. Use must not be detrimental to the individual's job responsibilities, be in their own time and not stop other staff members using Trust equipment to carry out their duties. The same procedures and restrictions apply as outlined within this policy.

18.2 The Trust can accept no responsibility for any matter arising out of personal use of email and cannot offer support for any problems encountered.

18.3 Users who give out home phone numbers, addresses, credit card numbers, financial or other confidential information do so at their own risk.

18.4 Personal use of Trust equipment does not extend to the printing of large documents. The cost of consumables is expected to be borne by the user.

19. REPORTING AND MONITORING MISUSE OF EMAIL

Any misuse of the email system or violations of this policy must be notified to the user's line manager and/or the Trust ICT Director immediately. The Trust may, with reasonable suspicion of Policy breach occurring, initiate monitoring of staff email usage and accounts.

20. TRAINING

20.1 Ad-hoc training may be available from the Information Governance team on request.

21. REPORTING

21.1 Compliance reports with this policy will be monitored by the Information Asset Managers, Owners and Administrators.

22. POLICY REVIEW

22.1 This policy will be reviewed every two years by the Information Governance Manager (or sooner if new guidance or national standards are to be introduced).