Lothian NHS Board

Waverley Gate
2-4 Waterloo Place
Edinburgh
EH1 3EG

Telephone: 0131 536 9000
www.nhslothian.scot.nhs.uk

Date: 29/02/2024
Our Ref: 8390
Enquiries to loth.freedomofinfomation@nhs.scot

Dear

FREEDOM OF INFORMATION – RECORD KEEPING

I write in response to your request for information in relation to record keeping in NHS Lothian.

Questions:

1. When should within Lothian records of e mails, phone calls or other discussions about a patient be added to the patients clinical file?

2. When should cross health board MDT or within disciplinary records of e mails, phone calls, conversations about a patient be added to a patients clinical file?

Answer:

All clinically relevant patient information must be recorded in patient records by clinical staff.

Questions:

3. When should Drs send written updates or summaries of discharge letters or outpatient discussions, to a patient?

4. When should Drs copy patients into correspondence being sent to GP?

Answer:

Immediate discharge summaries can be given to the patient in paper format at discharge. These may be updated if any information changes, and this is emailed to the GP. Correspondence between hospital clinicians and GP may be sent if required following a patient appointment. These may be sent to the GP and to the patient.

Questions:

5. How long should e mails about patients be kept for?

6. Instructions for e mail management and culling/deleting records

Answer:

Email is a communication tool and not a record system. All clinically relevant patient information must be recorded in the patient's records by clinical staff. I have enclosed NHS Scotland's email policy with this response.

Questions:

7. How to correct errors on existing electronic records

8. How to temporarily remove patient records from the electronic records system

9. How to permanently remove patient records from the electronic records system

Answer:

If an erroneous entry on an electronic record is identified and confirmed, this must be updated. Patient records cannot be removed from a system either temporarily or permanently as this is a legal record.

I hope the information provided helps with your request.

If you are unhappy with our response to your request, you do have the right to request us to review it. Your request should be made within 40 working days of receipt of this letter, and we will reply within 20 working days of receipt. If our decision is unchanged following a review and you remain dissatisfied with this, you then have the right to make a formal complaint to the Scottish Information Commissioner within 6 months of receipt of our review response. You can do this by using the Scottish Information Commissioner's Office online appeals service at www.itspublicknowledge.info/appeal. If you remain dissatisfied with the Commissioner's response you then have the option to appeal to the Court of Session on a point of law.

If you require a review of our decision to be carried out, please write to the reviewer at the address at the top of this letter. The review will be undertaken by a Reviewer who was not involved in the original decision-making process.

FOI responses (subject to redaction of personal information) may appear on NHS Lothian's Freedom of Information website at: https://org.nhslothian.scot/FOI

Yours sincerely

ALISON MACDONALD
Executive Director of Nursing Midwifery and AHPs
Cc: Chief Executive

Email Policy
for
Office 365 Email

V 1.0

June 2020

This Email Policy is specific to the NHS Scotland Office 365 Email Service. This policy does not replace any NHS Scotland or health board policies.

This Policy is the overarching email policy for NHS Scotland and details the requirements for the Office 365 Email Governance Framework (OEGF).

Document Control Sheet

Key Information

Title	Email Policy for 0365
Date Published/ Issued	12 June 2020
Version/ Issue Number	V1.0
Document Type	Overarching Email Policy for the O365 Email Governance Framework
Document Status	Issued
Author	Office 365 Cloud and Computing Programme, Information Security Governance Team
Owner	NHS Scotland National O365 Support (NOS) Team
Approvers	NSS SRO
Contact	nss.o365@nhs.net

Revision History

Version	Date	Summary of Changes
DV0.1	6 Jan 2020	Draft
0.2	4 Feb 2020	Email document set details identified and added
0.3	5 Mar 2020	Risk analyst review
0.4	6 Mar 2020	Final draft
0.5	12 Jun 2020	Information Governance review complete

Approvals

Version	Date	Name	Designation
1.0	12/06/2020	Deryck Mitchelson	NSS SRO
Signature:		Agreed via O365 Programme Manager	

Contents

1. Introduction

This policy has been created for the Microsoft Office (O365) email service. It is in separate from any NHS Scotland (NHSS) email policies held by health boards at local level. Where local policies exist, the more restrictive user controls take precedence, unless the policy statement is in reference to the O365 email service.

Where relevant, local policies should be updated to include O365 requirements, or this policy addendum to them.

Emails sent to and from NHSS using the O365 service will be subject to this policy to ensure users of email:

- Understand that it is their responsibility read, understand and comply with this policy.
- Understand the service.
- Activity by users does not put the infrastructure including devices and personal data at risk.
- As an Office 365 licence holder, users will receive updates and information from National Services Scotland (NSS).

This will allow NHSS staff to effectively and securely use O365 email and allow NHSS to ensure that patient identifiable data, plus sensitive and confidential information is transmitted and stored securely.

2. Requirements Specifications

The OEGF is to be applied to ensure the NHSS O365 solution conforms with NHS bodies and government departments across the United Kingdom.

Sensitive information classified OFFICIAL or below can be sent in compliance with:

- Other NHSmail addresses (i.e. from an ‘O365 email account to an ‘.nhs.scot, nhs.net’ or ‘.gov.uk’ account).
- Other email systems that comply with the UK Government secure email policy.
- DCB1596 secure email standard.

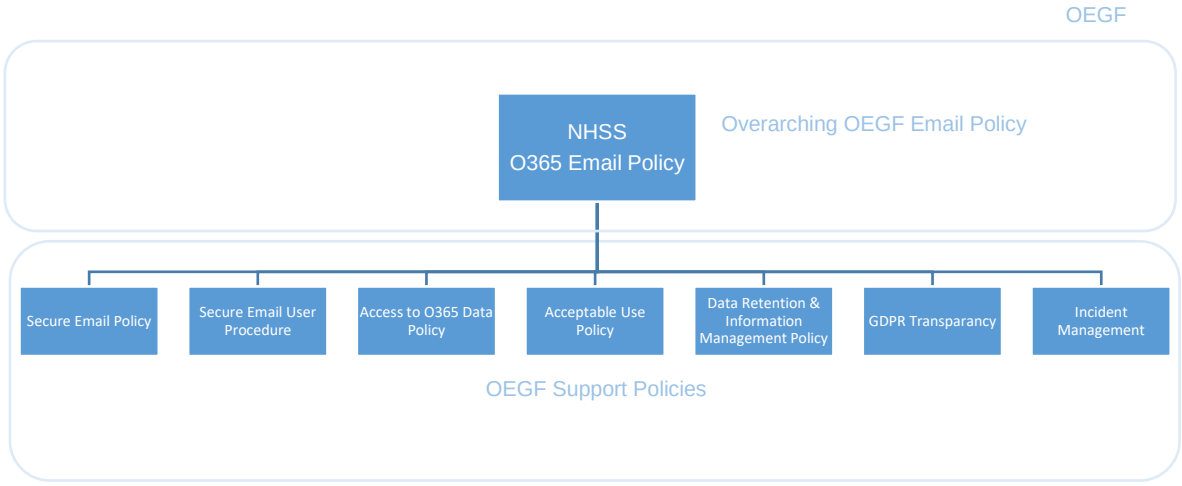
The O365 secure email policy gives further detail on the controls required.

3. NHSS Office 365 Email Governance Framework

This policy is the overarching email policy for the Office 365 (O365) Email Governance Framework (OEGF).

The OEGF is an evergreen document set. Microsoft services change on a regular basis, to that effect the OEGF support policies will be subject to change on a regular basis and will be updated to record those changes.

The following additional policies and procedures are included as part of the OEGF document set:



3.1 Scope

The scope of the O365 email service includes NHSS secure email provisioning. This is shared across multiple policy documentation and includes:

- Information Management.
- Information Governance.
- Account Management.
- User Management.
- Information Sharing.
- Mobile Device Management.
- Information Security.
- Incident Management.
- HR Responsibilities.

O365 provides a hosted messaging service using Microsoft Exchange Online. Exchange online uses the Microsoft Exchange Server as a cloud-based solution that gives authorised access from Laptops, PC's, web and mobile devices to:

- Email.
- Calendar.

- Contacts.

Note that Microsoft change their services regularly. Updated capabilities can be found here.

4. Information Management

4.1. Clinical Information Management

It is important that emails and calendar entries only contain pertinent data. Where the entries contain patient data, this should be attached to the patient record with consideration to the pertinence e.g. complaints information will contain patient data but that should not be attached to the patient record. Failure to do so could have implications on patient safety.

4.2. Email Use

Emails sent using the O365 email service are for business use, however some personal use may be allowed by your Health Board. Refer to local Acceptable Use Policy for guidance.

4.3. User Access

The O365 email service can be accessed by:

- O365 mail users.
- Federated third parties who have been approved by NHSS boards to access the service.

4.4. Access Controls

Access Controls are explained in the O365 Secure Email Policy.

5. Information Governance

5.1. Classification of Information

All data within the O365 service is subject to information governance and records management, this includes but is not limited to:

- The Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020.
- Data Retention Periods.
- NHSS Business Classification and Retention Schedule.
- Clinical Safety Requirements.

The following O365 email capabilities support information governance and records management.

5.2. Applying Labels

Documents sent by email should be manually labelled, retention periods set and the appropriate policy applied.

This can also be done automatically, however, an E5 licence is required for the user.

5.3. Retention Periods

User's email and calendar items should have retention policies applied to their mailboxes and documents contained within. Retention period information is included in the O365 Data Retention and Information Management Policy.

5.4. Account Management

The service model is being designed around a single tenancy for NHSS as follows:

- 1st Line, Password fixes, unlock, disable, delegate will be handled by individual boards.
- 2nd Line, more complex issues will be handled on a regional basis.
- 3rd Line, will be managed by the National team, these are largely permission based and may require assistance by suppliers e.g. Microsoft.

Each board has its own Azure Active Directory (Azure AD). The accounts are managed centrally within each board.

5.5. Email Ownership

Data retained within the O365 service is the property of NHSS. Users should remember that under the EU General Data Protection Regulations (GDPR) and the UK Data Protection Act (2018) that personal information such as patient data is accessible to the data subject.

Details of the data retained in the O365 service can be found in the GDPR Transparency Information for O365 Email Policy.

5.6. Responsibilities

Responsibilities are set out in the O365 Mail Acceptable Use Policy

5.7. Mailbox and Email Address Management

Information on Mailbox Management is in the:

- O365 Email Security Policy.
- O365 Data Retention and Information Management Policy.

5.8. User Management and Privacy

O365 email facilitates the exchange of information, however it cannot totally control the content of the email. This is a user responsibility.

NHSS are entitled to seek access to the contents of O365 email mailboxes and calendar entries to support information governance processes and legal requirements to access data. Such requests are to be strictly regulated with the process detailed in the Access to Data Procedure for O365 Email.

5.9. Change of Function

When moving roles between NHSS, users are to ensure any data stored within their email account of their previous role is archived appropriately and/or deleted. It must not be transferred to the new role without written consent of the previous employer.

On change or function or role, if users continue to receive data pertinent to their previous role, NHSS should carry out a risk assessment to identify if this is to be considered as a data breach and reported according to their local Data Protection Officer.

5.10. Archiving

Email mailboxes should not be used as a storage solution. In accordance with mailbox capacity management, users are responsible for reducing the amount of data held in mailboxes to ensure limits are not breached.

If users do not manage mailbox limits there is a risk that the mailbox will not be able to send or receive emails, which could compromise the availability of information.

5.11. Directory Entries

It is the users' responsibility to ensure that their directory details are correct, complete and up to date.

5.12. Using Calendars

Calendar settings are the responsibility of NHSS and should be set in accordance with their policies.

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

6. Information Sharing

6.1. Shared Mailboxes

Shared mailboxes may be used where there is a requirement for an authorised or designated individual to view the contents of emails and folders or send emails on behalf of a department or individual. Shared mailboxes should be created by administrators. Information on shared mailboxes for O365 is available **here**.

6.2. Contact Lists

To support the delivery of health and social care, through information sharing, NHSS staff using O365 Mail will have their contact details stored in the address book of the Outlook directory. Users can search for directory information using:

- Outlook.
- Outlook on the Web app.
- Within O365.

6.3. Contact Groups

Contact groups may be created by users to store lists of multiple contacts in a group to speed up the distribution list for emails.

6.4. Receiving Communications from the O365 Mail Team

National Services Scotland (NSS) will for an O365 Mail Team to manage the service. The team will send ad-hoc communications to O365 mail users about the O365 mail service informing users of changes or important updates to the service that may impact their use.

6.5. Using O365 Email to Exchange Sensitive Information

As O365 Exchange Online is authorised as part of the UK Government Cloud (G-Cloud) to process UK OFFICIAL data, including OFFICIAL-SENSITIVE, clinical care staff may use O365 email services to share information in relation to the treatment of patients in accordance with their own professional to Code of Conduct.

See O365 Email Acceptable Use Policy and Encryption Guidance for further information.

7. Information Security

7.1. Mobile Device Management

See the O365 Secure Email Policy for details regarding use of mobile devices and controls to be used.

7.2. Security of the Email Service

O365 email is a secure service. Microsoft have been certified to UK OFFICIAL for sending sensitive information and the classification of data. In order to maintain the confidentiality, integrity and availability of the O365 email service. The O365 National Team, in conjunction with NHSS O365 email teams, has the right to authorise activity on the O365 service to ensure the security and protection of the O365 email service.

7.3. Protection from Malicious Software

The O365 email service is protected against known malicious software (Malware) using detection, prevention and recovery controls. However new malware is increasingly being developed and introduce via email.

Training and awareness must be regularly used to ensure that users can identify potential malware threats.

7.4. Incident Management

See the O365 Email Incident Management Policy for details.

8. Human Resources Responsibilities

Identity management for O365 users should be managed through the integration of HR systems to ensure joiners, movers and leavers are managed effectively.

8.1. Identity Management

Prior to using the O365 email service, HR departments should ensure that:

- When users apply for O365 email accounts their information is captured accurately through screening questions and background verification checks.
- The use of email and the supporting policies is captured in the terms and conditions of employment.
- Users have access to training on initial employment and when Microsoft provide service updates.

End of Document