Sending Secure Email – User Encryption Guide
for
Office 365 Email

V1.0

June 2020

This Sending Secure Email User Encryption Guide is specific to the NHS Scotland Office 365 Email Service. This user guide does not replace any NHS Scotland or health board policies.

This user guide is a part of the Office 365 Email Governance Framework (OEGF).

This user guide is a support document to the overarching

Office 365 Email Policy.

DOCUMENT CONTROL SHEET

Key Information

Title	Sending Secure Email – User Encryption Guide for Office 365 Email
Date Published/ Issued	12 June 2020
Version/ Issue Number	V1.0
Document Type	Support Policy to the OEGF
Document Status	Issued
Author	Office 365 Cloud and Computing Programme, Information Security Governance Team
Owner	NHS Scotland National O365 Support (NOS) Team
Approvers	Approved as part of the overarching OEGF
Contact	nss.o365@nhs.net

Revision History

Version	Date	Summary of Changes
0.1	12/2/2020	Initial Draft
0.2	28/2/2020	Feedback and review from O365 risk analyst
0.3	3/3/2020	Final draft completed
0.4	12/6/20	IG SLWG review
1.0	12/6/2020	Issued as support policy to the OEGF

Contents

1. Introduction

This document applies to all personnel including permanent, temporary and contracted staff, who have access to the Office 365 (O365) email service, using desktop, laptop, mobile, tablet or phone devices, including iOS and Android systems, authorised for use by NHS Scotland (NHSS).

2. Purpose of Document

The O365 email service includes an encryption feature that allows users to exchange information securely with users of non-accredited or non-secure email services, for example, Gmail, Hotmail. This document is designed for all end users of O365 email and gives information on how and when to use the encryption feature.

3. How Encryption is Applied

Once a message is sent from O365 email, it is encrypted and protected with a digital signature to assure the recipient that the message is authentic and has not been forged or tampered with. Formatting of the message is preserved, and attachments can be included.

4. When to use the O365 Email Encryption Feature

O365 email users can exchange sensitive information securely with other O365 email users, without needing to use the encryption feature. For example, sending from and to nhs.scot and nhs.net email accounts.

If there is doubt or uncertainty, you should use the O365 email encryption feature. O365 email will then encrypt the email only if the destination domain is not secure. If sending an email to multiple organisations with some secure and some insecure domains, those that are secure will receive an unencrypted email and those that are not secure will receive an encrypted email.

5. How to Send an Encrypted Email

Before sending patient or sensitive data via the encryption service, it is good practice to set up the 'encrypted channel' which helps verify the correct recipient, the steps are:

- Send the recipient the NHSS accessing encrypted emails guide for non O365 users. This guide will give instructions on what to expect the first time an encrypted email is received.
    - Please be aware the user cannot register for the service until they have received an encrypted email.
    - Once the recipient of the information has registered for the encryption service and confirmed to the sender this is complete, patient and sensitive data can be sent within the nhs.scot email service as an email or as an attachment, subject to local governance policies.
- Follow the steps below to send an initial encrypted email but do not include patient or sensitive information the first time. This is to 'set-up' the secure channel of communication and ensure the correct recipient has successfully received the email.

5.1 Procedure to Send an Encrypted Email

1. Log in to your O365 email account.
2. Create a new email message in the normal way.
3. Ensure the recipient's email address is correct.
4. In the **subject** field of the email, enter the text [secure] before the subject of the message. The word secure **must** be surrounded by the square brackets for the message to be encrypted. If square brackets aren't used, the content of the email will be sent in plain text and not encrypted, potentially exposed to interception or amendment.
5. Type the message.

6. Click on **send** to send the message. An unencrypted copy will be saved in your **sent items** folder.

Once the initial registration process has taken place, you can then send other emails with required attachments.

The service will then encrypt the message and deliver it to the intended recipient. The sent item will be stored unencrypted in your sent items folder, and any replies received will be decrypted and displayed as normal in O365 mail.

Note: [secure] is not case sensitive and [SECURE] or [Secure], for example, could also be used.

6. Keeping Encrypted Email Secure

Before sending an encrypted email, you should ensure that the recipient is expecting it and is ready to handle the contents appropriately either as part of an agreed clinical or sensitive business workflow or process, particularly if it contains sensitive or patient identifiable information.

Exchanging patient / sensitive information should be done in accordance with local information governance policy / procedures and the O365 email Acceptable Use policy.

A number of attachment types are not permitted to be sent via O365 mail, these include .exe files. If a non-permitted attachment is detected it will automatically be removed. For the full list of non-permitted attachments see the NHSS Attachments Guide for O365 Email.

7. Data Protection

it is the users responsibility and legal duty under the Data Protection Act 2018, on behalf of their employing organisation, to safeguard any data received in line with the data protection and information governance requirements agreed between your organisation and the receiving organisation. If required, and in line with your local information management policies and processes, you should retain unencrypted copies of any encrypted email received in your local information repositories in accordance with NHSS Records Management Code of Practice.

8. Help and Further Guidance

Call the National O365 Support (NOS) Team helpdesk on ServiceNow

Portal http://nhsnss.service-now.com/teams (This may be updated as part of the O365 mail migration)

Phone 0131 275 7777 then option 1.

End of Document