Ashford and St. Peter's Hospitals
NHS Foundation Trust

POLICY FOR THE USE OF EMAIL (NHSmail)

Author: **Head of IT**

Executive Lead: **Simon Marshall Director of Finance and Information**

Status: Approval date: July 2017

Ratified by: Information Governance Steering Group

Review date: March 2022

History

Issue	Date Issued	Summary of Change	Author
1	Dec 1999	Initial issue	N/K
2	Jun 2004	Policy revised	Management Board
3	Feb 2006	Updated	Director of Information
4	Jun 2006	Updated	Director of Information
5	Sep 2007	Updated	Director of Information
6	Oct 2008	Updated	Director of Information
7	Jul 2010	Updated	Information Governance Steering Group
8	6 Nov 2014	Reformatted to new format	Head of IT
9	Feb 2017	Updated to reflect migration to NHSmail	NHSmail Project Manager
10	March 2017	Updated	Information Governance Manager
11	July 2017	Updated to expand upon Best Practice	Information Governance Manager
12	Dec 2018	Updated to expand: Section 1 - 8 Added full Trust Disclaimer to section 6	Head of IT
13	Jan 2019	Updated: Section 13 Updated: Author	Head of IT
14	March 2019	Added and Updated various sections **6, 6.2, 6.5, 6.9, 6.13, 13**	Head of IT
15	May 2019	Updated disciplinary terms used in sections **4, 5, 6, 13**	Assistant Director of HR, Corporate Services

For more information on the status of this document, please contact:	
Policy Author	Head of IT
Department/Directorate	Digital Services / Finance
Date of issue	July 2017
Review due	May 2022
Ratified by	Information Governance Steering Group
Audience	All staff

Executive summary

This policy sets out the framework for the protection of the confidentiality, integrity and availability of the email system and establishes the Trust and user responsibilities for the system.

1. Introduction

1.1. This document defines the Email Policy for Ashford & St Peter's Hospitals NHS Foundation Trust

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

2. Scope

2.1. This guidance is relevant to all staff groups.

3. Purpose

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

3.2. The objective of this policy is to ensure the security of the Trust's email system. The Trust will:

- **Ensure Availability**

  Ensure that the email system is available for users.

- **Preserve Integrity**

  Protect the email system from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets.

- **Preserve Confidentiality**

  Protect assets against unauthorised disclosure.

4. Explanation of Terms Used

4.1. **Defamation & libel**

What is defamation & libel?
A published (spoken or written) statement or series of statements that affects the reputation of a person (a person can be a human being or an organisation) and

exposes them to hatred, contempt, ridicule, being shunned or avoided, discredited in their trade, business, office or profession, or pecuniary loss. If the statement is not true, then it is considered libellous and the person towards whom it is made has redress in law.

What you must not do
Make statements about people or organisations in any email that you write without verifying their basis in fact. Note that forwarding an email with a libellous statement also makes you liable.

What are the consequences of not following this policy?
The Trust may be subject to legal action and you may personally be subject to legal action if it is determined that you acted without Trust authority. Failure to follow the policy may result in disciplinary action against you in accordance with the Trust's Disciplinary Policy.

4.2. Harassment

What is harassment?
Harassment may be defined as "any conduct based on age, sex, sexual orientation, gender reassignment, disability, HIV status, race, colour, religion, political, trade union or other opinion or belief, national or social origin, association with a minority, domestic circumstances, property, birth or other status which is unreciprocated or unwanted and which affects the dignity of men and women at work".

What you must not do
Use email to harass other members of staff by sending material they consider offensive or threatening.

What are the consequences of not following this policy?
The Trust deals with harassment by providing advice, support and mediation. Those perpetrating harassment can also be dealt with in the context of the Trust's Bullying and Harassment Policy and could result in disciplinary action up to and including dismissal.

4.3. Pornography

What is pornography?
Pornography can take many forms. For example: textual descriptions, still and moving images, cartoons and sound files. Some pornography is illegal in the UK and some is legal. Pornography considered legal in the UK may be illegal elsewhere. Because of the global nature of email these issues must be taken into consideration. Therefore, the Trust defines pornography as the description or depiction of sexual acts or naked people that are designed to be sexually exciting. The Trust will not tolerate its facilities being used for this type of material and considers such behaviour to constitute a serious disciplinary offence.

What you must not do
Send or forward emails containing pornography. If you receive an email containing pornography you should report it to the Information Governance Manager or your line manager.

Send or forward emails with attachments containing pornography. If you receive an email with an attachment containing pornography you should report it to the Information Governance Manager or your line manager.

Save pornographic material that has been transmitted to you by email.

What are the consequences of not following this policy?
Users and/or the Trust can be prosecuted or held liable for transmitting pornographic material in the UK and elsewhere.

The reputation of the Trust will be seriously questioned if pornographic material has been transmitted and this becomes publicly known.

Users found to be viewing, downloading or in possession of pornographic material, or to have transmitted pornographic material, may be subject to Trust disciplinary action.

4.4. **Copyright**

What is copyright?
Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So, a lack of the symbol does not indicate a lack of copyright. In the case of computer software, users purchase a licence to use the work. The Trust purchases licences on behalf of its users.

What you must not do
Alter any software programs, graphics, etc., without the express permission of the owner.
Claim someone else's work is your own.
Send copyrighted material by email without the permission of the owner. This is considered copying.

What are the consequences of not following this policy?
The Trust may be subject to fines and you may personally be subject to fines and/or up to two years imprisonment if it is determined that you acted without Trust authority. Failure to follow the policy may result in disciplinary action against you in accordance with the Trust's Disciplinary Policy.

5. Duties and responsibilities

The Trust will ensure that all users have access to training and support for using the email system.

The Trust will take all reasonable steps to ensure that users of the email service are aware of policies, protocols, procedures and legal obligations relating to the use of email. This will be done through training and staff communications at departmental and Trust-wide levels.

By following the guidelines in this policy, the email user can minimise the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable if it is determined that you acted without Trust authority and may be subject to disciplinary action in accordance with the Trust's Disciplinary Policy.

6. Policy

The Trust considers email as an important means of communication and recognises the importance of proper email content and speedy replies in conveying a professional image and delivering a good service. Therefore, the Trust wishes users to adhere to the following guidelines:

- Email is the main communication tool within the Trust. It is the line manager's responsibility to cascade that their staff must check their emails regularly for Trust communications in order to ensure that staff are aware of essential messages and accessing their email accounts. You are responsible for checking your mailbox regularly to receive important Trust messages, such as Trust strategy, cyber security risks, service changes, etc.
- All communication you send through the NHSmail is assumed to be official correspondence from you acting in your official capacity on behalf of ASPH NHS Trust.
- You must not send any material by email that could cause distress or cause offence to another user.
- 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.
- Signatures must include your name, job title, Trust name, and, where applicable, a contact number/ pager number.
- Do not send attachments unless necessary. Within the Trust, files can be shared on the network (e.g. using hyperlinks to documents on shared drives).
- Do not forward any work-related emails to your personal email address.
- Do not print emails unless explicitly required to do so as part of a Trust business process – e.g. during evidence gathering as part of an investigation.
- Only send emails if the content would be suitable for display on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password.
- Only mark emails as important if they really are important.
- Delete email messages when they are no longer needed.
- Personal identifiable information must not be detailed in the subject information field and must be encrypted if in the body of the message or an attachment (NHSmail to NHSmail messages are encrypted by default).
- Any member of staff wishing to open an NHSmail account (staffname@nhs.net) must complete the Trust's IT User Access Form or ask their Line Manager to request access via email.
- Email must not be used for personal commercial gain

- You must familiarise yourself with the NHSmail support pages which include important policy documentation, training and guidance materials.

6.1 **Legal Risks**

The Freedom of Information Act 2000 has enabled people to have access to much more information held by public bodies than previously. Communications sent via email may relate to decisions made that might have been sent in letters and memos a few years ago. Like their paper counterparts, these email records must be saved, filed and managed in a manner that will allow easy access in future. Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although email seems to be less formal by its nature than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- If you send emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the Trust can be held liable
- If you forward emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the Trust can be held liable
- If you unlawfully forward confidential information, you and the Trust can be held liable
- If you send an attachment that contains a virus, you and the Trust can be held liable

By following the guidelines in this policy, the email user can minimise the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable and may be subject to disciplinary action by the Trust in accordance with the Trust's Disciplinary Policy.

6.2 **BEST PRACTICE**

- Check your mailbox regularly to receive important Trust communications to ensure you are aware of essential messages.
- Line managers are responsible to regularly cascade to staff the importance of checking and reading their emails.
- Before sending an email, consider whether there is a more appropriate way of communicating - e.g. a telephone call or face-to-face contact
- Write well-structured emails and use short, descriptive sentences
- The Trust's email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smileys however, is discouraged
- Use the spell checker before you send out an email
- Do not write emails in capitals. This appears as if you are shouting and is considered rude
- Unwanted emails (often called Spam) that you are concerned about should be reported to spamreports@nhs.net
- If you forward emails, state clearly what action you expect the recipient to take
- Ensure you send your email only to people who need to see it

- Emails should be treated like any other correspondence and should be answered as quickly as possible
- If you suspect you received a virus by email, telephone the IT Help Desk immediately (ext. 3588). Do not attempt to remove the virus yourself as the IT Department will need to identify it
- "Cc" stands for carbon copy and allows multiple recipients to be included in an e-mail. When you Cc people the Cc list is visible to <u>all</u> recipients. The use of Cc should be avoided when holding a private conversation as a third party might inadvertently be included in the conversation. In such instances it is advisable to enter all recipients in the "To" box only.
  "Bcc" stands for blind carbon copy and works the same as Cc, except that the Bcc list is <u>not</u> visible to all other recipients. The Bcc list is private - no one can see this list except the sender. Care should be taken when deciding whether to use Cc or Bcc. "Bcc" should be used:
  1. When you send an email to ANY personal email address(es)
  2. When emailing more than 5 users from different organisations individually
- Using the "Reply All" feature will send a response to all visible recipients of the original email (the sender and anyone who has been Cc'd). Users should not use "Reply All" automatically in response to an email with multiple recipients. Users should consider carefully whether their reply really needs to be seen by all recipients rather than just the originator of the email.
- If the email contains patient identifiable data, then the email should be encrypted if any of the recipients are not using NHSmail or one of the secure domains listed below. If in doubt enter **[SECURE]** at the start of the subject line (see the CONFIDENTIAL INFORMATION section below). Before forwarding emails, consider whether you need the permission of the original sender

6.3 **<u>OUT OF OFFICE</u>**

An "out of office" message must be set up when absent from the Trust for one day or more.

If away for a significant period (e.g. maternity leave or long-term sick leave) your email account should be redirected to whoever is covering your role. The IT Department can help with this facility.

6.4 **<u>PERSONAL USE</u>**

The Trust's email system, NHSmail, is meant for business use only.

Email messages are increasingly a source of viruses, which often sit within attached documents. Anti-virus and anti-spam software are used to protect your email account but as with any email service, a new virus, spam or phishing message may not be detected immediately.

Due to increasing security risks NHSmail (email) should not be used:

- to share personal non-work related files. Video/audio or other large files should not be sent as attachments.
- as a registration name or contact detail with ANY online retailers or services that are not work related
- to forward on chain letters, junk mail, jokes.
- Executable programs are strictly forbidden.

In the event that you have used NHSmail for personal use:

- Change all non-work related accounts and services to use your personal email address as the default contact
- All emails must adhere to the guidelines in this policy.
- Personal emails should not interfere with the Trust's business.

6.5 **MONITORING OF EMAILS**

- All information held or passed through the email system is monitored for cyber-security threats and malware
  and is the property of the Trust
- The Trust reserves the right to monitor or intercept email communication, if required, in accordance with legislation such as:
  - The Regulation of Investigatory Powers Act 2000,
  - The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
  - The Data Protection Act 2018
  - The General Data Protection Regulation 2018
  - The Human Rights Act 1998

6.6 **CONFIDENTIAL INFORMATION**

The NHSmail service enables confidential information to be securely transmitted from one NHSmail user to another. It should be noted that this security is only extended when sending from an nhs.net account to another nhs.net account, or to the following secure domains:

Central Government	*.gsi.gov.uk
Central Government	*.gse.gov.uk
Central Government	*.gsx.gov.uk
Ministry of Defence	*.mod.uk
Ministry of Defence	*.mod.gov.uk
Police National Network	*.pnn.police.uk
Criminal Justice Services	*.cjsm.net
Local Government / Social Services	*. Gcsx.gov.uk
Locally hosted secure domains that have accredited to meet ISB 1595 (secure email standard)	*.secure.nhs.uk
NHS Digital (formerly known as	*.hscic.gov.uk

HSCIC)	

Email accounts ending with **nhs.uk** (other than secure.nhs.uk) or any that are not in the above list are not considered secure. In such cases, person identifiable information (including digital images) should not be forwarded by email unless it has been anonymised, encrypted or the personal identifiers have been removed. These can be provided to the recipient by separate communication.

If in doubt use **[SECURE]** (including the square brackets) in the email subject at the beginning when sending from NHSmail. This will automatically encrypt the email if there is no guaranteed secure delivery route (where secure delivery routes exist the message is not unnecessarily encrypted). Full details are available in the guidance documents on the NHSmail web site.

The safe standards of confidentiality should also be applied to staff related personal details.

Any email containing person identifiable information held in an email account should be deleted as soon as no longer required.

6.7 **DISCLAIMER**

The following NHSmail disclaimer will be added to all outgoing email.

This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it.
Please do not disclose, copy or distribute information in this email or take any action in relation to its contents. To do so is strictly prohibited and may be unlawful. Thank you for your co-operation.

NHSmail is the secure email and directory service available for all NHS staff in England and Scotland. NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and other accredited email services.

For more information and to find out how you can switch, https://portal.nhs.net/help/joiningnhsmail

6.8 **SYSTEM MONITORING**

All emails are monitored for viruses. All email traffic to NHSmail (incoming and outgoing) is logged automatically. The logs do not include email content and are audited periodically.

The content of emails is not routinely monitored, however, NHSmail keeps audit logs and message tracking logs.

6.9 **Data retention, archiving and email management**

- Staff is responsible for the management of their emails and must routinely delete nonessential email messages as soon as possible on a regular basis.

- Any emails that form part of a Trust record must be retained and stored for example in a departmental shared drive and kept for the appropriate length of time as identified in the Department of Health Records Management Code of Practice, The Trust's Records Management Policy or the local departmental retention schedule.

- When a member of staff has left the Trust, their email account will be made inactive and then deleted.

- Where staff have a need to archive their emails, these must be stored on a Trust server in the member of staff's personal folder (H: drive).

- Any email is discoverable for a period of time (see NHSmail data retention period document in the NHS Portal under Guidance) and could be held as part of the record in an investigation or allegation.

- If there is evidence that you are not adhering to the guidelines set out in this policy, the Trust reserves the right to take disciplinary action, which may lead to a termination of contract and/or legal action.

6.10 **REQUEST FOR ACCESS TO A MAILBOX DATA**

The process for requesting data for investigations can be found in the NHSmail Access to Data Policy.
NHS Digital will only accept investigation requests from the Chief Executive or HR Director or Divisional Directors.
Investigations must be in writing or email via feedback@nhs.net (NHS Digital) as a first instance.

6.11 **NHSmail EMAIL MAILBOXES**

All email mailboxes maintained on NHSmail are property of the NHS.

Email mailboxes will be deleted 30 days after a user is flagged as a 'leaver' on NHSmail, unless they are marked as a starter at a new organization within that period.

The Freedom of Information Act 2000 has enabled people to have access to much more information held by public bodies than previously. Communications sent via email may relate to decisions made that might have been sent in letters and memos a few years ago. Like their paper counterparts, these email records must be saved, filed and managed in a manner that will allow easy access in future. Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature, email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

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

- If you forward emails with any libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions, you and the Trust can be held liable.
- If you unlawfully forward confidential information, you and the Trust can be held liable.
- If you send an attachment that contains a virus, you and the Trust can be held liable.

6.12 **GLOBAL EMAILS**

Any information for distribution to all users should be included in the Trust's daily Aspire e-bulletin and must be sent to the following email address: **asp-tr.aspire@nhs.net** Attachments must not be included. The Aspire e-bulletin will be sent out in the morning and content is subject to approval by the Communications Department.

Any member of staff that needs to send an urgent global email can send it to the above address and it will then be approved and sent out by the communications department as a "Newsflash" item where appropriate.

Any other message arriving after the day's Aspire e-bulletin has been sent will have to wait until the next day.

The ability to send any other global email will be restricted to:

- Executive Directors and their PA's
- The Chaplain
- Communications Staff
- Transport Staff
- IT Support Staff
- Pathology (out of hours)
- Facilities (out of hours)
- Imaging (out of hours)

6.13 **The Trust offers the following form of email access:**

Full Outlook client

This is available to staff accessing email from computers that are **not** routinely shared or accessed via a generic network login i.e. it is intended for office-based staff who routinely use the same computer.
The full Outlook client will **not** be installed on shared-use computers, however all staff with NHSmail email accounts will be able to use the OWA service to access their email on these machines. There is a link to NHSmail OWA on TrustNet.

Outlook Web Access (OWA)

This is available to all staff, but in particular those accessing email from computers in a **shared** environment - e.g. outpatient clinic rooms, **or** from computers that use a generic network login such as inpatient wards.

IOS or Android App

NHSmail is available on personal devices via built in apps or apps available via the relevant 'store'. Where the built-in email app is not able to keep NHSmail separate from personal emails, staff must download the Outlook app and configure it accordingly. Your personal device will be forced to encrypt, and you will be required to set up a passcode or PIN.
Details of how to configure a personal device can be found here.
ASPH NHS Trust and NHSmail is not responsible for any loss of personal data or required to provide support for personal devices.

7 Training

Contact IT Training in the Minerva Centre to:
7.1 **Learn how to create and send an email**
7.2 **Manage your Calendar**
7.3 **Learn how to reset your password**
7.4 **Learn how to set up memorable security questions**

8 Stakeholder Engagement and Communication

8.1 Managers and staff from Digital Services were involved in the creation of this policy document

9 Approval and Ratification

9.1 Ratification of this policy will be via the Information Governance Steering Group.

10 Dissemination and Implementation

10.1 The policy will be disseminated through the Aspire global email.

10.2 This policy will be published on the trust intranet and internet sites

11 Review and Revision Arrangements

11.1 This policy will be reviewed by the author every 3 years, or before if necessary.

12 Document Control and Archiving

12.1 This is a trust-wide document and archiving arrangements are managed by the Head of Regulation & Accreditation and Information Content Manager who can be contacted to request master/archived copies.

12.2 On the internet site, the document will be highlighted as green, when in date, amber 3 months prior to review date, and red if expired.

13 Monitoring compliance with this Policy

13.1 Where it is identified a member of staff is not adhering to this policy, and guidance and training have not ensured compliance with the policy, then the Trust may take disciplinary action, which may include restriction of access to NHS e-mail.

13.2 When monitoring staff usage of email, monitoring is undertaken in full consideration of Article 8 of the Human Rights Act 1998 and the Information Commissioners Office "The Employment Practice Code: Part 3 Monitoring at Work".

14 Supporting References / Evidence Base

- Data Protection Act 1998
- Confidentiality Code of Conduct
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Information Commissioner - Employment Practices Data Protection Code:
- Monitoring at Work (2011).
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 Telecommunications (Lawful business
- Practice) (Interception of Communications Regulations 2000

This document will be monitored regularly to ensure it is effective and to assure compliance

Requirement to be monitored	Leads	Tool	Frequency of monitoring	Reporting Arrangements	Lead(s) for acting on recommendations
This policy will be regularly reviewed and updated	IT Department and Information Governance lead(s)	Report to Information Governance Steering Group	At least every 3 years or more frequently if required	HIS policy audit report to: Information Governance Steering Group	Assigned by Information Governance Steering Group

- **APPENDIX 1: EQUALITY IMPACT ASSESSMENT**

Equality Impact Assessment Summary

Name and title: Morné Beck, Head of IT
Policy: Policy for the use of email

Background • Who was involved in the Equality Impact Assessment
The EIA was performed by the Head of IT
Methodology • A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age) • The data sources and any other information used • The consultation that was carried out (who, why and how?)
The policies were examined and reviewed to ensure that no negative impact on equality would result from the policies.
Key Findings • Describe the results of the assessment • Identify if there is adverse or a potentially adverse impact for any equalities groups
There is no impact on equality.
Conclusion • Provide a summary of the overall conclusions

The policies apply to all staff regardless of race, ethnic origin, gender, culture, religion or belief, sexual orientation and age.
Recommendations • State recommended changes to the proposed policy as a result of the impact assessment • Where it has not been possible to amend the policy, provide the detail of any actions that have been identified • Describe the plans for reviewing the assessment
The policy should be approved.