NHSmail Acceptable Use Policy (AUP)

September 2018
Version 3

Contents

1. Introduction

This document explains how the NHSmail service should be used. It is your responsibility to ensure you understand and comply with this policy. It ensures that:

- You understand your responsibilities and what constitutes abuse of the service
- Computers and personal data are not put at risk.
- You understand how NHSmail complies with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) by reading the Transparency Information.

As an NHSmail account holder, you should expect to receive ad-hoc communications about NHSmail:

- from NHS Digital if you are based in England
- from National Services Scotland if you are based in Scotland

informing you of changes or important updates to the service that may impact your use.

NHS Digital, in line with NHSmail Board approval, has the right to authorise activity on the service to protect and manage it against external threats, to maintain its security and integrity.

If you have any questions about these terms and conditions, you should contact the NHSmail team at feedback@nhs.net (England) or nhsmail.scotland@nhs.net (Scotland).

The NHSmail team reserves the right to update this document as necessary. A copy of the current version can be found at https://portal.nhs.net/Home/AcceptablePolicy It is your responsibility to ensure you are fully compliant at all times.

Supporting information can be found via the NHSmail Portal help pages at: https://portal.nhs.net/Help/

2. General information about NHSmail

2.1 NHSmail includes the core services of secure email, the NHS Directory, Skype for Business (Instant Messaging and Presence) and portal administration tools. There are a number of additional top-up services which will only be available if your organisation has chosen to provide them.

2.2 The NHSmail services have been provided to aid the provision of health and social care and this should be your main use of the service.

2.3 There may be circumstances under which it is necessary for a designated and authorised person other than you, to view the contents of your files and folders within NHSmail. For example, if you have a secretary or PA that organises your diary.

2.4 If you are a member of clinical or care staff, you may use NHSmail services in relation to the treatment of private patients in accordance with your own professional codes of conduct.

2.5 Health and social care staff contact details are provided in the NHS Directory to support the delivery of health and care - these details will be shared across:

- All NHSmail users
- Approved, federated 3rd party organisations

2.6 All data retained within the service remains the property of the NHS. Details about the management of data within the NHSmail service is detailed within the Transparency Information.

2.7 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 are provided to health and social care staff for their use to support publicly funded healthcare. Where accounts are no longer used they are automatically removed after a period of inactivity as defined in the Data Retention and Information Management Policy.

2.8 The NHSmail team reserves the right to withdraw an NHSmail account from use should operational requirements dictate. This may include limiting service or complete de-activation.

2.9 Your organisation maintains day to day administration responsibility for your NHSmail account. If your use breaches this AUP or the Access Policy, your organisation has the right to undertake disciplinary procedures in accordance with your local HR policy.

2.10 NHSmail is governed by its Clinical Safety Case. A summary of this can be viewed within the NHSmail Portal help pages.

2.11 NHSmail facilitates the exchange of information but it may not determine the definitive position of a situation and should always be read in context of the situation it concerns. i.e. patient notes may be exchanged using NHSmail but may not consider additional information added into the patient's record.

3. Your responsibilities when using NHSmail

3.1 General responsibilities when using NHSmail

3.1.1 You must not use NHSmail to violate any laws or regulations of the United Kingdom or other countries. Use of the service for illegal activity is grounds for immediate dismissal and any illegal activity will be reported to the police. Illegal activity includes, but is not limited to, sending or receiving material related to paedophilia, terrorism, incitement to racial harassment, stalking, sexual harassment and treason. Use of the service for illegal activity will result in the immediate disablement of your NHSmail account.

3.1.2 You must not use any of the NHSmail services for commercial gain. This includes, but is not limited to: unsolicited marketing, advertising and selling goods or services.

3.1.3 You must not attempt to interfere with the technical components, both hardware and software, of the NHSmail system in any way.

3.1.4 When you set up your NHSmail account you must identify yourself honestly, accurately and completely.

3.1.5 You must ensure your password and answers to your security questions for the NHSmail services are kept confidential and secure at all times. You should notify your Local Administrator if you become aware of any unauthorised access to your NHSmail account. You must **never** input your NHSmail password into any other website other than nhs.net sites, including social media sites. You will never be asked for your NHSmail password. Do not divulge this information to anyone, even if asked.

3.1.6 Email messages are increasingly a source of viruses which often sit within attached documents. NHSmail is protected by anti-virus and anti-spam software although occasionally, as with any email service, a new virus or spam message may not be immediately detected. If you are unsure of the source of an email or attachment you should leave it unopened and inform your local IT services. If you receive spam messages you should report them to spamreports@nhs.net using the process detailed in the Cyber Security Guide. You must not introduce or forward any virus or any other computer programme that may cause damage to NHS or social care computers or systems. If you are found to be deliberately responsible for introducing or forwarding a programme that causes any loss of service, NHS Digital or National Services Scotland may seek financial reparation from your employing organisation.

3.1.7 If your organisation has enabled the sharing of files or links using Skype for Business, the same precautions must be adopted as stated above for email.

3.1.8 You must not use the NHSmail service to disable or overload any computer system or network. Where excessive account activity is detected your account could be suspended, without notice, to safeguard the service for all other users.

3.1.9 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.

3.1.10 You must familiarise yourself and regularly check the NHSmail Portal help pages which include important policy documentation, service status information, training and guidance materials, information about known issues with the service and user/administration guides.

3.1.11 If you are accessing your NHSmail account from a non-corporate device i.e. a home computer, personally owned laptop or in an internet café, you should only access the service via the web at www.nhs.net and not through an email programme such as Microsoft Outlook, unless you have explicit permission from your own organisation to do so.

3.1.12 It is your responsibility to ensure you regularly archive data, in accordance with your local archiving policy, contained within your mailbox and ensure your quota is not breached. NHSmail is designed for the exchange of information and is not a storage solution and archiving should be carried out in line with your local policy and process. If you do not manage your mailbox quota you are at risk of your mailbox no longer being able to send or receive email, potentially compromising clinical safety.

3.2 It is your responsibility to ensure you are up to date with your local Information Governance training. To access NHSmail, health and care organisations must meet **or exceed** one of the following:

- A 2017/18 Information Governance Toolkit (IGT) rating of ‘Level 2’ (applicable until 31 March 2019).
- A Data Security and Protection Toolkit rating of ‘Entry Level’. Please note a rating of ‘Entry Level’ is a minimum and will not be sufficient to meet wider contractual and regulatory requirements to connect to other NHS Digital services.

3.3 Responsibilities when using the NHSmail email service:

3.3.1 You must not attempt to disguise your identity, your sending address or send email from other systems pretending to originate from the NHSmail service. Where there is a need to provide someone else with the ability to send email on your behalf, this should be done via the delegation controls within the service. Where an organisation wishes to send email on behalf of its staff the organisation may request the ability to do this via Impersonation accounts. Individuals being impersonated must always be informed prior to emails being sent.

3.3.2 You must not send any material by email or Skype for Business that could cause distress or offence to another user. You must not send any material that is obscene, sexually explicit or pornographic. 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.

3.3.3 You must not use the NHSmail service to harass other users or groups by sending persistent emails or instant messages to individuals or distribution lists.

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

3.3.5 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.

3.3.6 It is your responsibility to check that you are communicating with the correct recipient when using Skype for Business to send Instant Messages. There may be more than one person with the same name using the service. Ensure you establish contact via other means before exchange of any confidential or sensitive information. 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 General Data Protection Regulation (GDPR) 2018 and the Data Protection Act 2018, Freedom of Information Act 2000 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.

3.3.7 You must ensure any application integrating with NHSmail has an in-built error messaging capability to highlight any messages that are not delivered. This is to protect your business process and to ensure any errors are highlighted to the sender in order for the error to be fixed as soon as possible.

3.4 Responsibilities when using the NHS Directory service

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

3.4.2 You must not use the NHS Directory to identify individuals or groups of individuals to target for marketing or commercial gain, either on your behalf or on that of a third party.

3.5 Responsibilities when using your calendar

3.5.1 Ensure your calendar settings are set in accordance with your local organisation policies.

3.5.2 The default setting is Free/Busy Time. Patient or sensitive data should not be stored in calendar appointments - this is essential where organisations choose different default calendar settings to ensure data is not accidentally seen by inappropriate colleagues.

3.5.3 Attachments within calendar appointments are counted as part of your mailbox quota and should be regularly deleted to ensure your quota is not breached.

3.6 Information governance issues

3.6.1 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, Instant Messages or Skype for Business recordings (if available) are immediately attached to the patient record. Failure to do so could have implications on patient safety.

3.6.2 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.

3.6.3 Your organisation is entitled to seek access to the contents of your mailbox, sent/received messages or other audit data as required to support information governance processes without your prior consent. Such requests are strictly regulated with the process detailed in the Access to Data Policy.

3.6.4 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.

3.6.5 NHSmail email addresses will be re-used two years after an account has been deleted off the platform.

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 (i.e. from an '*.nhs.net' or '.hscic.gov.uk' account to an '*.nhs.net' or '.hscic.gov.uk' account)
- 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 Portal help pages. 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 Skype for Business Instant 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 (Instant 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 If personal identifiable information is visible to other people, it is your responsibility to make sure those people have a valid relationship with the person.

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 Instant Messaging and Presence.

4.3.8 If it is likely you may be sent personal and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.

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

5. Using the NHSmail Office 365 (O365) Hybrid Service

5.1. In addition to the above policy, the following specifically relate to those using the NHSmail O365 Hybrid Service and all the available O365 applications such as Yammer, Teams, SharePoint etc.:

5.1.1 The NHSmail service is not responsible for the content of any user-created posting, listing or message made on the service. The decision to post, view or interact with content and others via the service is a local risk decision.

5.1.2 The NHSmail O365 Hybrid Service provides all users within it the ability to share content with each other. It is your responsibility to ensure you are sharing content with the appropriate individual as there may be more than one person with the same name using the service.

5.1.3 You must not attempt to post, access, delete, modify, or disclose any sensitive content/information if you do not have a legitimate reason to do so.

5.1.4 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 help pages.

5.1.5 It is your responsibility to ensure content you upload to the NHSmail O365 Hybrid Service does not infringe copyright or be in contravention to the law.

5.1.6 You must not use NHSmail O365 application services to create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, discriminatory, or extremist material that risks drawing people into terrorism.

5.1.7 Organisational administrators are entitled to request access to the contents of your O365 application services including; SharePoint, OneDrive, Teams and Yammer and other applications you may be licensed for to support information governance processes without your prior consent. Such requests are strictly regulated, the process is detailed in the NHSmail Portal help pages.

5.1.8 You must abide by the regulations applicable for your organisation with regards to uploading of content to the NHSmail O365 Hybrid Service. The NHSmail O365 Hybrid Service must not be used as a replacement for clinical systems. The NHSmail O365 Hybrid Service is a collaboration system not a clinical records or patient data system. Content of this nature must be stored in your local organisations patient record systems in accordance with local information governance policies.

5.1.9 Access to O365 services via mobile devices - 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.

5.1.10 When moving roles between health and care organisations, it is your responsibility to ensure any data stored in the O365 Hybrid relating to your current/previous role is archived appropriately and/or deleted. It must not be transferred to your new employing organisation without consent of the organisation you’re leaving. Guidance is available in the Leavers and Joiners Guide. The Local Administrator (LA) has the right to empty the users OneDrive at any time without the consent of the user.

5.2. Office 365 Collaboration Tools Acceptable Use Guidelines

5.2.1 Common standards of behaviour apply to the NHSmail O365 Hybrid tools including, but not limited to, Yammer, Teams and SharePoint.

5.2.2 The Yammer network is open to all individuals whose organisations have procured O365 licences within the NHSmail tenant and can be used as an open space for collaboration. Closed group creation is recommended for users so access to content and collaboration can be managed appropriately by a group owner.

5.2.3 Yammer and Teams are not document or content libraries. Formal records should be created for anything you want to keep.

5.2.4 Confidential information should only be shared as allowed by your organisation. You must not post content/information belonging to other people without permission from them to do so.

5.2.5 You must not post or make available any message that is grossly offensive, indecent, obscene or of a menacing nature. Spamming, unrelated, or inappropriate content is not acceptable. Further specific guidance is available from the Crown Prosecution Service (CPS).

5.2.6 The NHSmail O365 Hybrid Service reserves the right to remove any Yammer group it deems inappropriate or offensive.

5.2.7 SharePoint sites must be restricted to those individuals whom require access. You must notify your LA to remove permissions when an individual no longer requires access.

5.2.8 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. NHSmail Portal does not have an automated procedure to remove permission for individuals who have left your organisation.

5.2.9 All communications using Office 365 tools must be used in line with the same guidance defined for the use of email and Skype for Business.