Essex Partnership University
NHS Foundation Trust

NHSMAIL USAGE PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG50H
VERSION NUMBER	1
REPLACES SEPT DOCUMENT	CPG50F
AUTHOR	Associate Director IT Business Operations
CONSULTATION GROUPS	IGSSC
IMPLEMENTATION DATE	November 2018
AMENDMENT DATE(S)	
LAST REVIEW DATE	
NEXT REVIEW DATE	November 2021
APPROVAL BY IGSSC	19/11/18
RATIFICATION BY	N/A
COPYRIGHT	

PROCEDURE SUMMARY

These procedural guidelines will ensure that the risk associated with not having a procedural document in relation to information governance / security in regard of NHS Mail use is minimised and that there is a co-ordinated approach to its safe use.

This procedure should be read in conjunction with the Trust's Email / Internet / Intranet Usage Procedure

The Trust monitors the implementation of and compliance with this procedure in the following ways;

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this procedure is Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

NHSMAIL USAGE PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

NHSMAIL USAGE PROCEDURE

Assurance Statement

Staff working for EPUT will ensure that they comply with the requirements of the General Data Protection Act 2018 Regulation and safeguard the confidentiality of any personal information which is held.

These procedural guidelines will ensure that the risk associated with not having a procedural document in relation to information governance / security in regard of NHS Mail use is minimised and that there is a co-ordinated approach to its safe use.

This procedure should be read in conjunction with the Trust's Email / Internet / Intranet Usage Procedure

1.0 INTRODUCTION

1.1 NHSmail is a secure national email service which enables the safe and secure exchange of sensitive and person identifiable information for all email exchanges between other healthcare professionals using the nationally hosted NHS Mail service.

1.2 NHSmail can be used to send sensitive/person identifiable information using the secure send feature of NHS Mail to any other email system, details on how to do this are available in this document

1.3 This document identifies EPUT's expectation for the use of NHS Mail.

2.0 ACCESSING NHS MAIL

2.1 Staff can access NHSmail using:-

- A Trust issued device using Outlook
- The web-based interface (https://portal.nhs.net)
- Trust issued smartphone/tablet enabled with the trust mobile device management system (Airwatch)

2.2 Accessing email using non-Trust equipment at non-Trust location.

- Access NHSmail via the web based interface (https://portal.nhs.net). Do not use any other software to view this site.
- Select the default option of public or shared computer. The public computer option prevents you downloading information to a non-NHS device. You can view an attachment as a web page unless the document is password protected.

- Do not select private computer. Although you may be using your personal computer in your home, there is the potential for other members of your household to access or an external source with access to your networks.
- Staff must refer to records management guidance when exporting patient information from email.
- Remember the Trust's Code of Confidentiality - think about the sensitivity of what you view and who can see the screen.

2.3 You must not configure your personal mobile device to access NHSmail via any other means other than the web portal (https://portal.nhs.net)

- Some devices do not have built-in encryption at rest capability. Password/PIN does not guarantee a device has built-in encryption.

- Mobile devices keep a copy of emails on the device itself and the security of this data cannot be guaranteed and as a result is a breach of the trust IT security policy.

3.0 USE OF NHSMAIL

3.1 When sending emails be aware that:-

- When sending an email to a recipient for the first time, always select them from the Essex Partnership NHS Foundation Trust address book and not the global address list. (Recipients outside of NHSMail will not appear in the address book and will need to be entered manually, the first time) The chance of there being another person with the same name **is likely** within NHSmail and could result in confidential / sensitive information being sent to the wrong person. Wherever possible contact recipient by phone and confirm address for the first time.

- All staff must provide their security questions and answers via the https://portal.nhs.net portal in the event of the mailbox password being forgotten. The IT helpdesk can reset passwords but this will only be done if the user has already tied to reset/change their password themselves via the self-service option.

- A mobile phone number must be provided in support of the secret questions for this function to work, if this is a personal mobile, it can be hidden from the address book.

- If sensitive information is received by the wrong recipient whether internal to the Trust or not, it is reportable via Datix as an information security incident and will be investigated.

- Do not include person identifiable information in the subject line of your email.

- Only include person identifiable information in the body of the email if you are confident that the recipient is entitled to see it and that the information can be shared with them.

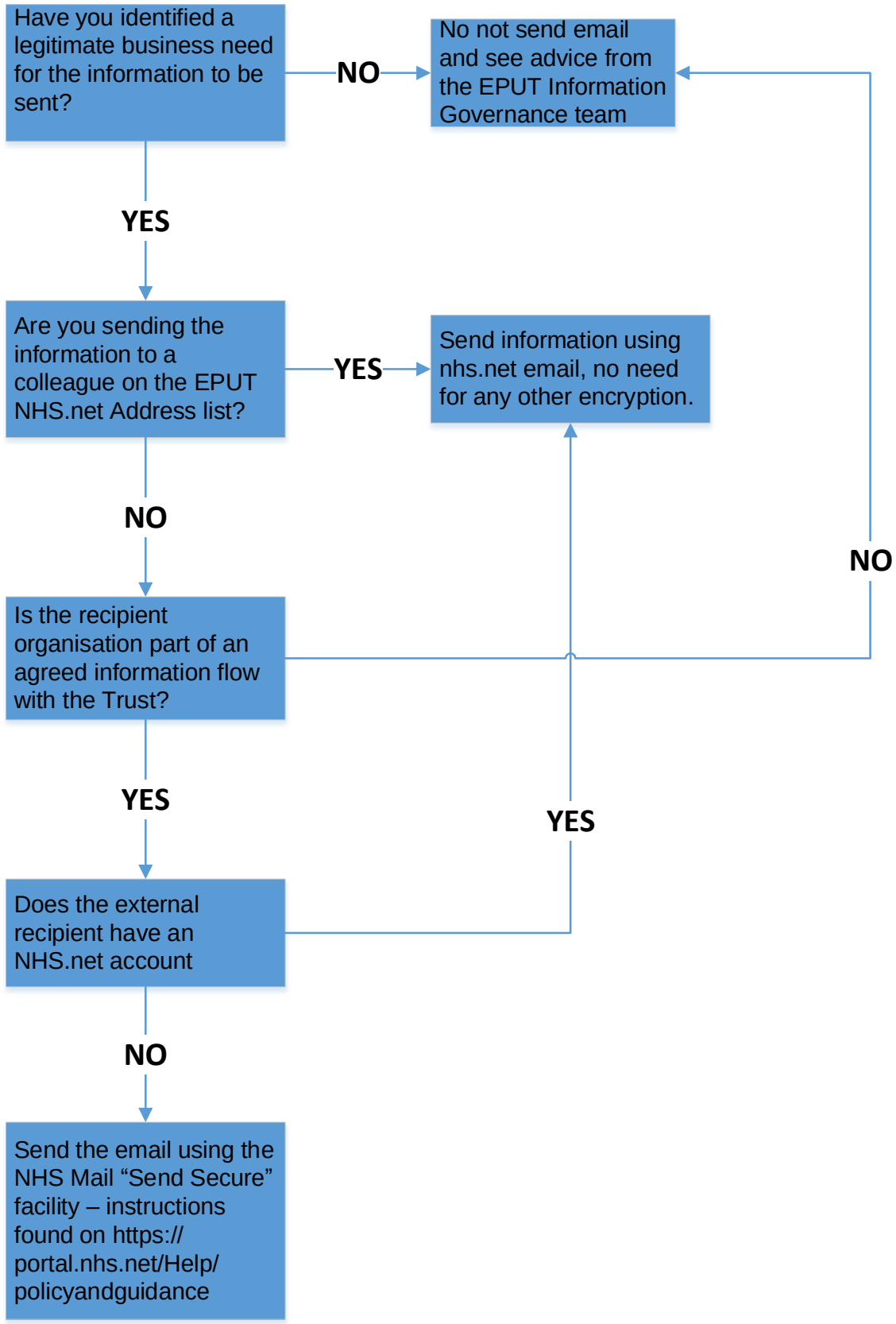
.

Important points to remember:-

- Emails can be disclosed to the public in response to a Freedom of Information, Subject Access or Environmental Information Regulations Request. Do not write anything in an email that could not be written in a letter or spoken face to face. Do not write anything defamatory about an individual or the organisation.
- Before sending your email, check: -
    - your spelling (ensure you enable spell check if not already enabled)
    - the content is clear and correct;
    - the layout is consistent.
    - Do not assume that people read their email every day. Urgent messages are best communicated by phone in the first instance, and only sent by email as a backup.
    - Be selective - only send the email to those who really need it.

3.3 Before sending any personal identifiable information, please follow the steps on the following page and take the action identified.

Sending sensitive information workflow:



Important points to remember:-

- Information sharing agreements are published on the intranet in the Information Governance section. Information Sharing Agreements set out a legitimate reason for information to be shared with external organisations/third parties which staff within the trust are able to view.
- Consider who has access to the mailbox. Recipients may have assigned delegates who can read emails on their behalf.
- NHSmail is an encrypted service. You do not need to encrypt attachments when sending to another NHSmail mailbox. Emails will not be encrypted if they are forwarded onto another account which is not recognised as secure.
- If communication will be routine as part of an information sharing agreement, and the recipient does not have a secure email address, consider asking the ITT Service Desk to investigate creating a 3rd Party NHSmail account.
- Check the email address is accurate and secure before you send person identifiable information.

3.4 **Distribution lists**

- ***Important points to remember:-***

- Set the default address book to EPUT, this will allow internal staff to be easily found.
- Distribution lists enable you to send one email to many people without needing to select each individual.
- Staff who have left the Trust may continue to use their NHS mail address. Owners of distribution lists should review your distribution lists regularly to ensure that members who have left the Trust do not continue to receive Trust data.
- Use distribution lists with care so that information is only communicated to those people with a need to know.
- Global communication (All Staff) should only be sent by the trust Coms department.
- There must be a business need for non-Trust individuals to be included in your distribution list.
- Distribution lists are the responsibility of the owner and therefore it is the owner's responsibility to add/remove members.

3.5 **Receiving emails**

- ***Important points to remember:-***

- Process or action your emails as soon as possible.
- Set a reminder to yourself by marking items "urgent" or "flagged" for follow up.
- Do not print emails unless absolutely necessary.
- Once you have actioned an email, either delete or file it. See **Mailbox Management**.
- Keep the number of emails in your Inbox to a minimum.
- Make sure deleted items really are deleted by emptying the Deleted Items folder.
- Manage any attachments you receive by either:

- filing the whole email (including attachments) in your email file system.
- saving either the whole email or the attachment separately on the network.

3.6 **Replying and forwarding emails**

- ***Important points to remember:-***

- Only reply to or forward emails when necessary.
- Be careful when using the "Reply to all" facility – consider who will see your reply.
- Attachments are automatically removed when you use "Reply" and included when you use "Forward".

3.7 **Using the calendar**

- ***Important points to remember:-***

- Staff who have left the Trust may continue to use their NHS mail address. Review access to your calendar regularly to ensure that it is restricted to Trust staff.
- Your calendar must not contain any patient or personal identifiable information unless authorised by the Information Governance Team to ensure person/patient confidentiality is maintained.
- Documents embedded in your calendar are viewable by all staff with access to your calendar.
- Hyperlinks will not work if using NHSmail via a non-Trust network.

4.0 MAILBOX MANAGEMENT

4.1 All emails generated in the course of NHS activity are Public Records. They are subject to the same legislation and operational requirements of any other Public Record. It is your responsibility to manage your email messages appropriately
The Trust endorses the use of SMS to communicate with service users provided this is for simple communications such as appointment reminders and provided strict Trust protocol (outlined below) is followed when sending messages.

4.2 Attachments – sending and saving **Important points to remember:-**

- NHS mail is provided for the secure exchange of information and not for long term information storage.
- **Review** your inbox and sent items regularly.
- **Save** attachments that you need to keep on your **shared drive**.
- **Save** corporate records on the network (shared drive) following Corporate Records Management Guidance.
- **Save** patient related information in the patients' record as per the Records Management Guidance.
- **Send a hyperlink** instead of an attachment if the recipient has access to the location where the document is saved.

- If sending an attachment that is saved on your shared drive, **remove** the attachment from your email in the **sent items** folder. Otherwise you are doubling the space needed to store any document you have created and emailed

4.3 **Mailbox limits**

- ***Important points to remember:-***

- Your mailbox has a standard maximum size limit of 4 GB (see Appendix 1 – NHS mailbox quotas).
- **All** email sub-folders **and** calendar items count towards the amount of space used in your mailbox - not just the mail in your Inbox. Look at the folders that are taking up the most space and decide whether you really need to keep all the messages in them.
- The maximum size of attachments is 20MB.
- You will receive a warning when your mailbox is nearing its size limit.
- If your mailbox reaches its size limit, you will be unable to send and receive email until you have removed a sufficient number of messages from your mailbox. You are responsible for ensuring that your mailbox is able to send and receive information.
- If your mailbox is dormant for a period of time (6 months) then your account will be closed and you will need to log back into your account to reactivate it.
- Emails in your account maybe deleted by the NHSmail system after 4 months of account inactivity. This is not controlled by the Trust therefore filing emails is important to ensure Trust information is not lost.
- It is worth noting that the newly implemented Mailsafe system is now the Trust's email archive tool that will archive email over 90 days old and will assist in managing the user's mailbox size.
- In exceptional circumstances, mailbox size limits can be extended but this should only be considered if the user's mailbox exceeds the standard 4 GB due to the user being responsible for large mail volumes/attachments that will regularly cause 3 months' worth of email to reach the limit. This option should not be used as a substitute for mailbox management and housekeeping.
- To request an increase in mailbox size, the following criteria must be met:
    - Justification for why standard mailbox management has been unsuccessful
    - Explanation of the role of the user that constitutes an above average volume of mail/attachments.
    - Written approval by the Executive Director to support the above claims sent in via the Service desk self-service portal
- Mailbox extensions can only be undertaken by a member of the trust IT Department and only on the authorisation from a senior IT manager. A check will be made to identify if the mailbox limit has been reached or is 95% full (under 200mb of the 4 GB limit) and that all other attempts to reduce the size of the mailbox have been exhausted.

4.4 **Shared mailboxes**

- Shared mailboxes have an owner nominated to them who is responsible for managing that mailbox and allocating delegated access where necessary.

4.5 **Deleting unwanted emails**

- Deleting an email from your “Inbox” or “Sent Items” will move it to the “Deleted Items”. The email will not be permanently deleted until you delete it from “Deleted Items”, or you have set your “Deleted Items” to empty automatically.

5.0 ACCOUNT MANAGEMENT

5.1 **New accounts**

- New accounts are requested through the ITT service desk once approved by your line manager.

5.2 **Transferring an account from a different organisation**

- You can transfer an existing NHSmail account from a different organisation. You must ask your previous organisation to mark you as a “leaver”. Only when this has been completed can the ITT service desk mark you as a “joiner” to the EPUT directory.

5.3 **Closed accounts**

- Your line manager must follow the leavers’ process and inform the ITT service desk when a staff member leaves the organisation. You **must** clear your mailbox of all Trust information prior to transferring to a new NHS organisation.

5.4 **Passwords**

- ***Important points to remember:-***

- Your NHSmail account must have a unique password which you **must not share**; the password must adhere to the EPUT Password Policy.
- If you forget your password, you can reset the password yourself - staff are encouraged to attempt a password self-service reset through nhs.net portal prior to engaging any other support request.
- If a self-service password reset is unsuccessful, please log your request via the EPUT IT Service desk at https://servicedesk.eput.nhs.uk
- If it is imperative that your account is unlocked immediately, please contact 0845 603 6009 and hold for an agent to assist you.
- You will be prompted to change your password every 90 days.

For additional “hints and tips” please refer to Appendix 3 attached

6.0 MONITORING OF EMAILS

6.1 The Trust retains the right to access an 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, clinical safety when staff are on long-term sick, suspension etc. or as required by law, by application of the appropriate legal statutes.

6.2 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 or suspicion of email misuse.

6.3 All email will be automatically scanned for viruses, inappropriate content and unauthorised attachments by the NHSMail platform provider.

6.4 The Trust will work with NHSmail to find a reasonable process to ensure emails can be accessed appropriately and within a reasonable time period. The time period will be set by NHSmail as the system is managed by NHS Digital and the Trust has no control over this process

7.0 MONITORING ARRANGEMENTS

7.1 These procedural guidelines will be monitored and reviewed in line with Trust policy, every three years and / or in line with changes to national / local guidance.

7.2 Compliance to this procedure will be undertaken in line with Trust policy and timetables for compliance audits.

7.3 The Caldicott Network and Information Governance Steering Committee will have overall responsibility for overseeing the implementation of these procedural guidelines

8.0 RELATED DOCUMENTS

8.1 **Trust Policies and Procedures**
8.1.1 Information Governance & Security Policy and associated Procedures
8.1.2 Data Protection & Confidentiality Policy and Procedure
8.1.3 Freedom of Information Policy and Procedure
8.1.4 Corporate Records Management Policy and associated Procedures
8.1.5 Records Management Policy and associated Procedures
8.1.6 Information Sharing & Consent Policy and Procedure
8.1.7 Mobile Phone Policy and associated Procedures
8.1.8 Other relevant policies and procedures not mentioned
8.1.8 NHS Mail usage policy

8.2 **National Legal Statutes**
8.2.1 General Data Protection Regulation
8.2.2 Human Rights Act 2000
8.2.3 EU Privacy and Monitoring Directive 2000
8.2.4 Regulation of Investigatory Powers Act 2000
8.2.5 Freedom of Information Act 2000
8.2.6 Computer Misuse Act 1990 and amended 2006
8.2.7 Copyright, Design and Patents Act 1998
8.2.8 Caldicott 2
8.2.9 Sexual Offences Act 2003
8.2.10 Health & Social Care Act 2012
8.2.11 NHS Constitution
8.2.12 Records Management Code of Practice
8.2.13 Data Protection Act 2018

END