Tees, Esk and Wear Valleys NHS
NHS Foundation Trust

Email procedure

Ref IT-006-001 v2.8

Status: Ratified

Contents

1 Purpose

This procedure describes:

- How to use NHS Mail for Trust business;
- When you can and cannot send personal or business-sensitive information;
- The Trust's rules for minimising the risk of sending information electronically.

2 Who this procedure applies to

This procedure applies to all employees of Tees, Esk and Wear Valleys NHS Foundation Trust, as all employees are given access to NHS mail.

3 Related documents

This procedure must be read with the following policy:-

- Email policy

The Email Policy defines acceptable and unacceptable use of The Trust's Email System (NHSmail). You must read and understand the Email Policy before carrying out the procedures described in this document.

4 Accessing NHSmail

You can access NHS Mail from a Trust device using:

1. Microsoft Outlook
2. Web-based interface www.nhs.net
3. Touchdown (From Trust Smartphones)

You can access NHS Mail from a NON-Trust device using:

1. The web-based interface (www.nhs.net)

4.1 Best method for accessing email

Location	Equipment	MS Outlook	www.nhs.net	TouchDown*
Trust premises	Trust equipment	✓	✓	✓
Non-Trust premises	Trust Remote Access Solution (Pulse) connection or Trust Smartphone	✓	✓	✓
Anywhere	Personal mobile device or personal Smartphone	×	✓	×
Non NHS premises	Non-Trust supplied laptop/pc	×	✓	×

*Touchdown is only available on Trust issued Smartphones.

Trust Smartphones are set up to access NHSmail via TouchDown. You must not configure your Trust Smartphone to access NHSmail in any other way.

Non-Trust equipment **must not** be connected to the Trust network.

4.2 Accessing email using non-Trust equipment at non-Trust location

- Access NHSmail via the web based interface (www.nhs.net). Do not use any other software to view the 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 of public access to the device (i.e. other members of your family).
- In exceptional circumstances, you may be allowed to choose the private option and download information but this must be authorized by Information Governance **before** the information is downloaded.
- Remember the Trust's Code of Confidentiality - think about the sensitivity of what you view and who can see the screen.

4.2.1 Using your personal smartphone – important information

Adding your NHSmail account to your personal mobile device is the same thing as configuring your personal device to receive emails from NHSmail. The only authorised way for accessing NHSmail on mobile devices is by Trust issued Smartphone or using www.nhs.net through the internet browser on your personal device.

You must not configure your personal mobile device access NHSmail because:

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

- When a device is configured to access NHSmail, it keeps the data on the phone. If this device is lost or stolen, the data on it can be accessible to anyone that has access to the device.
- Some applications can access data held on mobile devices, including email. Trust-issued devices have Touchdown installed which prevents any application accessing email data held on the phone.
- Most mobile devices provide an initial synchronisation option which can replace the Calendar and Contact information in your NHSmail account with the data held on the device. If you select this option, all existing calendar and contact information in your NHSmail account will be removed and replaced with the data on your device and it could, as a result, be left blank. If you select this option, there is no way to recover your NHSmail Calendar and Contacts.
- When using a personal device to access NHSmail, the device uses the built-in email application. If you have other personal emails configured on your device, this can update with your NHSmail account, creating misleading information when your calendar is shared with others.
- When you enter your device password wrongly eight times in succession, your phone will be automatically wiped of ALL data and restored to its default factory settings. This is not the case with Trust issued device as these devices are managed centrally using a separate service.

5 Using NHSmail

5.1 Sending emails

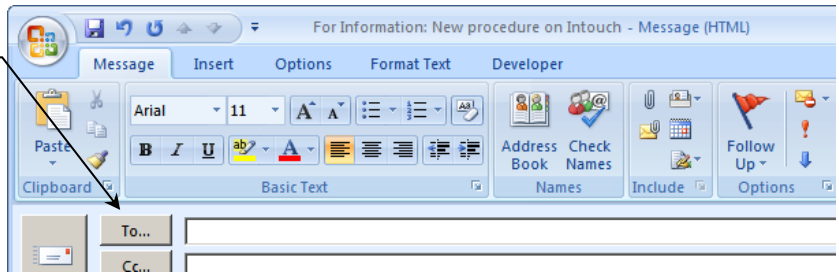
When sending an email to a recipient for the first time, **always** select them from the address book. The chance of there being another person with the same name is likely within NHSmail and could result in sensitive information being sent to the wrong person.

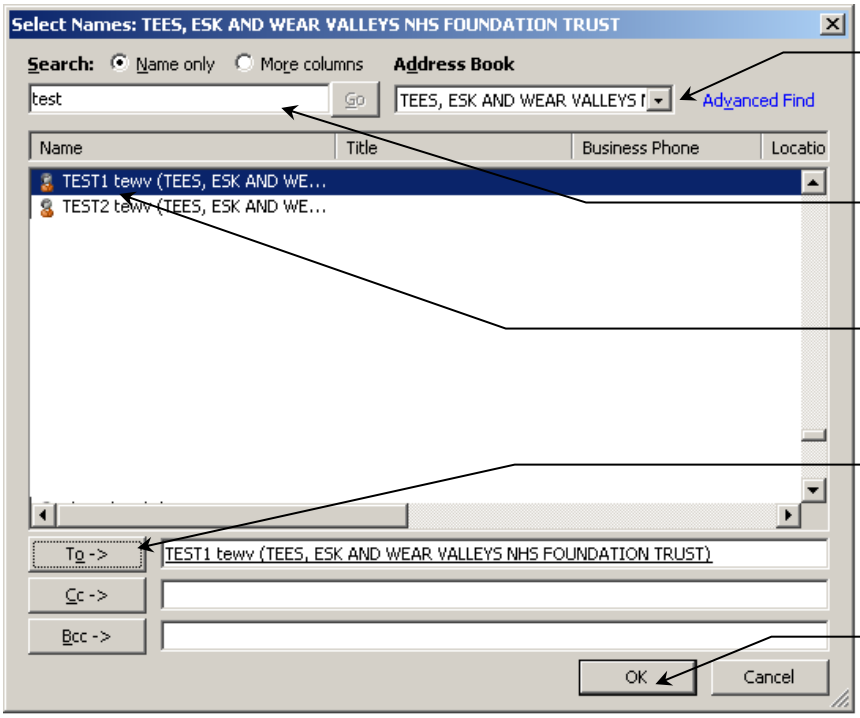
When using distribution lists (see section 5.3), staff who have left the Trust may be working elsewhere within the NHS and therefore have a valid NHSmail email address.

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.

5.1.1 Using the address book (MS Outlook)

1. Click **To** (or **Cc** as needed) to show the Address Book

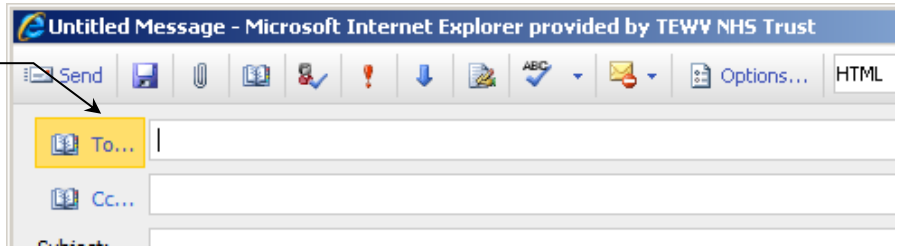




2. Click the drop down to find Tees, Esk and Wear Valleys NHS Foundation Trust
3. Type the name of the recipient, surname first
4. Click on the name of the recipient if they are on the list
5. Click **To** or **Cc** to select the recipient. Repeat for other staff as needed.
6. When finished, click **Ok**

5.1.2 Using the address book (www.nhs.net)

1. Click **To** (or **Cc** as needed) to show the Address Book



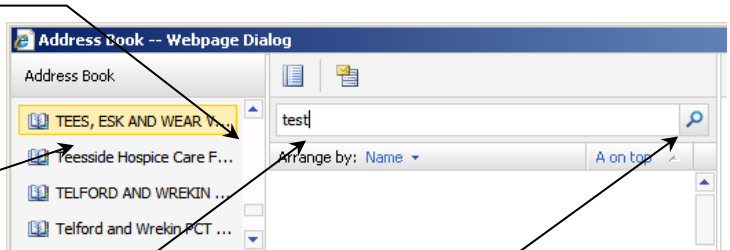
2. Click on **Show other address lists**

3. Scroll through the list of addresses until you find Tees, Esk and Wear Valleys NHS Foundation Trust

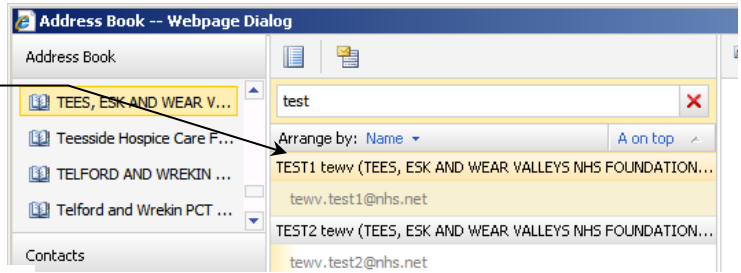
4. Click on the Trust's name to display the names of Trust staff

5. Type the name of the recipient, surname first

6. Click the magnifying glass to start the search



7. If more than one person is listed, click on the correct recipient



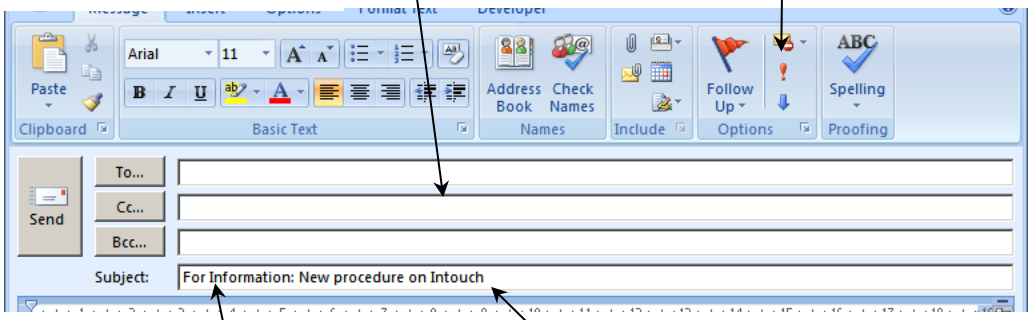
8. Click **To** or **Cc** to select the recipient. Repeat steps 5-8 to add other staff as needed

9. When finished, click **Ok**

5.1.3 Starting your email

Use ‘cc’ if adding someone for information only. Do not use cc if the recipient needs to act on the information.

Mark emails as ‘High importance’ only on messages that warrant it.



Start your subject with ‘For Action’, ‘For Information’, ‘For approval’ etc, to help the recipient prioritise their actions.

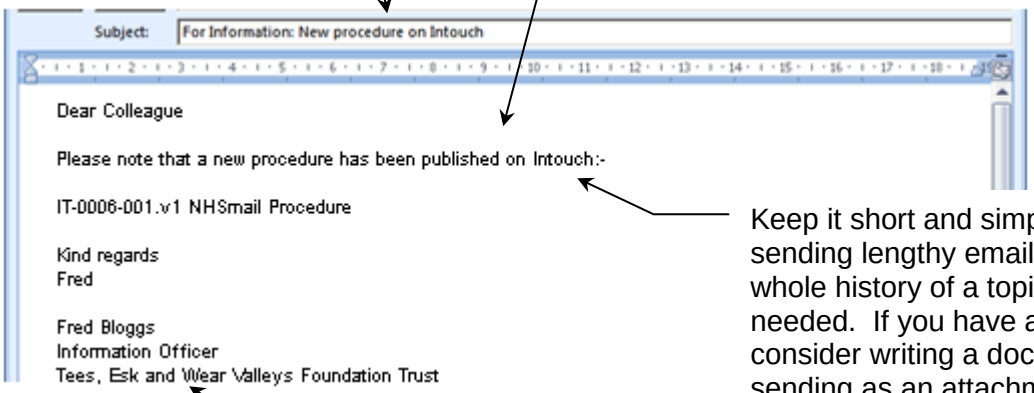
Always complete the subject line. Make the subject of your email relevant, clear and brief to help you and the recipient file, retrieve and prioritise the message.

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

5.1.4 The content of your email

Put different topics in separate emails; don’t put them in one long email

Use lower case. CAPITALS are considered aggressive, like shouting



Keep it short and simple. Avoid sending lengthy emails with the whole history of a topic unless needed. If you have a lot to say, consider writing a document and sending as an attachment

Add a ‘signature’ for a professional end to your email (following the Trust standard)

Do not include person identifiable information in the body of your email.

5.1.5 Trust standard email signature

Use the Trust standard email signature for a consistent and professional end to your email.

Font type and size	Arial 11
Background	None

Example:-

Name
Job Title
Tees, Esk and Wear Valleys NHS Foundation Trust
Building/hospital name
Address Line 1
Address Line 2
Town
County
Postcode

Email :
Office :
Mobile :

5.1.6 Important points to remember

- Emails can be disclosed to the public in response to a Freedom of Information, Subject Access or Environmental Information 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; 
  - The content is clear and correct.
  - The layout is consistent.
- A read receipt shows a message was opened; not read, understood and acted upon. Read receipts should not be routinely requested as this increases email traffic volumes.
- Avoid sending large attachments, especially to multiple email addresses as this causes network congestion and storage space problems. Where possible, include a link to the document/s instead.
- A large file is anything over 2 Mb in size. Avoid sending emails containing scanned images or large pictures. Avoid sending large multiple attachments. Take care sending databases as they can be very large.
- 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.
- Think about whether email is the best form of communication and be selective – only send the email to those who really need it.
- Do not assume that the responsibility for an action has been passed to someone by sending them an email. It is important to get confirmation from the recipient that they have read and understood the content.

5.2 Sending person/patient identifiable (PII) or business sensitive information

5.2.1 Secure email grid and whitelist

✓ secure email transfer × unsecure email transfer **?** see white list		**Receiving address**												
		*nhs.net	*.gcsx.cov.uk	*.hscic.gov.uk	*.gsi.gov.uk	*.gse.gov.uk	*.gsx.gov.uk	*.mod.uk	*.pnn.police.uk	*.scn.gov.uk	*.cjsm.net	*.gov.uk	*.nhs.uk	Other email address
Sending address	*nhs.net	✓	×	✓	×	×	×	✓	✓	✓	✓	**?**	×	×
	*.gcsx.gov.uk	×	×	×	×	×	×	×	×	×	×	×	×	×
	*.hscic.gov.uk	✓	×	✓	×	×	×	✓	✓	✓	✓	×	×	×
	*.gsi.gov.uk	×	×	×	×	×	×	×	×	×	×	×	×	×
	*.gse.gov.uk	×	×	×	×	×	×	×	×	×	×	×	×	×
	*.gsx.gov.uk	×	×	×	×	×	×	×	×	×	×	×	×	×
	*.mod.uk	✓	×	✓	×	×	×	✓	✓	✓	✓	×	×	×
	*.pnn.police.uk	✓	×	✓	×	×	×	✓	✓	✓	✓	×	×	×
	*.scn.gov.uk	✓	×	✓	×	×	×	✓	✓	✓	✓	×	×	×
	*.cjsm.net	✓	×	✓	×	×	×	✓	✓	✓	✓	×	×	×
	*.gov.uk	**?**	×	×	×	×	×	×	×	×	×	×	×	×
	*.nhs.uk	×	×	×	×	×	×	×	×	×	×	×	×	×
	Other email addresses	×	×	×	×	×	×	×	×	×	×	×	×	×

Email exchanged between *nhs.net email accounts and *.gov.uk email accounts are deemed by the trust as **not** secure, as such they should not be used to exchange PII or other sensitive information. For example *@CouncilName.gov.uk is not secure.

The **only** exception to this rule is if the *.gov.uk domain name appears on below white list as being accepted as compliant by the Trust. It is safe for Trust staff using *nhs.net email accounts to exchange email with local authority staff using email with the below white list email domain names. For example exchanging email between *nhs.net and a correct email address ending *@darlington.gov.uk is secure.

White List:-

@darlington.gov.uk	Compliant
@northyorks.gov.uk	Compliant

@york.gov.uk	Compliant
@hartlepool.gov.uk	Compliant
@stockton.gov.uk	Compliant
@middlesbrough.gov.uk	Compliant
@durham.gov.uk	Compliant
@redcar-cleveland.gov.uk'	Compliant
@teesvalley-ca.gov.uk	Compliant
@justice.gov.uk	Compliant
@cntw.nhs.uk	Compliant

NHS Mail have introduced an encryption service that now allows secure emails and attachments to be sent to un-secure email systems. The email must be sent from an @nhs.net email address.

5.2.2 Secure email process

Before you send PII or Business Sensitive Information
Have you identified a legitimate business need for the information to be sent?

Yes / **No**

No → **Do not send PII/sensitive information by email**

Yes → **Are you sending the information to a colleague on the TEWV contacts list?**

No / **Yes**

Yes → **Does the recipient have access to the relevant shared drive?**

No / **Yes**

Yes → **1.** Send hyperlink to the information in the body of the email

No → **Do you need to send the PII/sensitive information on a regular basis?**

No / **Yes**

Yes → **2.** Arrange to set up a shared drive for this purpose.
Contact Information Service Desk

No → **3.** Send PII/sensitive information as an attachment

Is the recipient organisation part of an agreed information flow with the Trust?

Yes / **No**

No → **Do not send PII/sensitive information by email**

Yes → **Does the recipient have a secure email address? (see secure email grid)**

No / **Yes**

Yes → **4**. Send PII/sensitive information as an attachment – no encryption necessary

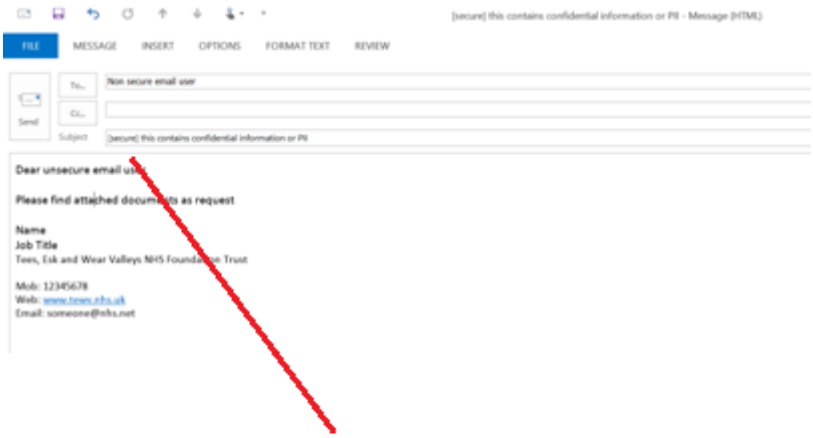
No → **Use the NHSmail encryption service to securley send the information and any attachements.**

5.2.3 Using NHSmail encryption service

NHSmail to Non Accredited System

If you have a contact that uses a non-accredited or non-secure email service (marked with a *x* in the secure email grid in section 5.2.1) with whom you need to exchange sensitive information, you will need to send the initial encrypted email that they can then open, read and reply to securely.

All the sender needs to do is in the subject field of the email enter **[secure]** before the subject of the message, the word MUST be surrounded by square brackets. i.e. subject: [secure] information as discussed



Type **[secure]** in the subject message - remember to include the square brackets

Then compose the message as normal, including any attachments. It is good practice to send a test email first.

The service then encrypts the message and delivers it.

The recipient will then get a message to say they have received the email, and they must then login to a secure portal to access this. Guidance is available on the NHSmail website and at Accessing Encrypted Emails Guide for Non-NHSmail users; and it would be good practice to send this guidance to the recipient prior to sending the message.

Further guidance for trust staff is available at Encryption Guide for NHSmail users.

5.2.4 Important points to remember

⚠	Information sharing agreements are published on InTouch > Services > Nursing and Compliance > Information Governance > Information Sharing Agreements
⚠	Consider who has access to the mailbox. Recipients may have assigned delegates who can read email on their behalf.
•	If password-protecting a document, you must use a secure password which must include a mixture of words, numbers, higher and low case digits.

• NHSmail is an encrypted service. You do not need to encrypt attachments when sending to another NHSmail account and some government email addresses (see 5.2.1).
• Encrypted attachments are blocked by NHSmail and some government email systems to avoid the risk of computer viruses being sent or received.
• Could it be recorded and communicated via PARIS instead of via email?
• 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 Information Service Desk to investigate creating a 3rd Party NHSmail account.
• 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.
• Check the email address is accurate and secure before you send PII.

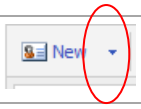
5.3 Distribution lists

Distribution lists enable you to send one email to many people without needing to select each individual.

5.3.1 Creating a distribution list (MS Outlook)

Step	Action
1	On the **File** menu, point to **New**, and then click **Distribution List**.
2	In the **Name** box, type a name.
3	Click **Select Members**.
4	In the **Show names from the** list, click the address book that contains the e-mail addresses you want in your distribution list.
5	In the **Type name or select from list** box, type a name you want to include. In the list below, select the name, and then click **Members**. Do this for each person you want to add to the distribution list, and then click **OK**.
6	If you want to add a longer description of the distribution list, click the **Notes** tab, and then type the text.
7	The distribution list is saved in your **Contacts** folder by the name you give it.

5.3.2 Creating a distribution list (www.nhs.net)

Step	Action
1	Click **Contacts**
2	Click the drop down arrow next to the **New** option 
3	Select **Distribution list**
4	Click **Members**
5	Click **Show other address lists** to find Tees, Esk and Wear Valleys NHS Foundation Trust
6	Search for the person to add to your list and click on **Members** 
7	Repeat steps 2 – 6 as needed
8	When your list is complete, click **OK**
9	Click **Save and close**

5.3.3 Important points to remember

Staff who have left the Trust may continue to use their NHS mail address. Review your distribution lists regularly to ensure that members who have left the Trust do not continue to receive Trust data.

If the distribution list contains contact details for anyone other than staff, send your email using the BCC option (see 5.3.4 below). This will prevent contact details being shared accidentally with those who do not have a right to know them.

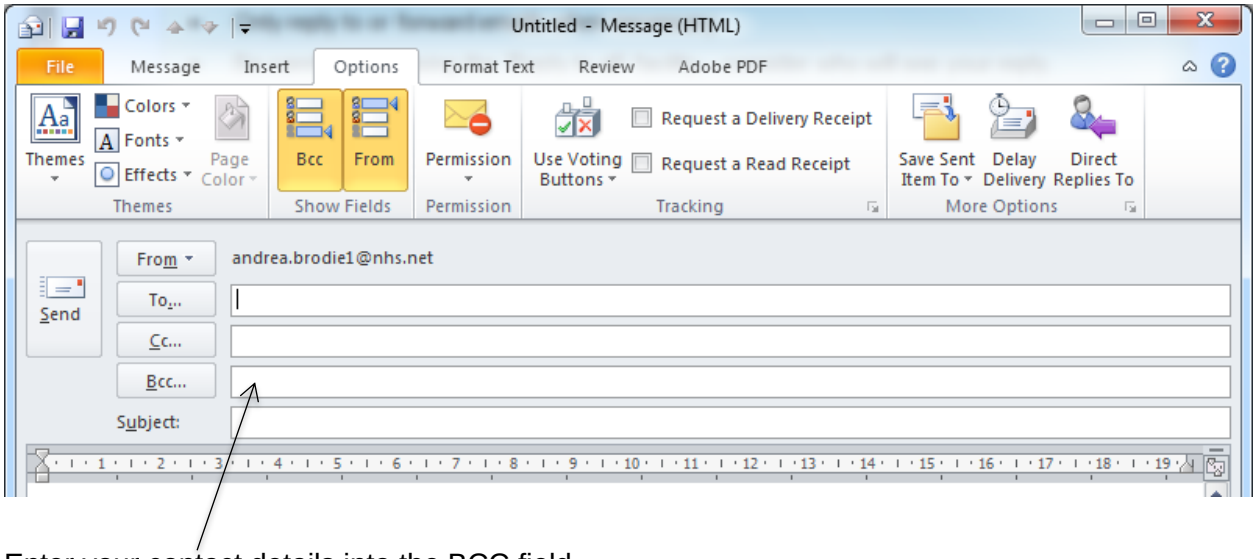
- Use distribution lists with care so that information is only communicated to those people with a need to know.
- Global communication should be done via the Information Service Desk.
- There must be a business need for non-Trust individuals to be included in your distribution list.

5.3.4 How to use the BCC option

The BCC (or blind carbon copy) feature maintains security and privacy when sending emails to a group of people. When you place email addresses in the BCC field, those contact details are invisible to the recipients of the email.

To switch on the BCC option:

1. Create a new email
2. Click Options
3. Click the BCC icon



Enter your contact details into the BCC field.

5.4 Receiving emails

- 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 (www.nhs.net).
- 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.

5.5 Replying and forwarding

- 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’.

5.6 Out of office assistant

Always set up the ‘Out of Office Assistant’ if you are going to be away from your email, giving details of anyone who is covering for you.

5.6.1 Setting up out of office assistant (MS Outlook)

Step	Action
1	On the **Tools** menu, click **Out of Office Assistant**.
2	In the Out of Office Assistant dialog box, select **Send Out of Office auto-replies**.
3	If you want to specify a set time and date range, select the **Only send during this time range** check box. Then set the **Start time**, and then set the **End time**.
4	In the **Inside my organization** tab, type the message that you want to send within your organization, and in the **Outside my organization** tab, type the message that you want to send outside your organization.
5	Click **Ok**.
6	If you selected the “Only send during this time range” option in step 4, Out of Office messages will be sent until the date and time set for the End Time in step 5. Otherwise, the Out of Office Assistant will continue to run until you repeat step 1 and select the “Do not send Out of Office auto-replies” option.

5.6.2 Setting up out of office assistant (www.nhs.net)

Step	Action
1	Click **Options**.
2	Click **Out of Office Assistant**.
3	In the Out of Office Assistant dialog box, select **Send Out of Office auto-replies**.
4	If you want to specify a set time and date range, select the **Send out of office replies only during this time period** check box. Then set the **Start time**, and then set the **End time**.
5	In the **Inside my organization** box, type the message that you want to send within your organization, and in the **Outside my organization** box, type the message that you want to send outside your organization.
6	Click **Save**.
7	If you selected the “Only send during this time range” option in step 4, Out of Office messages will be sent until the date and time set for the End Time in step 5. Otherwise, the Out of Office Assistant will continue to run until you repeat step 1 and select the “Do not send Out of Office auto-replies” option.

5.7 Emailing service users

Question	Answer
Does the Trust allow email communication with service users?	Yes, if the secure email guidance is followed Secure Email Guidance for Non-NHSmail recipients and Encryption Guide for NHSmail users

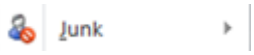
What do I do if a service user contacts me via email?	Contact them to let them know that you would prefer to communicate with them through a secure email system and explain the procedure for this. If after fully understanding the risks of communicating outside of a secure email system they still wish to go ahead then record the communication in the patient's care record together with the patients decision.
What do I do if the service user insists that they have information about their care emailed to them?	They can choose to communicate with the Trust in this way but we must explain the risks to them and offer them the most secure options first. If there are any queries arising from the communication request contact the Information Governance department.

5.8 Nuisance emails and blocking senders

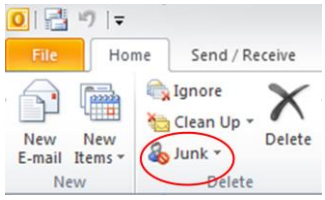
If you receive nuisance emails such as newsletters, marketing or social media updates which you do not wish to continue receiving but do not think pose a threat, you can block the sender or sender's domain.

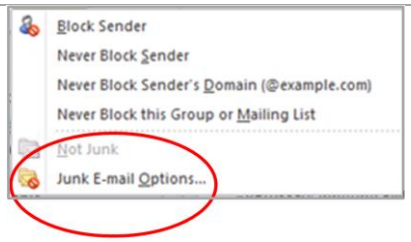
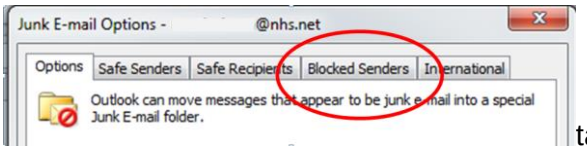
5.8.1 Blocking senders in Microsoft Outlook 2010

Block a single sender.

Step	Action
1	**Right click** on the email in your inbox
2	Choose **Junk**  from the dropdown list.
3	Choose **Block Sender**  from list

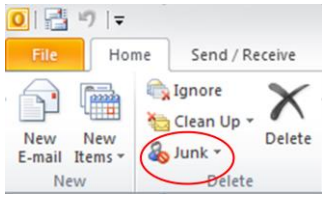
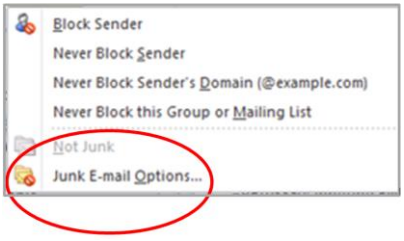
Block multiple senders at once (or block a sender that you have not yet received an email from)

Step	Action
1	Click **Home** at the top of the screen and click on **Junk**  in the menu bar.
2	Click on **Junk Email Options** from the drop down list

	
3	Select the **Blocked Senders**  tab from the top ribbon of the window that appears on screen
4	Click **Add** on the right side of the window
5	Type the email address you wish to block and click **OK**
6	Repeat steps 4 & 5 to add more addresses you wish to block
7	When you have finished, click **OK** at the bottom of the window

5.8.2 Un-Blocking senders in Microsoft Outlook 2010

You can also use the same **Blocked Senders** tab to remove a sender from your blocked senders list if you have added them in error.

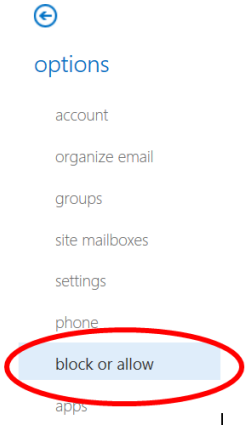
Step	Action
1	Click **Home** at the top of the screen and click on **Junk**  in the menu bar.
2	Click on **Junk Email Options**  from the drop down list
3	In the **Blocked Senders**  tab, highlight the email address you wish to remove and click **Remove**. You can highlight and remove more than one email address at once
4	Repeat step 3 to remove more addresses
5	When you have finished, click **OK** at the bottom of the window

5.8.3 Blocking senders with Outlook Web App (OWA)

Block a single sender.

Step	Action
1	**Right click** on the email in your inbox
2	Select **Move** from the dropdown list (if present, click on **More**)
3	Select **Junk Email**

Block multiple senders at once (or block senders that you have not yet received an email from).

Step	Action
1	Click on the **settings** icon at the top right of the screen and select **Options**
2	 Click **Block or Allow** on the left side of the screen
3	Scroll down to the **Blocked Senders** section
4	Click the **plus** icon on the right side of the window
5	Type the email address you wish to block and press **Enter** on your keyboard
6	Repeat steps 4 & 5 to add more addresses to block
7	When you have finished, click **Save** at the bottom of the page
8	Click on left pointing arrow in circle icon , top left off screen, to “Return to Outlook Web App”

5.8.4 Un-Blocking senders with Outlook Web App (OWA)

You can also use the same **Blocked Senders** section to remove a sender from your blocked senders list if you have added them in error.

Step	Action
1	Follow steps 1 – 3 in above instructions to find **Blocked Senders** section.

2	In the **Blocked Senders** section, highlight the email address you wish to remove and click the **minus** icon ➖. You can highlight and remove more than one email address at a time
3	Repeat step 2 to remove more addresses
4	When you have finished, click **Save** at the bottom of the page

6 Using the calendar

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 should contain the minimum patient or personal identifiable information to allow you to attend your appointment.

- Documents embedded in your calendar are viewable by all staff with access to your calendar.
- Creating hyperlinks to documents restricts access to those staff who have access to the documents via the shared drive as hyperlinks will only work if the distribution list has access to the drive where the documents are stored.
- Hyperlinks will not work if using NHSmail via a non-Trust network.

7 NHSmail web access functionality

As of the 1st April 2015, NHS Mail withdrew the SMS and Fax Functionality of NHSmail. The Trust has purchased a service to provide SMS functionality from another provider. This service now involves a cost and access to it must be requested via the information service desk.

Upon access being granted, guides on how to use the service are issued.

There is no replacement fax functionality, you should always think about sending a fax and ask your self could the information be sent via secure email?

8 Mailbox management

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.

8.1 Attachments – sending and saving

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.
- **Send a hyperlink** instead of an attachment if the recipient has access to your shared area.
- If sending an attachment that is saved on your home or 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.

8.2 Mailbox limits

- Your mailbox has a size limit depending on your business need (see Appendix A – NHS mailbox quotas).
- **All** email sub-folders **and** calendar items count towards the amount of space you are taking up - 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.

8.3 Generic mailboxes

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

8.4 Managing email messages that are corporate records

Question	Answer
When is an email classed as a corporate record?	Anything that is evidence of a decision or a business transaction should be saved and filed as a record on the shared drive and within the correct folder. Emails containing important links to projects and processes and/or including decisions should be kept.
Can I leave such emails in my mailbox?	You need to identify those emails that are records of your business activity, and manage them differently to routine email messages. **Move** the message/attachment to the relevant folder in the shared drive. If the information is in draft or is confidential, save it to your personal area on the drive (H drive). If you leave emails which are records in your mailbox, it is difficult for other people to retrieve them in your absence.
When might other people want to see my emails?	Because emails are a form of record they are subject to Records Management protocols and legislation. Emails can be disclosed to the public in response to a Freedom of Information, Subject Access or Environmental Information Request. You must never delete email (or any other type of record) if you know or suspect that it may be subject to a Freedom of Information request.
How long do I need to keep my emails for?	It is not possible to set a standard retention period for all emails because email is used to communicate a wide range of things, ranging from the instantly disposable (e.g. discussion about someone's availability for a meeting) to the highly significant (e.g. financial decisions). As such the retention period for each email is defined by its content. Depending on their content, some emails may have to be kept for a certain period of time. Guidance on retention periods can be found in the NHS Code of Practice on Records Management (Part 2).

Use your professional judgment for emails not governed by legislation, the Code of Practice or Trust policies. If in doubt ask your line manager or contact the Information Governance Team for further advice.

8.5 How do I delete unwanted mail?

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 your have set your Deleted Items to empty automatically.

8.5.1 To delete a single email

Step	Action
1	Click on the message that you want to delete.
2	Press the **Delete** key. This will move the message to your **Deleted Items** folder.
3	Click on the **Deleted Items** folder.
4	Repeat steps 1-2 above.

8.5.2 To delete many emails

Step	Action
1	Click on **Tools** menu.
2	Click on **Empty Deleted Items Folder**.

9 Account management

9.1 New accounts

- New accounts are created automatically for new staff as part of their access to the Trust network. Your email account may have a different user name to your network user name.

9.2 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 Service Desk mark you as a joiner to the TEWV directory.

9.3 Closed accounts

- Your line manager must follow the leavers' process and inform the Information Service Desk when a staff member is leaving the organisation. You must clear your mailbox of all Trust information prior to transferring to a new NHS organisation.

Do not delete emails that are corporate records. See Section 8.4 – Managing email messages that are corporate records.

9.4 Passwords

- Your NHSmail account must have a unique password which you **must not share**.
- If you forget your password, you can reset the password yourself using www.NHS.net or contact the Information Service Desk (01642 283949).
- If you lock yourself out of your account, it can only be unlocked from a Trust connection.
- You will be prompted to change your password every 90 days.

Appendix A - NHSmail Mailbox Quotas

*Local Organisation Administrators may un-suspend the account. It will be automatically re-suspended each night if still 250Mb over quota. The restrictions will remain in place until your mailbox size is reduced to below the quota limit so it's important that you take action to reduce your mailbox size as soon as you receive a warning. It's important to note that restrictions on sending email will have a knock-on effect on other areas such as the calendar - you won't be able to send meeting invitations, for example. If your account is unable to receive email, anyone sending you a message will be notified that your account is over quota and unable to receive email.

Quota status	Restrictions
Under quota	No quota related restrictions applied
Nearing quota	Daily warning email sent (for generic mailboxes the warning email will be sent to the LOA, mailbox owner and account holders who subscribe to the mailbox)
Over quota	Cannot send mail (for generic mailboxes the warning email will be sent to the LOA, mailbox owner and account holders who subscribe to the mailbox)
200Mb over quota	Cannot send mail (for generic mailboxes the warning email will be sent to the LOA, mailbox owner and account holders who subscribe to the mailbox) Cannot receive mail Anyone attempting to send to a mailbox which is receive-disabled will be sent a message stating that the message cannot be received
250Mb over quota	Cannot send mail Cannot receive mail Account suspended*

10 Document control

Date of approval:	13 January 2016	
Next review date:	31 December 2023	
This document replaces:	Ref-IT-006-001 v2.7	
Lead:	Name	Title
	Keith I'Anson	Desktop Product Manager
Members of working party:	Name	Title
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 Safety and Governance Board	04 July 2018
An equality analysis was completed on this document on:	19 October 2012	
Amendment details:	26 July 2017 – added guidance for use of BCC feature at 5.3.3 and 5.3.4 4 July 2018 – section 5.8 added – dealing with nuisance and unwanted email 09 January 2019 - Document under review, review date extended to allow review work to be done. 27 February 2019 – 5.2.1 p11- reference to list of secure email systems removed; Secure email guidance links updated on 5.2.3 p13, and 5.7 p17. 04 March 2019 – 5.2.1 p11 - amended to include whitelist of approved secure *.gov.uk domains. 17 April 2019 – 5.2.1 p11 – amendment to secure email grid. 15 May 2019 – 5.2.1 p 11- amendment to secure email grid whitelist 28 June 2019 – Review date extended from 01 Jul 2019 to 01 July 2020 25 July 2019 – (v2.7) 5.2.1 p 11- amendment to secure email grid whitelist 10 December 2019 – (v2.8) 5.2.1 p 11- amendment to secure email grid whitelist July 2020 – review date extended to January 2021 02 December 2020 – (v2.8) review date extended to 31 March 2021 18 March 2021 – (v2.8) review dated extended to 31 May 2021 May 2021 – (v2.8) review date extended to 31 Oct 2021 Oct 2021 – (v2.8) review date extended to 31 March 2022	

	Jan 2022 – Review date extended to 30 September 2022 Sept 2022 – Review date extended to 30 April 2023 May 2023 – Review date extended to 31 December 2023