NHSmail O365 Shared Tenant Acceptable Use Policy (AUP)

September 2023
Version 6.0

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

NHS England, in line with NHSmail governance framework, 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 Local Administrators for your organisation in the first instance.

The NHSmail team reserves the right to update this document, as necessary. A copy of the current version can be found at Acceptable Use Policy – NHSmail Support. It is your responsibility to ensure you are always fully compliant.

Supporting information can be found via the NHSmail support site at: https://support.nhs.net/

2. General information about the NHSmail O365 Shared Tenant

2.1 NHSmail includes the core services of secure email, the NHS Directory, O365 including Teams and NHSmail portal administration tools. There are a number of additional O365 Top-up and Add-on licence services which will only be available if your organisation has chosen to purchase and enable 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 It is recommended that all NHSmail user accounts enroll Multi-Factor Authentication (MFA) to enhance the security of the NHSmail platform. Further guidance on setting up MFA is available on the NHSmail support site - User Guides – NHSmail Support.

2.4 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.

2.5 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.

2.6 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, guest and federated third party organisations

2.7 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:

- Data Protection Impact Assessment
- Transparency Information
- Data Retention and Information Management Policy
- Data Retention and Information Management Policy – Office 365
- NHSmail UK GDPR Joint Data Controller Table

2.8 NHSmail accounts are owned by:

- NHS England on behalf of the Secretary of State for Health in England

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.

2.9 You are expected to only utilise one NHSmail email account. Should you require multiple accounts, this would be a local organisation decision dependent on each use case.

2.10 If your organisation already has another publicly funded email account, you are not eligible for NHSmail, for example 'nhs.uk','gov.uk' or domains accredited to the secure email standard.

2.11 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.

2.12 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.

2.13 NHSmail is governed by its Clinical Safety Case.

2.14 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.

2.15 You must abide by the local policies and regulations applicable for your organisation with regards to uploading of content to the O365 applications and collaboration tools. NHSmail 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.

2.16 NHSmail can be accessed across the internet from any location throughout the world, however this should only be done in accordance with your local organisation's policies and

procedures. Multi-factor authentication (MFA) is required for NHSmail access outside of the UK and should be enrolled prior to travel - Information – NHSmail users working outside of the United Kingdom (UK) – NHSmail Support

3. Your responsibilities when using the NHSmail O365 Shared Tenant

3.1 General responsibilities when using NHSmail:

3.1.1 You must not use NHSmail to violate any laws, copyright 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. 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.

3.1.2 You must not use any of the NHSmail services for personal or 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/ account secret for the NHSmail services are always kept confidential and secure. You should notify your Local Administrator if you become aware of any unauthorised access to your NHSmail account or believe your account to be compromised. You must **never** input your NHSmail password into any websites 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.

Applications integrated with NHSmail single sign-on will redirect the user to enter their NHSmail credentials via the NHSmail portal.

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 on Reporting Cyber Threats on the NHSmail support site. 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 England may seek financial reparation from your employing organisation.

3.1.7 If your organisation has enabled the sharing of files or links using O365 collaboration

tools including Teams, the same precautions must be adopted as stated above for email.

3.1.8 When considering privacy settings, you must ensure you select the appropriate setting of private or public. The private setting should always be applied if you are working on documents containing personal data of patients, staff, or others. If you choose to change the settings to public and use the 'allow everyone' setting you will publicly share content with across the platform. It is unlikely you would ever need to do this, and you may breach data protection, safety, and security protocols if you do so.

3.1.9 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.

3.1.10 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 Teams messages or any other collaboration tools.

3.1.11 You must familiarise yourself and regularly check the NHSmail support site which includes important policy documentation, service status information, training and guidance materials, information about known issues with the service and user/administration guides.

3.1.12 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.

3.1.13 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. Your organisation may decide to use Exchange Online Archiving to help you manage your mailbox quota. NHSmail is designed for the exchange of information and is not a storage solution and archiving should be conducted 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.

3.1.14 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 complete and publish the Data Security and Protection Toolkit as applicable to the organisation type.

3.2 Responsibilities when using the NHSmail service

3.2.1 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. Impersonation enables an application account to impersonate all user accounts within an organisation.

3.2.2 You must not send any material by email, Teams or any other O365 collaboration tool 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 ICB (formerly CCG).

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

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

3.2.5 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.

3.2.6 It is your responsibility to check that you are communicating with the correct recipient when using O365 collaboration tools including Teams to send 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. 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.

3.2.7 NHSmail is not a guaranteed delivery mechanism. If your application is integrating with NHSmail and is used to exchange clinical (or other) data your local safety case must take into accounts hazards associated with email such as non-delivery, delivery delays, out of sequence delivery and unavailability as well as having a robust tracking mechanism to identify any delivery failures. This is to protect your business process, reduce clinical risk and to ensure any errors are highlighted to the sender for the error to be fixed as soon as possible.

3.3 Responsibilities when using the NHS Directory service

3.3.1 It is your responsibility to make sure your details in the NHS Directory are correct and up to date. Your NHSmail Local Administrator has access to update details in the NHS Directory.

3.3.2 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.

3.4 Responsibilities when using your calendar

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

3.4.2 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 incorrect users across the NHSmail Shared Tenant.

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

3.5 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. Access for any other reason, for example long term sick, is subject to local processes and procedures and is not governed by NHSmail.

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 organisation's SharePoint sites, Teams groups, your Yammer network or has access to your OneDrive. The NHSmail Portal does not have an automated procedure to remove permissions 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..

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.