Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Email and Internal Communications Policy

This procedural document supersedes: **CORP/ICT 27 v.2 – Email and Internal Communications Policy**

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s):	Ken Anderson, Trust CIO and SIRO
Author/reviewer: (this version)	Roy Underwood, David Linacre
Date written/revised:	December 2021
Approved by:	IG Committee
Date of approval:	20 December 2021
Date issued:	May 2022
Next review date:	November 2024
Target audience:	Trust-wide

Amendment Form

Please record brief details of the changes made alongside the next version number. If the procedural document has been reviewed **without change**, this information will still need to be recorded although the version number will remain the same.

Version	Date Issued	Brief Summary of Changes	Author
Version 3	Dec 2021	• Tri-Annual Review • Advance warning from NHS providers associated with the National COVID-19 Public Enquiry – expected Spring 2022	Roy Underwood David Linacre
Version 2	January 2019	• Review and inclusion of further detail concerning NHS Mail's Subject Access (Para 3.1.4) & Organisational Investigation (Para 3.1.5 and 3.2) Policies and Processes – compliant with GDPR and DPA 2018. • Advise on setting up and using controlled 'shared network folders' (Para 3.1.7) for staff personal data held by managers and POD staff.	Roy Underwood Joanne Hutchinson Nigel Hall
Version 1	November 2017	• This is a new procedural document, please read in full.	Roy Underwood Joanne Hutchinson

Contents

Page No.

1 INTRODUCTION

The use of email and electronic internal communication (Skype for Business) methods has risen exponentially in the last decade and for many organisations it is an indispensable tool offering fast and efficient messaging regardless of geographic boundaries and using common standard protocols. As a result, email has developed into a key tool for sharing information both within the Trust and externally with partner organisations. Email is used across the full scope of Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust (DBTH) activities including both clinical and corporate data.

NHSMail accounts are owned by:

- NHS Digital (HSCIC) on behalf of the Secretary of State for Health in England
- NHS National Services Scotland (NSS) in Scotland

and provided to NHS staff for their use. Where accounts are no longer used, they are automatically removed after a period of inactivity as defined in the Data Retention Policy.

For all NHSMail and Skype for Business policy and Guidance Materials please visit https://portal.nhs.net/Help/policyandguidance

2 PURPOSE

This policy applies to all Trust staff authorised to use the NHSMail email service including but not limited to contractors, NHS Professionals, bank staff, voluntary organisations or suppliers granted email accounts / access for support purposes.

The policy supports the NHSMail Acceptable Use Policy (AUP) which all NHSMail users are required to accept upon first logging in to the NHSMail portal. A copy of the current version can be found at https://portal.nhs.net/Home/AcceptablePolicy.

3 DUTIES AND RESPONSIBILITIES

The following staff groups will have duties and responsibilities within the Email Usage Policy.

3.1 NHSMail

3.1.1 NHSMail will manage all email accounts in accordance with the following policies which can be found on the NHSMail support website.
http://support.nhs.net/policyandguidance

- Access Policy
- Acceptable Use Policy
- Clinical Safety

- Information Management Policies
- NHSMail Information Management Policy
- NHSMail Data Retention Policy
- NHSMail Access to Data Policy

3.1.2 NHSMail will delete accounts automatically if they have not been accessed in line with their policies.

3.1.3 Where the IM&T department have been notified to disable a user account this will remain, however NHSMail will delete the account in line with their policies if it is not re-enable by IM&T.

3.1.4 NHSMail are the responsible Data Controller for managing subject access requests for individual's personal data under the subject access provisions of GDPR and the Data Protection Act (DPA) 2018 (current data protection legislation). Please refer to NHSMail's Policies listed above for further information. The Trust is not responsible for handling the NHS Mail Systems personal data requests as it is not the data controller**.** Individual NHS Mail Users addresses can easily be confused e.g. a person called Any Body could have an email address of:

- any.body@nhs.net
- a.body@nhs.net
- anybody@nhs.net, or indeed
- any.body[1-n]@nhs.net

therefore, only NHS Mail will be able to positively identify individual Users based on the additional personal data that Users provide when they sign up for the service. They will use these additional data provided by Users to positively identify them when dealing with their individual subject access requests.

3.1.5 NHSMail are responsible for providing public authorities with authorised access[1] to User's account data for the lawful discovery of evidential data in connection with their duties as a public authority on a case by case basis.

3.1.6 NHSMail is a messaging system and should not be used for long term data storage or archive. Emails containing Patient information must be handled as detailed in section 4.6.

3.1.7 NHSMail should not be used to carry messages containing personal data relating to Staff. These data should increasingly be held by relevant managers in bespoke, secure and private network folders where controlled access may be shared appropriately and on an as necessary basis. Email messages may then be sent to shared folder users where they need to be informed or alerted to new or changed content resident in a secure network folder. This will make it much easier for managers including People & Organisational Development Business & Casework Managers to manage individual subject access requests for personal data held within single user or multiple user

[1] The Trusts authorised officers are: The Trust CEO or their Deputy, and the Director of People & Organisational Development

secure network folders. Shared network folder controls can be set by authorised managers through the IT Services helpdesk.

3.2 Chief Executive & Director of People and Organisation Development

3.2.1 The Chief Executive and the Director of People and Organisational Development must familiarise themselves with the NHSMail Access to Data Policy. http://support.nhs.net/policyandguidance.

3.2.2 Only the Chief Executive or their Deputy and the Director of People and Organisational Development can make requests on behalf of the organisation to access an individual's NHSMail account contents as part of a formal investigation or for the purposes of organisational business continuity and patient safety, full details of the content that can be requested is contained in the NHSMail Access to Data Policy. This request does not fall under the Subject Access provisions of the DPA 2018.

- All requests must be sent from the Chief Executive Office or the Director of People and Organisational Development to the NHSMail Programme team via email feedback@nhs.net.
- Individual subject access requests for access to Users personal data should be made in accordance with NHS Digital's GDPR Transparency Policy – Your Rights: https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/NHS+Digital+(NHSmail+Live+Service)+Transparency+Information.pdf.

3.3 Information Management & Technology

The Information Management & Technology (IM&T) Department will:

3.3.1. Provide advice to staff on email usage as requested.

3.3.2. Disable, Create, provide business continuity/patient safety access to, or Associate existing NHSMail accounts to the DBTH organisation on NHSMail, as appropriate, when duly authorised.

3.3.3. Request an increase the mailbox limit from 4GB where authorised to do so by General Managers or Executives.

3.3.4. The IT Service Desk will request the recover items on behalf of the user, where the items fall between >30 days <180 days since it was deleted and when duly authorised in writing. See NHSMail Data Retention policy for exceptions.

This may be in connection with:

- A user request
- A request associated with an authorised investigation as in 3.2.2.

3.4 Line Manager

Line Managers are responsible for ensuring that:

3.4.1. Their staff members comply with the NHSMail policies, this Trust policy and associated procedures.

3.4.2. Their staff members and external users under their management who use email for work purposes, are aware of, and comply with, the NHSMail policies, this policy and associated procedures.

3.4.3. Account set-up and / or deletion requests for staff are submitted to the IM&T department in a timely manner.

3.4.4. They take disciplinary action, as appropriate, against any member of staff in breach of this policy.

3.4.5. They notify any suspected breaches of this policy to the IM&T Department by notification to the IT Service Desk and logging the incident on DATIX.

3.5 NHSMail Users under DBTH Organisation

NHSMail users under DBTH organisation, without exception, must:

3.5.1. Familiarise and Comply with the NHSMail Policies
http://support.nhs.net/policyandguidance

- Access Policy
- Acceptable Use Policy
- Clinical Safety
- Information Management Policies
- NHSMail Information Management Policy
- NHSMail Data Retention Policy
- NHSMail Access to Data Policy
- NHSMail Data Protection Statement

3.5.2. Report instances of receiving spam messages to spamreports@nhs.net

3.5.3. Familiarise yourself with the NHSMail support pages http://support.nhs.net/

3.5.4. If you are accessing your NHSMail account from a non-corporate device i.e. a home computer, personally owned laptop or in an internet cafe, you should only access the service via the web at www.nhs.net and not through an email programme such as Microsoft Outlook, without explicit permission from the IM&T department.

3.5.5. It is your responsibility to check that you are sending email to the correct recipient, as **there may be more than one person with the same 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.
e.g. fredflintstone@nhs.net is not the same person as fred.flintstone@nhs.net or indeed f.flintstone@nhs.net etc…

3.5.6. It is your responsibility to make sure that your details in the NHS Directory are correct and up to date.

3.5.7. The General Medical Council (GMC) Good Medical Practice guidance requires doctors to keep clear, accurate and legible records. It is important that emails and Instant Messages do not hinder this. You should ensure that relevant data contained in emails or Instant Messages are immediately attached to the patient record. Failure to do so could have implications on patient safety:
https://portal.nhs.net/Home/AcceptablePolicy#Information_governance

3.5 Information governance considerations:

3.5.1 Information you provide or upload to the service may be stored outside of the country in which you reside. More information on this can be found on the NHSmail Portal support site.

3.5.2 The General Medical Council (GMC) Good Medical Practice guidance requires doctors to keep clear, accurate and legible records. It is important that emails and Teams messages do not hinder this. You should ensure that relevant data contained in emails, Teams messages, Teams recordings (if available) and other collaboration tools are immediately attached to the patient record as directed by your local organisation policies. Failure to do so could have implications on patient safety.

3.5.3 NHSmail is a communication tool to support the secure exchange of information and is not designed as a document management system. Documents, emails, or messages that are required for retention/compliance purposes should be stored within your organisation's document management system in accordance with local Information Governance policies. It is the mailbox owner's responsibility to ensure the mailbox is kept within quota to avoid restrictions being imposed and impacting business processes. Local archive solutions must be in place to manage the retention of data or your organisation may decide to use Exchange Online Archiving to help you manage your mailbox quota.

3.5.4 Organisational administrators are entitled to request access to the contents of your mailbox and O365 applications and collaboration tools you may be licenced for to support information governance processes without your prior consent. Such requests are strictly regulated, the process is detailed in the NHSmail access to data procedure.

3.5.5 When moving your NHSmail account between health and care organisations, it is your responsibility to ensure any data relating to your role is archived appropriately and is not transferred to your new employing organisation in error. Your Local Administrator should be part of this process to ensure archived data is stored appropriately. Guidance is available in the Leavers and Joiners Guide. If you continue to receive data in your new role within a different organisation this should be treated as a data breach and reported according to local governance policy and process.

3.5.6 It is your responsibility to check who has access to your SharePoint sites, Teams groups, is a member of your Yammer network or access to your OneDrive. The NHSmail Portal does not have an automated procedure to remove permission for individuals who have left your organisation.

3.5.7 A standard disclaimer will be applied to any email leaving the NHSmail infrastructure.

3.5.8 NHSmail provide a MailTip so that users can easily identify when an external email is received, this helps to raise user awareness from unsolicited email and phishing attacks. The MailTip can be moved to the top of the email as needed, should threat intelligence indicate a high alert.

3.5.8. All communication you send through the NHSMail services is assumed to be official correspondence from you acting in your official capacity on behalf of your organisation. This should be in accordance with your local organisation's policies for exchanging data. Should you need to, by exception, send communication of a personal nature you must clearly state that your message is a personal message and not sent in your official capacity. This includes Instant Messaging.

More detail from the NHSD AU Policy relating to the exchange of 'sensitive' trust data.

4. Using NHSmail services to exchange sensitive information

4.1 The NHSmail service is a secure service. This means NHSmail is authorised for sending sensitive information, such as clinical data, between NHSmail and:

- Other NHSmail addresses
- Other email systems that comply with the Data Coordination Board (DCB)1596 secure email standard
- Other email systems that comply with the pan-government secure email standard

4.2 If you need to exchange sensitive data outside of NHSmail or other email systems that do not comply with the DCB1596 secure email standard or the pan-government secure email standard, the NHSmail encryption tool must be used in accordance with the guidance materials available on the NHSmail support site. Sending an email with [secure] in the subject line will automatically protect the message for you if you are unsure if the system you are sending to is secure or not. Good practice is to share sensitive information via email as opposed to Teams messaging, as this will provide a clear audit trail.

4.3 If you intend to use the service to exchange sensitive information you should adhere to the following guidelines:

4.3.1 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.

4.3.2 Caldicott and local Information Governance principles should apply whenever sensitive information is exchanged.

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

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

4.3.5 If you accidentally share sensitive or patient data with an incorrect recipient, it is your responsibility to report this in line with your local information governance policies and processes. This is a local data breach and should be treated accordingly.

4.3.6 Where sensitive information is being saved, it is your responsibility to make sure the privacy settings of O365 collaboration tools are set to private.

4.3.7 You must always be sure you have the correct contact details for the person (or group) that you are sending the information to. If in doubt, you should check the contact details in the NHS Directory or use the search bar within Teams.

4.3.8 If it is likely that you may be sent personal and/or sensitive information you must make sure that the data is protected. Unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

4.3.9 If you are accessing your NHSmail O365 services from a non-corporate device i.e. a home computer, personally owned laptop or in an internet cafe, you must gain explicit permission from your organisation to confirm this is acceptable use.

4.3.10 Remember that personal information is accessible to the data subject i.e., the patient or staff member, under General Data Protection Regulation (GDPR) legislation.

3.5.9. Take note of para 3.3.2 above, especially where it relates to the business accessing Users accounts for business continuity and patient safety. Where appropriate, Users will be notified of any such access. Access must be authorised by a member of the Exec Team, and any access will be:

- For limited business continuity and patient safety purposes, and it will be
- Chaperoned by IT Services.

4 PROCEDURE

4.1 Legal Status of Email

4.1.1. You must not attempt to disguise your identity, your sending address or send email from other systems pretending to originate from the NHSMail service.

4.1.2. You must not send any material by email that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit, pornographic, libellous, or connected in any way with terrorism or illegal

organisations or politically extreme. If you need to transmit sexually explicit material for a valid clinical reason, then you must obtain permission from your local Caldicott Guardian. [Note: GPs may need to refer to the Caldicott Guardian at their local CCG].

4.1.3. You must not use the NHSMail service to harass other users or groups by sending persistent emails to individuals or distribution lists.

4.1.4. You must not forward chain emails or other frivolous material to individuals or distribution lists.

4.1.5. It is your responsibility to check that you are sending email to the correct recipient, as there may be more than one person with the same name using the service.

4.1.6. 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, current data protection legislation and amendments and Freedom of Information (Scotland) Act 2002. Emails should be treated like any other clinical communication and care should be taken to ensure that content is accurate and the tone is appropriate.

4.1.7. Email has the same legal status as any other form of written communication. In business dealings, unless the contrary is stated, an email can constitute a "written and signed amendment or modification" to a contract. A contractual commitment made via email will be legally binding. Improper statements made in email messages can give rise to personal or Trust liability. As with other forms of correspondence, email messages may be read by people other than the addressee.

4.1.8. In law, sending an email is the same as sending a letter or publishing a document, so inappropriate behaviour, such as sending defamatory comments, could result in legal action. Internal email has been used successfully as evidence in civil and criminal law. The content of emails may also be used as evidence in industrial tribunals, formal inquiries, including internal disciplinary and grievance hearings.

4.1.9. Information in the NHSMail service may be subject to disclosure under current data protection legislation or the Freedom of Information Act 2000 (FOI) and, except in exceptional circumstances, these must be supplied. Messages no longer retained by the sender may exist in a recipient's mailbox, or the mailbox of someone a recipient has forwarded it to, and so can be supplied from this source.

4.1.10. In view of this, users must word all Trust email messages as if they will be made public. All email users are strongly advised to use the same personal and professional courtesies, considerations and conventions in electronic mail as they would in other forms of communications.

4.2 Email Signature Format

4.2.1. When sending emails, it is important that the email and signature format is followed as a standard throughout the Trust. (See 4.2.4 for an example) If you need to cater for an individual reader's special needs this can be changed for that occasion.

4.2.1 All email should use Calibri font at size 11.

4.2.2 No emails should use Outlook themes or stationary backgrounds and all emails should be white and no staff should deviate by using Outlook themes or images picked from stationery.

4.2.3 It is Trust policy that staff will use standard signatures to be present on all emails (sent, replied to and forwarded) as follows:

- Name
- Job title
- Department
- Base – full address and postcode
- Telephone No: Fax No (optional but if present stating if it is NOT safe haven); Mobile (optional)
- NHSMail address
- If staff work part-time the days and hours they work

Example
Subject: Brief Description of Content

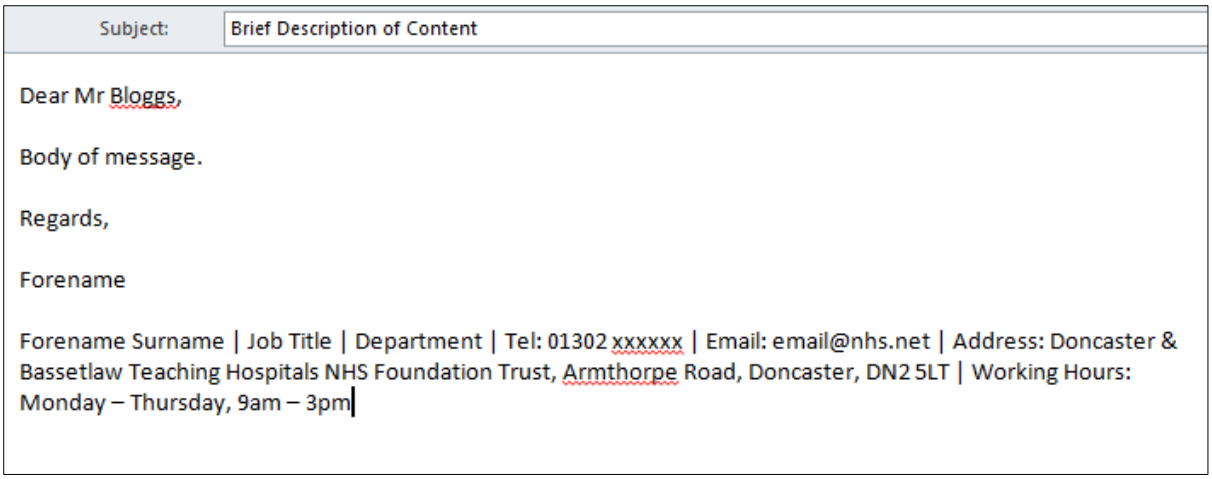
Dear Mr Bloggs,

Body of message.

Regards,

Forename

Forename Surname | Job Title | Department | Tel: 01302 xxxxxx | Email: email@nhs.net | Address: Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust, Armthorpe Road, Doncaster, DN2 5LT | Working Hours: Monday – Thursday, 9am – 3pm


Subject: Brief Description of Content

Dear Mr Bloggs,

Body of message.

Regards,

Forename

Forename Surname | Job Title | Department | Tel: 01302 xxxxxx | Email: email@nhs.net | Address: Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust, Armthorpe Road, Doncaster, DN2 5LT | Working Hours: Monday – Thursday, 9am – 3pm

4.3 Unsolicited Email and Cyber Security

4.3.1. Unsolicited email (SPAM, or junk email) is generally unwanted email content and may even be an attempt at cybercrime. This may consist of advertisements or mischievous content, although frequently sent by criminals attempting to spread malicious software intended to encrypt, delete or to steal data. All staff must understand the risks and must take adequate steps to protect themselves and the Trust. Report instances of receiving spam messages to spamreports@nhs.net

4.3.2. Email is a key tool used to spread malicious software (viruses, Trojan, etc.) either through attachments or web links and often underpinned with social engineering whereby the sender will use tactics to appear legitimate or trustworthy. Never open attachments or click on links from unknown senders.

4.3.3. Another tactic commonly used by criminals is phishing, which is the attempt to acquire sensitive information (usernames, passwords, and credit card details, etc.) by masquerading as a trustworthy entity. All staff should be mindful of requests asking for information, especially passwords, personal information, bank details, etc. If in doubt find the companies telephone number from a legitimate source and verify the request.

4.3.4. The Trust uses sophisticated technical controls to protect the Trust against the risks associated with email but there is always a chance that some threats will manage to circumvent the layers of protection. All staff should be vigilant and treat suspicious messages with extreme caution.

4.3.5. In summary, to protect yourself and the Trust, all staff must:

- Treat emails from unknown senders with caution.
- Never open attachments or links from unknown or un-verified sources.
- Never divulge sensitive information such as passwords or personal details. If in doubt find the companies telephone number from a legitimate source and verify the request.

- Be aware of social engineering techniques that criminals use to appear legitimate or trustworthy.
- Never open or respond to spam emails, a response lets the fraudsters know that the address is valid and will inevitably lead to further spam messages to that address.
- Be cautious when disclosing email addresses to non–NHS sources to reduce the likelihood of receiving SPAM.
- If there are any doubts, contact the IT Service Desk immediately for advice.
- If it looks too good to be true, it probably is!!

4.3.6. If a user suspects that they have been compromised they must immediately contact the IT Service Desk. They must also cease using their PC until advised they may do so by the IM&T Department.

4.3.7. Users must not re-send email chain letters and should use caution with any email that asks the reader to forward it to others. If in doubt, users should seek advice from their line manager or the IM&T Department.

4.4 Email Address Disclosure

4.4.1. Staff must not disclose colleagues' email addresses or personal information to non-NHS sources. If a request is made, forward it to the person in question. Only work-related contact information should be disclosed to NHS sources without colleague's express agreement.

4.5 Transmission of Personal Data via Email

Personal data is data relating to an individual who is or can be identified either from the data or from the data in conjunction with other information.

4.5.1. NHSMail is a secure national email service run centrally by NHS Digital for the NHS and is protected to pan-government secure email standards. This ensures that sensitive and confidential information is kept safe. This is achieved by the encryption of messages during transmission, which ensures that the message cannot be intercepted, read or tampered with during transmission.

4.5.2. NHSMail is the only email service DBTH staff may use to exchange personally identifiable and or confidential information.

4.5.3. All emails sent between NHSMail accounts or trusted email domains documented in the NHSMail **Acceptable User Policy Section 4** are encrypted and secure.

4.5.4. Any emails sent to domains not listed in the NHSMail **Acceptable User Policy Section 4** must be encrypted using the NHSMail encryption tools. This secure

service facilitates communication across secure and non-secure email service providers.

- NHS Digital has produced detailed guidance on the use of this service for both senders and recipients, the guidance that is available through the NHSMail Portal Help pages. https://portal.nhs.net/Help/policyandguidance

- Encryption Guide for NHSMail https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/encryptionguide.pdf
- Accessing Encrypted Emails Guide for Non-NHSMail users https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/Accessing+Encrypted+Emails+Guide.pdf

4.5.5. If staff receive emails containing Patient Identifiable Data (PID) via a non-approved email account (as listed in the NHSMail Acceptable Use Policy Section 4), they should make best efforts to inform the sender so that they may amend their records and cease the use of insecure transmissions.

4.5.6. The Trust utilises 'shared mailboxes' where several members of staff are granted access based on business requirements. These are utilised by both clinical and non-clinical teams to improve business efficiencies and reduce the risks associated to delays in a response or action being taken.

- A rota for checking the Shared mailbox Inbox must be put in place by the local Manager.
- The local manager is responsible for ensuring that the access to the shared mailbox is accurate through regular review of and must inform the shared mailbox owner of any changes required, such as adding additional users or removing users.

4.5 Clinical Use of Email

4.6.1. All clinical staff members are individually responsible and accountable to their registration body for their conduct with regard to record keeping. Staff must follow the Standard Operating Procedure for the appropriate electronic patient record.

4.5.1 Any email communication about a patient either between clinicians/practitioners/ admin support staff, or the patient themselves, and/or their carers must be recorded in the patient's clinical record. This includes:

- Email conversations regarding the delivery of care, details of any appointments, or changes to appointments.
- Emails regarding the patient with other agencies/individuals involved in the delivery of care.

- Emails received from carers; or other significant people involved in the care of the patient.
- Emails from clinicians/practitioners/admin support staff to and from the patient.

4.5.2 If the patient has an electronic record, then the clinically relevant content of the email must be copied and pasted into the record. Copied information must include the date and time of the original email(s), sender and recipient(s), as well as the date/time entered into the electronic care record.

4.5.3 If the clinical record is paper, the clinically relevant content of the email must be printed out and filed in the record.

4.5.4 It is the responsibility of each clinician/practitioner/admin support staff to review the content of the email trail to ensure:

- Only clinically relevant information is copied into the patient's electronic record.
- All 3rd party information (that is not relevant to the patient and/or their care) is removed before the content of the email is copied into the patient's record.
- Each clinician/practitioner/admin support staff is responsible for ensuring that the right information gets into the right patient's record.
- Once the clinician/practitioner/admin support staff has ensured that the patient's clinical record is up to date and accurate, the emails should be deleted from their personal in-box.

4.5.5. If staff receive emails containing Patient Identifiable Data (PID) via a non-approved email account (as listed in the NHSMail Acceptable Use Policy Section 4), they should make best efforts to inform the sender so that they may amend their records and cease the use of insecure transmissions.

4.5.6. The Trust utilises 'shared mailboxes' where several members of staff are granted access based on business requirements. These are utilised by both clinical and non-clinical teams to improve business efficiencies and reduce the risks associated to delays in a response or action being taken.

- A rota for checking the Shared mailbox Inbox must be put in place by the local Manager.
- The local manager is responsible for ensuring that the access to the shared mailbox is accurate through regular review of and must inform the shared mailbox owner of any changes required, such as adding additional users or removing users.

4.6 Clinical Use of Email

4.6.1. All clinical staff members are individually responsible and accountable to their registration body for their conduct with regard to record keeping. Staff must follow the Standard Operating Procedure for the appropriate electronic patient record.

4.6.2 Any email communication about a patient either between clinicians/practitioners/ admin support staff, or the patient themselves, and/or their carers must be recorded in the patient's clinical record. This includes:

- Email conversations regarding the delivery of care, details of any appointments, or changes to appointments
- Emails regarding the patient with other agencies/individuals involved in the delivery of care
- Emails received from carers; or other significant people involved in the care of the patient
- Emails from clinicians/practitioners/admin support staff to and from the patient

4.6.3 If the patient has an electronic record, then the clinically relevant content of the email must be copied and pasted into the record. Copied information must include the date and time of the original email(s), sender and recipient(s), as well as the date/time entered into the electronic care record.

4.6.4 If the clinical record is paper, the clinically relevant content of the email must be printed out and filed in the record.

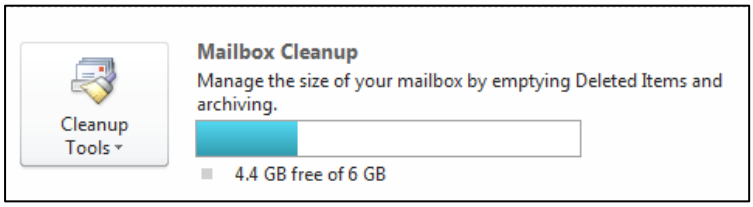
4.6.5 It is the responsibility of each clinician/practitioner/admin support staff to review the content of the email trail to ensure:

- Only clinically relevant information is copied into the patient's electronic record.
- All 3rd party information (that is not relevant to the patient and/or their care) is removed before the content of the email is copied into the patient's record.
- Each clinician/practitioner/admin support staff is responsible for ensuring that the right information gets into the right patient's record.
- Once the clinician/practitioner/admin support staff has ensured that the patient's clinical record is up to date and accurate, the emails should be deleted from their personal in-box.

4.7 Quotes/Retention

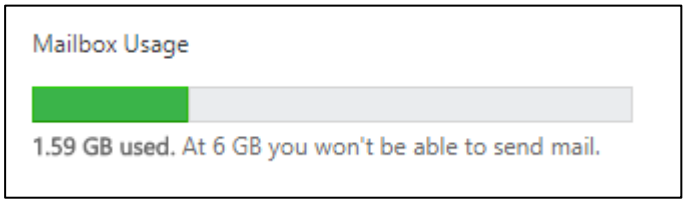
4.7.1. Please refer to the NHS NHSMail: Data Retention Policy on the NHSMail Portal Help pages. https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/Data+Retention+Policy+2017.pdf

- Outlook – Click 'File'. Under the heading 'Mailbox Management' you will see your mailbox allocated size and current usage.



- Outlook Web Application (OWA) – click the settings icon (cog), then select Options. Under the 'Mailbox Usage' you will see your mailbox allocated size and current usage.

OWA settings icon



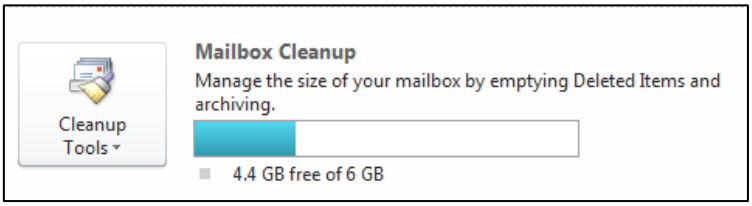
4.7.2. The standard mailbox quota for NHSMail is 4Gb, this will be given to all email users. Should an individual require a larger mailbox a request must be sent by the General Manager or department Executive.

4.7.3 Larger mailboxes will only be supplied to individual users who can provide evidence of effective mailbox management.

4.8 Mailbox Management

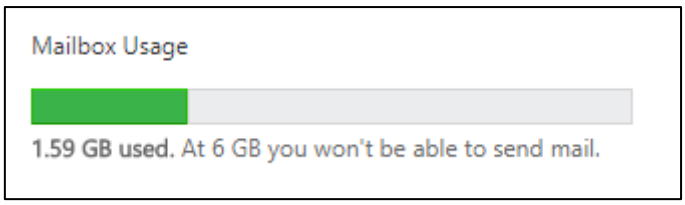
4.8.1. All staff should keep the amount of email in their inbox to a minimum – email is a communication tool and is not suitable or appropriate for long term file storage.

- Outlook – Click 'File'. Under the heading 'Mailbox Management' you will see your mailbox allocated size and current usage.



- Outlook Web Application (OWA) – click the settings icon (cog), then select Options. Under the 'Mailbox Usage' you will see your mailbox allocated size and current usage.

OWA settings icon



4.8.2. Delete[2] emails after reading, response or action, (unless you need to save them to a shared or personal folder). Retention of unnecessary messages uses valuable disk space and results in additional costs.

4.8.3 Only email messages that are records of Trust business activities should be saved. Emails that you need to keep should not be stored in Outlook (or other email services). In the same way that you would keep all paper records relating to one subject in the same file within a filing cabinet, all electronic records relating to a particular subject should be stored together in an appropriately named folder(s) on shared network drives (see Guidance for managing electronic records).

4.8.4 Most email messages form part of an email 'conversation' string. Where an email string is formed as part of a discussion it is not necessary to save each new part of the 'conversation', i.e. every reply. Email strings should be saved as records at significant points during the 'conversation' as it is not always apparent when the 'conversation' has finished.

4.8.5 Review saved emails (and other file types) every month and delete the ones that are no longer required.

4.9 Use of Email Purposes Not Related to Work

4.9.1. NHSMail does not permit the use of an NHSMail account for personal non-work related reasons.

4.10 Unacceptable Use of Email

The following is not an exhaustive list but is an indication of the types of misuse that may be regarded as serious misconduct. Users must not use email for any of the following:

[2] NHS Trusts have been advised by NHS Providers that any emails or indeed any other correspondence associated with COVID-19 must not be deleted in line with instructions associated with the National COVID-19 Public Enquiry expected to begin in the spring of 2022

4.10.1. The transmission of any offensive, obscene or indecent images, data or other material.

4.10.2. The transmission of material, which is likely to cause annoyance, inconvenience or needless anxiety.

4.10.3. The transmission of abusive, sexist, terrorist or illegal or politically extreme organisations, racist or defamatory material.

4.10.4. The transmission of material such that this infringes the copyright of another person.

4.10.5. The transmission of unsolicited commercial or advertising material.

4.10.6. Deliberate activities with any of the following characteristics:

- Wasting staff effort or network resources, including the effort of staff involved in the support of those resources (this includes broadcasting trivial emails to all network users without prior permission).
- Corrupting or destroying other users' data.
- Disrupting the work of other users.
- Using email in a way that denies service to other users.
- Introducing unauthorised software or hardware, and misuse of email, such as the introduction of viruses or malicious code etc.
- Obtaining unauthorised access to the Trust or another organisation's IT facilities.
- Providing email addresses to commercial companies inappropriately.
- Expressing personal views which could be misinterpreted as those of the Trust.
- Committing the Trust to purchasing or acquiring goods or services without proper authorisation.
- Accessing confidential information without proper authorisation.
- Using NHSMail for any fraudulent purposes – Concerns in regard to fraud, bribery or corruption must be reported without delay and in accordance with CORP/FIN 1 (D) to the Local Counter Fraud Specialist or via the NHS fraud line on 0800 0284060 (https://cfa.nhs.uk/reportfraud)

4.10.7. You must be able to justify your use of email and the time spent on this to a Trust senior manager if challenged to do so.

4.11 Emailing Service Users

4.11.1 Where there is a request by a service to communicate using email this consent should be recorded and attached to the patient's record.

4.11.2 Where possible email communication to a service user should be done securely using the NHSMail [secure] encryption functionality. Once an email has been

received by a service user from an NHSMail account then the service user may use the service to securely respond to the sender.

4.11.3 Staff should encourage the use of the secure NHSMail encryption functionality in all instances, although where a service user is reluctant to use the service then the risks associated with insecure transmission of data must be fully explained and accepted by the service user. If the service user understands the risks and is willing to accept those risks, then this should be documented within the service user's health records.

4.11.4 Please refer to the NHSMail email encryption and links to guidance documents as detailed in Section 4.5.4.

4.11.5 Any requirement to send information to more than external addressee in a single Email should be done via the 'Blind Carbon Copy' (Bcc) option; unless there has been explicit consent to share Email addresses. This is of particular relevance where Email addresses are in a distribution list.

- In some cases where the external addresses are NHS employees working in partnership with us, it may be appropriate to use 'To' and 'Carbon Copy' (Cc)

4.12 Starters and Leavers

4.12.1 The IT Service Desk must be notified of:

- All new starters in advance of their start date and if they have an existing NHSMail account on the New Starter web form to ensure that an email account is created appropriately.

- All leavers from the organisation. NHSMail accounts are transferred with the user should they join another NHS organisation, where the account is not allocated to a new organisation within 30 days this is deleted. Refer to NHSMail Information Management Policy for up-to-date retention periods.

- Access to Shared mailboxes and other staff mailboxes will remain as the email address is transferred with the user. The email address will also remain in static distributions list. Line Managers are responsible for notifying the Owners of Shared Mailboxes and Distribution list where the individual should no longer have access to the contents.

- Individuals must notify the IT Service Desk if they believe that they have inappropriate access to Shared Mailboxes and or other staff mailboxes.

- All staff who are on Long Term Leave including Maternity, Sabbaticals etc. so that their NHSMail account be disabled and re-enable upon their return to work, ensuring that their NHSMail account is not centrally deleted by NHS

Digital, due to inactivity. The NHSMail account can be re-enable up to 18 months after it is disabled, after which time the staff member will be allocated a new NHSMail account upon returning to work.

4.13 Monitoring Usage

4.13.1. NHSMail will monitor usage of the email account as described in the NHSMail Acceptable Use Policy (AUP). A copy of the current version can be found at https://portal.nhs.net/Home/AcceptablePolicy

4.13.2. All users should monitor and manage the size of their mailbox as detailed in 4.8.1.

5. TRAINING/SUPPORT

All staff members are required to complete Information Governance Training on an annual basis.

Please note: The training requirements of staff will be identified through a learning needs analysis (LNA). Role specific education will be co-ordinated/ delivered by the topic lead. Alternatively, training may be accessed via an approved e-learning platform where available.

5.1 NHSMail and Outlook

5.1.1. NHSMail users should make use of the guides available on the NHSMail portal when utilising the Web access. http://support.nhs.net/

5.1.2 Outlook users should make use of the training guides available on the IT Training Intranet page. http://intranet/education_and_development/IT_Training/NHSMail/NHSMail_Training_Page.aspx

6. MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
NHSMail monitor email and Skype for Business in line with their policies.	NHSMail	In line with their policies.	Issues and Incidents are reported to the Trust
The allocation of larger mailbox over the standard allocation.	IM&T department	Bi-annually	Reports produced via NHSMail and financial expenditure by care group / department

7. DEFINITIONS

IM&T	Information Management & Technology
NHSMail	The email service provided by Accenture in conjunction with NHS Digital on behalf of NHS England
P&OD	People and Organisation Development
SPAM	Email spam, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email.

8. EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment for All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 1)

9. ASSOCIATED TRUST PROCEDURAL DOCUMENTS

This policy is not directly associated to any other Trust Policies; however you should familiarise yourself with:

- CORP/ICT 2 - Information Management and Technology (IM&T) Security Policy
- CORP/ICT 28 – Internet Usage Policy.
- CORP/EMP 4 – Fair Treatment for All Policy
- CORP/EMP 27 – Equality Analysis Policy
- CORP/FIN 1 (D) – Fraud, Bribery and Corruption Policy & Response Plan

10. DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

11. REFERENCES

The following resources/guidelines have been used in the developments of this policy:

- Data Protection Act 2018
- Computer Misuse Act 1990
- UK GDPR 2021
- Freedom of Information Act 2000
- Records Management: NHSx Code of Practice 2020

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Email and Internal Communications	All Staff	Roy Underwood	Existing	December 2021

1) Who is responsible for this policy? Name of Division/Directorate: IG Committee

2) Describe the purpose of the service / function / policy / project/ strategy? Who is it intended to benefit? What are the intended outcomes? Trust Policy

3) Are there any associated objectives? Legislation, targets national expectation, standards: N/A

4) What factors contribute or detract from achieving intended outcomes? – No

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? Details: [see Equality Impact Assessment Guidance] - No

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation] –

6) Is there any scope for new measures which would promote equality? [any actions to be taken] No

7) Are any of the following groups adversely affected by the policy? No

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form – see CORP/EMP 27.

Date for next review: **November 2024**

Checked by: **David Linacre** **Date:** **December 2021**