Sherwood Forest Hospitals
NHS Foundation Trust

Email Guidance

Document Category:	**INFORMATION GOVERNANCE**
Document Type:	**STANDARD OPERATING PROCEDURE**

Keywords:	How to manage emails

Version:	**Issue Date:**	**Review Date:**
1	August 2018	August 2020

Supersedes:	Not applicable		
Approved by (committee/group):	Information Governance Committee	**Date Approved:**	August 2018

Scope/ Target Audience: (delete as applicable / describe)	**Trustwide**

Evidence Base/ References:	NHS Digital

Lead Division:	Corporate Services
Lead Specialty:	Information Governance
Author:	Information Governance Manager
Sponsor:	Chief Executive

	Name the documents here or record not applicable
Associated Policy	Email and Internet Policy
Associated Guideline(s)	
Associated Procedure(s)	
Associated Pathway(s)	
Other associated documents e.g. documentation/ forms	

Consultation Undertaken:	Information Governance Working Group

Template control:	v1.3 January 2018 (Supports the Trust's 'Policy for Policies')

Contents

NHSmail Account Management for Managers (Frequently Asked Questions)[1]

This document is designed to support managers with the process of managing NHSmail accounts for staff. NHS staff are permitted to have one publicly funded email account.

1. New Member of Staff

NHSmail accounts are transferrable between organisations. When a new member of staff is appointed it is therefore important to find out if they already have an NHSmail account before you request one from the Nottinghamshire Health Informatics Service desk.

1.1. How do I check if someone has an NHSmail Account?

You can check for an existing NHSmail account on the NHSmail Portal using People Finder, alternatively you can search in the NHSmail global address list. Often the best approach is to ask the individual if they have an NHSmail account.

1.2. I have a new member of staff that needs an NHSmail Account, how do I get one set up?

A new NHSmail account should be requested via the Nottinghamshire Health Informatics Service desk using the Nottinghamshire Health Informatics Service portal. At the top of the page access **IT Accounts** and select **Request a New Account.**

On completion of the form you will be provided with a call reference number, when the account has been created you will be notified by email. The mailbox owner will need to call

[1] This NHSmail Account Management for Managers was written by Helen Ben-Fredj, Nottinghamshire Health Informatics Service.

the Nottinghamshire Health Informatics Service desk and quote the call reference number to obtain the account details.

Please note the password on a newly created NHSmail account expires if the account is not activated within 30 days.

1.3. I have a new member of staff with an existing NHSmail account, what do I need to do?

Before Nottinghamshire Health Informatics Service can add this email account to your Trust the previous organisations IT service desk will need to mark the NHSmail account as a leaver, please advise the individual that if this hasn't already been done they need to action this before commencing their new role in the Trust.

When the account has been marked as a leaver by the previous organisation, log into the Nottinghamshire Health Informatics Service portal and in the **IT Accounts** section select **Amend an Account.**

Complete the form and in the **Optional** field at the bottom of the form add the existing NHSmail address. The service desk will join the account to the Trust.
N.B If the user cannot remember the contact details of their previous IT department they should contact the NHSmail service desk and log a call for their account to be marked as a leaver. Please see section 4.3 for contact details.

2. Long Term Absence

If an NHSmail account password is not changed within 90 days the account will be disabled, after a further 90 days the account is deleted. Email accounts for staff on long-term absence (e.g. maternity leave) need to be managed to ensure they are not deleted as part of this automated inactive account deletion process.

2.1. I have a member of staff on long-term absence, what do I need to do?

Log into the Nottinghamshire Health Informatics Service portal and in the IT Accounts section select Delete an Account (you are not deleting the account). Enter the individual's name, Select the NHSmail 2 button then select continue.
Complete the details section and in the drop-down box for 'Type of Leaver' select 'Disable the account'. This will hide the account from the address book, prevent the user from logging into the account, and keep the account available to be activated by the Nottinghamshire Health Informatics Service desk for 180 days.

2.2. A member of staff has returned from long-term absence, what should I do?

Contact the Nottinghamshire Health Informatics Service desk on 01623 410310 (Mitel 4040) and ask for their account to be enabled. If the individual requires a password re-set, they will need to contact the service desk personally.

If the account has not been enabled for over 180 days Nottinghamshire Health Informatics Service will need to contact the national service desk with a request to re-instate the account.

3. Amending an Account

If a member of staff changes their name, job role or phone number the Nottinghamshire Health Informatics Service desk should be contacted to amend the account.

3.1 How do I amend an NHSmail account?

All staff are able to add and amend contact numbers linked to their NHSmail account, this is done by logging into the NHSmail Portal and BEFORE logging into email, select the **'Profile'** link on the blue banner at the top of the page, from here you will be able to add and remove phone numbers.

All other account changes e.g. name, job role and organisation, must be carried out by the service desk. Log into the Nottinghamshire Health Informatics Service portal and select **IT Accounts,** select **Amend an Account, c**omplete and submit the changes form.

3.2 I have changed my name; will amending this change my email address?

The service desk can amend your name on your email account by following the steps in section 3.1. The old email address, with your previous name, will be held in the NHSmail portal, which means any emails sent to your previous email address will be automatically forwarded to your new email address.

4. NHSmail Account Terminations

When a member of staff leaves, it is important that the NHSmail account be removed from your organisation promptly.

4.1. A member of staff is leaving the NHS what do I need to do?

Log into the Nottinghamshire Health Informatics Service portal, select the **IT accounts** section and then select **Delete an Account**; this will open a leaver form.

Complete the form and at the end select in the type of leaver drop down box **Mark as Leaver**. As the email account will not be 'joined' to another NHS organisation, the account will be permanently deleted after 30 days.

4.2. A member of staff is leaving to work at another NHS organisation, what do I need to do?

Log into the Nottinghamshire Health Informatics Service portal, select the **IT Accounts** section and then select **Delete an Account**, this will open a leavers form.

Complete the form and in the type of leaver drop down box **Mark as Leaver**. The account can then be ‘joined’ to the new NHS organisation by their IT service desk. They have 30 days in which to do this before the account is disabled.

4.3. I want the emails created while in my organisation removing from a leavers account, what do I need to do?

Firstly, you need to manage the account exactly as in point 4.2 above. For the emails in the account to be deleted a call will need to be logged with the national service desk (Nottinghamshire Health Informatics Service are unable to delete data within email accounts). The National NHSmail Helpdesk can be contacted on 0333 200 1133 or helpdesk@nhs.net.

How to correctly manage your emails

Email Principles

- Do not forward confidential email correspondence without acquiring permission from the sender first (where permission is given, ensure the email is sent securely); when forwarding emails containing confidential information staff have a duty to ensure that they are not inadvertently disclosing information to inappropriate recipients
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's account.
- Do not breach copyright or licensing laws when composing or forwarding email and email attachments.

Trust email accounts irrespective of how they are accessed (Trust/non-Trust devices) are intended for business use in support of the Trust's objectives. Accordingly, all email accounts and email transmission residing on the Trust's computing and networking facilities are the property of the Trust and contain potentially official/corporate records. This includes emails and attachments created by staff or individuals conducting Trust business as part of their work.

Any emails received in error having been misdirected should be deleted and the sender notified of the error. Misdirected emails must not be disclosed. For the purposes of this policy 'misdirected' includes any mail sent to an individual in relation to a post which he/she no longer occupies.

Appropriate Email Content – Legal risks and Considerations

Email is a business communication tool and users are obliged to use it in a responsible, effective and lawful manner.

Email content is admissible in a court of law as evidence where it would be treated in exactly the same way as verbal or written statements. Business email correspondence should be written in the same context and style as a signed letter. It is important to consider if email is the most appropriate way to convey the information, for example if a message needs to be passed onto a person in the same office speaking to them face to face might be more productive, particularly if they receive large volumes of email.

Emails that contain information about a living, identifiable person (personal information), are subject to the requirements of Data Protection Legislation.

NHS email records are Public Records under the terms of the Public Records Act 1958 and may be subject to a request for information under Data Protection Legislation and the Freedom of Information Act 2000. It is therefore the Trust's intention to ensure that they are lawfully managed to protect patients, and the Trust's rights, liability and reputation.

Emails are records and can be requested under the Freedom of Information Act, to which the Trust has a legal duty to respond to the Freedom of Information Act and this includes information held in non-work personal email accounts (e.g. Hotmail, Yahoo and Gmail), where they relate to the official business of the Trust. The Trust reserves the right to ask staff to search their personal email accounts for such information, where the Trust might be required to ask an individual other than the member of staff to search for information, such requests and the outcome of the findings will be documented to demonstrate, if required, that appropriate searches have been made in relation to a particular request. The content of NHSmail email accounts linked to Trust staff is also searchable and disclosable. Where a search of NHSmail email is required, the Trust will follow the process as outlined in the Subject Access Policy.

The wide range of information available and the nature of the internet and email systems raise concerns about security, integrity, confidentiality, monitoring and proper conduct. Inappropriate use of these can cause problems ranging from minor distractions up to and including legal claims being made against an individual member of staff or user and/or against the Trust if a national or international law is violated.

Managing email correspondence

Staff are responsible for the appropriate management of their email correspondence. In order to do this, staff need to distinguish emails (sent and received) that are records of their business activities from short-lived email messages that do not need to be kept. It is important that email correspondence that constitutes business records are moved out of mailboxes, and managed in the same way as other records.

What constitutes an email record?

Whenever an email is sent or received a decision must be made about whether the email needs to be kept as a business record. You should be able to determine if email correspondence is a record using the following questions:

- The email proves that a business related event or activity did or did not occur.
- The email demonstrates a transaction e.g. what was purchased or sold, for how much, in what quantity, when it was delivered or where it went. Even if the email only records some of such information, it is still a business record; however staff are reminded that emails are not contractually binding and should not be used in place of formal Trust approved processes.
- The email identifies who participated in a business activity or had knowledge of the event. (All address lines To, From, Cc, and Bcc, are equally important).
- The email has legal or compliance value.
- You need the email to support facts upon which you have based a business decision.

As email correspondence can be sent to multiple recipients, there are general guidelines which can help to indicate ‘who’ is responsible for capturing an email as a record:

- For **internal** email correspondence, the **sender** of an email, or initiator of an email dialogue that forms a string of email correspondence
- For correspondence **sent externally**, the **sender** of the email message
- For **external correspondence received** by one person, **the recipient**
- For **external correspondence received by more than one person**, the **person responsible for the area of work** relating to the message e.g. a project manager, initiative lead, committee administrator etc. If this is not clear it may be necessary to clarify who this is with the other people who have received the email.
- If in doubt, the safest action is to retain a copy yourself.

The standard size of email mailboxes is limited and it is the responsibility of the individual to fulfil relevant 'housekeeping' activities to stay within that limit. Once mailbox limits are reached, staff will be unable to send emails until their mailbox is brought within the specified limit.

The sending of large files (2MB or more) as attachments should be avoided where possible, if necessary they should be in a compressed format (i.e. as 'zip' files). The size limit for a sent email is 10MB.

Emails containing personal confidential data

Email correspondence containing personal information about a living individual is subject to the Data Protection Legislation and must be treated in line with the principles outlined in the Act. Under the Data Protection Legislation, personal information includes opinions about an individual or the personal opinions of an individual. Email correspondence containing this type of information should only be used for the purpose for which the information was provided, be accurate and up to date, transmitted securely and must not be disclosed to third parties without the express permission of the individual concerned.

Consideration must be given to the suitability of using email as a method to convey personal confidential data (or other confidential information).

The transfer of personal confidential data including clinical information to staff personal non NHSmail email accounts i.e. yahoo.co.uk, hotmail.com, ntlworld.com, doctors.net.uk and other such email services provided by internet service providers, is unacceptable.

The use of the auto-forwarding functionality in Outlook is not allowed as this creates an increased risk of sensitive emails being forwarded to email accounts which might not necessarily be authorised to receive such communication or the email being communicated insecurely.

Precautions must be taken to ensure a confidential email is only sent to the intended authorised recipient by:

(a) accurately selecting the recipient's email address from an established directory e.g. Global address list or equivalent, making sure the addressee is correct – take extra care when using 'auto-complete' functions;
(b) by sending a test email and requesting confirmation of receipt before sending the confidential information (Safe Haven procedures);
(c) taking care that only appropriate addressees are included when using 'reply to all' and 'forward';
(d) personal data is not contained in the subject line of the email.

Email communication with patients

Email should not normally be used to establish a patient-clinician relationship. Rather, it should add to and follow other, more personal encounters, when the patient has given permission to communicate with them by email.

Where a patient/carer has asked (and subsequently consented) to be communicated with via email it is advised that the patient is asked to email their request to the consultant/secretary etc. to verify their email address, before any correspondence takes place. A copy of this email should be placed in the patient's record and any correspondence must be sent encrypted using the following instructions: http://www.mansfieldandashfieldccg.nhs.uk/media/26871/email-guidance-for-non-nhsmail-recipients-version-21.pdf

Managing emails during staff absence

Staff should make arrangements for their emails to be managed during planned absences and use the Out-of-Office message facility to advise contacts of their unavailability this should include when they are next available and alternative contact details for example a colleague in the department. Staff on secondment or other planned long term absence should contact the Nottinghamshire Health Informatics Service helpdesk to make special arrangements.

However, there may be occasions when it is necessary to access business email correspondence in an individual's mailbox when they are away from the office for an extended period, e.g. due to sudden illness or failure to make adequate arrangements for planned absences.

In these situations, it may not be possible to ask the permission of the member of staff whose mailbox needs to be accessed; the procedure for gaining access to a member of staff mailbox in such circumstances is to:

- Gain the Head of Department / Line Managers authorisation

Submit a request to the IG Team, completing the Approval For Staff Monitoring / Audit Data (see appendix 3)

- Only one person who is senior to the absent employee should be authorised to gain access with limited time restriction
- Access must be kept to a minimum on a strict need-to-know basis

- An Out-of-Office message is set up to alert subsequent contacts of the unavailability of the addressee which should include an alternative contact in their absence
- Inform the person whose mailbox was accessed as soon as it is practical to do so.

Authorised access to another person's Inbox may be provided for the continuation of business purposes only, and access must be justified as a business purpose and kept to a minimum to meet that need. Emails that are clearly personal communications must not be accessed under any circumstances where such access is granted during staff absence.

Examples include:

- Subject Access Requests made under Data Protection Legislation
- Freedom of Information requests
- Evidence in legal proceedings
- Evidence in a criminal or other internal investigation
- Line of business enquiry or other information relevant to the Trust.

Advice must be sought from the Information Governance team where there are believed to be grounds for accessing someone else's personal emails.

Nottinghamshire Health Informatics Service acting on behalf of the Trust, reserves the right to inspect the content of an email, including personal emails, if there is credible reason to believe that it contains evidence of unlawful activity, including instances where there may be a breach of policy constituting gross misconduct, or where there is reason to believe that it contains harmful material e.g. a file containing a virus, or where the law requires it.

NB: It is less likely that this procedure will need to be followed if email records are managed appropriately or mailbox access has been delegated to a trusted third party.

Management of Public and Shared Mailboxes

In the case of shared mailboxes, management is likely to be shared between everyone who has access. And for public mailbox folders, the identified folder owner is responsible for its management, including content and managing who has access to the folder, taking into account transfers/leavers. The purpose of managing email, whether in a shared mailbox or in public folders is to identify emails that should be retained as a record of an activity and delete short-lived messages.

It is not always the person for whom the email is intended who opens an email; for example secretaries, personal assistants and admin staff may all be responsible for managing public and shared email in-boxes. Share and Public mailboxes and their associated calendars should not be used to manage patient attendance and information, patient information and attendance should be recorded in the appropriate hospital system.

Managing your Mailbox

Staff should follow the methodology that works best for them in order to manage their email box effectively. Recommended approaches are:

- Allocating sufficient time each day or week to read through and action email correspondence
- Prioritising which email correspondence need to be dealt with first (a priority may be set by the sender)
- Looking at the sender and the title to gauge the importance of the message
- Flagging where you have been ‘cc’d’ into email correspondence. These correspondence are often only for informational purposes and do not require immediate/any action
- Setting rules for incoming correspondence so they can automatically be put into folders
- Using folders to group email correspondence of a similar nature or subject together so they can be dealt with consecutively
- Identifying email correspondence that are records or need to be brought to other people’s attention
- Keeping email correspondence in personal folders only for short-term personal information. Emails that are required for longer purpose should be managed as records
- Deleting email correspondence that are kept elsewhere as records
- Deleting email correspondence that are no longer required for reference purposes from the in and out box.

Giving Permissions to your Outlook Inbox, Calendar or Contacts

All email accounts or mailbox users’ are responsible for the conduct and content of their mailbox. The Trust recognises that there are situations where staff may need to share the contents of either their inbox, calendar or contacts with colleagues and it is possible to formally share or delegate a selection of diary and e-mail functions while maintaining accountability.

Where an account holder uses his/her email account to communicate personal/sensitive data, any ‘Read’ access should only be granted to colleagues who have a legitimate reason to access such communication (consultants, medical secretaries etc.). ‘Create’ access should be used with great care owing to the risk of impersonation. The email account holder is responsible for updating access rights as staff move or leave, and will be accountable in the event of any breaches arising from inappropriate access rights being granted.

Email Etiquette

Although email messages can be sent and delivered quickly there may be circumstances where email transmission can be subject to unexpected and/or undetected delays. Confirmation of delivery and read receipts can be set when sending an email (via the Options facility of Outlook) so the sender can keep track of its progress, however, where information needs to be communicated as a matter of urgency or an urgent response is required it may be better to use the telephone and send an email confirmation if it is deemed to be necessary.

The ability to send an email to everyone at the Trust is restricted to limited staff within Nottinghamshire Health Informatics Service and the Communications Team. If a message needs to be conveyed to everyone in the Trust an email should be sent to the

Communications Team requesting that they send an email to everyone detailing the nature of the information and providing a link to the appropriate point on the Intranet. It should be noted that only email correspondence that are considered to be of immediate interest to the majority of staff at the Trust will be sent to everyone.

- Emails should be created in a standard format using typeface Arial and an 11 point font in NHS black or NHS blue.
- There should be no backgrounds or animations included.
- A template signature should be used that includes as a minimum, the sender's full name, job title, Trust name, department and full contact details - telephone, email and fax; images should not be used in email signatures.
- Staff should not reflect views of Trust unless authorised to do so.
- Staff should not accept or endorse suppliers/ products unless authorised to do so.
- Staff should not be political in any view.
- Do not write in capitals (this is viewed as shouting).
- Answer emails quickly – (this is the whole point of the system).
- If responding to an email in another language other than English only bona fide translators should be used – Accessible through PETS.
- Corporate approved disclaimers and notices only should be used.
- Use a spell checker prior to sending an email.
- Regularly empty the 'Deleted Items' folder in your email.
- Email correspondence that contains information that is not supported by fact should indicate that it is the sender's opinion that is being expressed.

When writing an email the following conditions must be met:

- Any behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in email correspondence
- Care should be taken when composing email correspondence to ensure they are inoffensive and cannot be construed as harassment
- The impersonal nature of email correspondence can mean that it is easier to cause offence than when speaking. If you are annoyed or angry about something take time to ensure the message does not inflame the situation
- Email correspondence containing inaccurate information in the form of opinion or fact about an individual or Trust, may result in legal action being taken against the person sending the email message and anyone forwarding the email message on to others.

Consider:

- What information you are sending and to whom (i.e. is this the right audience)?
- Is it appropriate or suitable to use the 'Reply All' function in Outlook; if your response will be crucial to know for the original sender and a few other recipients, simply copy their addresses from the original email
- If sending attachments, consider the file size to make sure you don't fill the recipients inbox (send a link to the file instead)

Email Retention & Archiving

A record of email sent and received on the Trust's email system will be retained for a maximum of 6 years. Emails may be put into archive storage at any point before this time so server space can be appropriately managed. This archive is independent of the users housekeeping activities including deleted message. Access to and retrieval of archived email messages will only be authorised in exceptional circumstances by the IG Team. Users are required to identify and save important emails that are business 'records' and need longer term preservation on shared or home directory/drive . See 6.1.1

Email System Monitoring

The Trust will ensure compliance with the various laws that apply to electronic communications. This includes ensuring monitoring systems are in place for back-up purposes and to protect the security and integrity of the Trust's IT and email systems.   All email traffic (incoming and outgoing) is logged automatically with backup copies of email logs kept by the Nottinghamshire Health Informatics Service department and audited periodically.

The Trust deploys a tool that automatically scans email content and intercepts and blocks the transmission of incoming and outgoing emails if harmful content is detected "Harmful" covers a variety of suspicious contents including viruses or similar and inappropriate material. Harmless material may also get blocked inadvertently. Where an email message is blocked, the sender will be notified of the blocked transmission via an automated email. It is the sender's responsibility to follow the procedure set out in the email to unblock that transmission where it is appropriate. Staff should also exercise due care when opening attachments contained in emails, especially if they are from a source not known to them.

The Trust reserves the right to audit and investigate any usage which impacts on the effectiveness, efficiency or security of the network or as required to meet legal and statutory obligations. Additionally, the Trust reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action, where unlawful activity or gross misconduct is detected through these monitoring processes.

In the event of a serious incident relating to fraud, corruption or other serious crime, a referral may be made to NHS Counter Fraud Services or the police for investigation.