# Sending secure email – user encryption guide for Office 365 email

| | |
|---|---|
| **Approval date:** | **March 2021** |
| **Version number:** | **1.0** |
| **Author:** | **Sam Collier, Senior IG Officer and Deputy DPO**<br>**NHS Scotland Office 365 Cloud and Computing Programme, NSS Information Security Governance Team** |
| **Review date:** | **February 2024** |
| **Security classification:** | **Official – Green: unclassified information** |

If you would like this document in an alternative language or format, please contact Corporate Services on 01595 743069.

Document reference number: HRGUI004

## NHS Shetland Document Development Coversheet*

| | | | |
|---|---|---|---|
| **Name of document** | Sending secure email – user encryption guide for Office 365 email | | |
| **Document reference number** | HRGUI004 | **New or Review?** | New |
| **Author** | Sam Collier, Senior IG Officer and Deputy DPO<br>NHS Scotland Office 365 Cloud and Computing Programme,<br>NSS Information Security Governance Team | | |
| **Executive lead** | Director of Human Resources and Support Services | | |
| **Review date** | February 2024 | | |
| **Security classification** | Official – Green: unclassified information | | |

| **Proposed groups to present document to:** | | |
|---|---|---|
| IGSG | | |
| | | |

| Date | Version | Group | Reason | Outcome |
|---|---|---|---|---|
| 09/03/21 | 0.1 | IGSG | Professional input and final approval | Approved |
| | | | | |
| | | | | |
| | | | | |

| **Examples of reasons for presenting to the group** | **Examples of outcomes following meeting** |
|---|---|
| • Professional input required re: content (PI) | • Significant changes to content required – refer to Executive Lead for guidance (SC) |
| • Professional opinion on content (PO) | • To amend content & re-submit to group (AC&R) |
| • General comments/suggestions (C/S) | • For minor revisions (e.g. format/layout) – no need to re-submit to group (MR) |
| • For information only (FIO) | • Recommend proceeding to next stage (PRO) |
| • For proofing/formatting (PF) | • For upload to Intranet (INT) |
| • Final Approval (FA) | • Approved (A) or Not Approved, revisions required (NARR) |

***To be attached to the document under development/review and presented to the relevant group**

**Please record details of any changes made to the document in the table below**

| Date | Record of changes made to document |
|---|---|
| 26/01/2021 | Document adapted from NSS original. Changes made to formatting for accessibility and compliance with Framework for Document Development. Screenshot replaced and alt-text added. Added local contact details and corrected minor errors (links to non-existent/accessible documents). Saved as version 0.1 |
| 09/03/2021 | Approved at IGSG and saved as version 1.0 |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

**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 or 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. The 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:

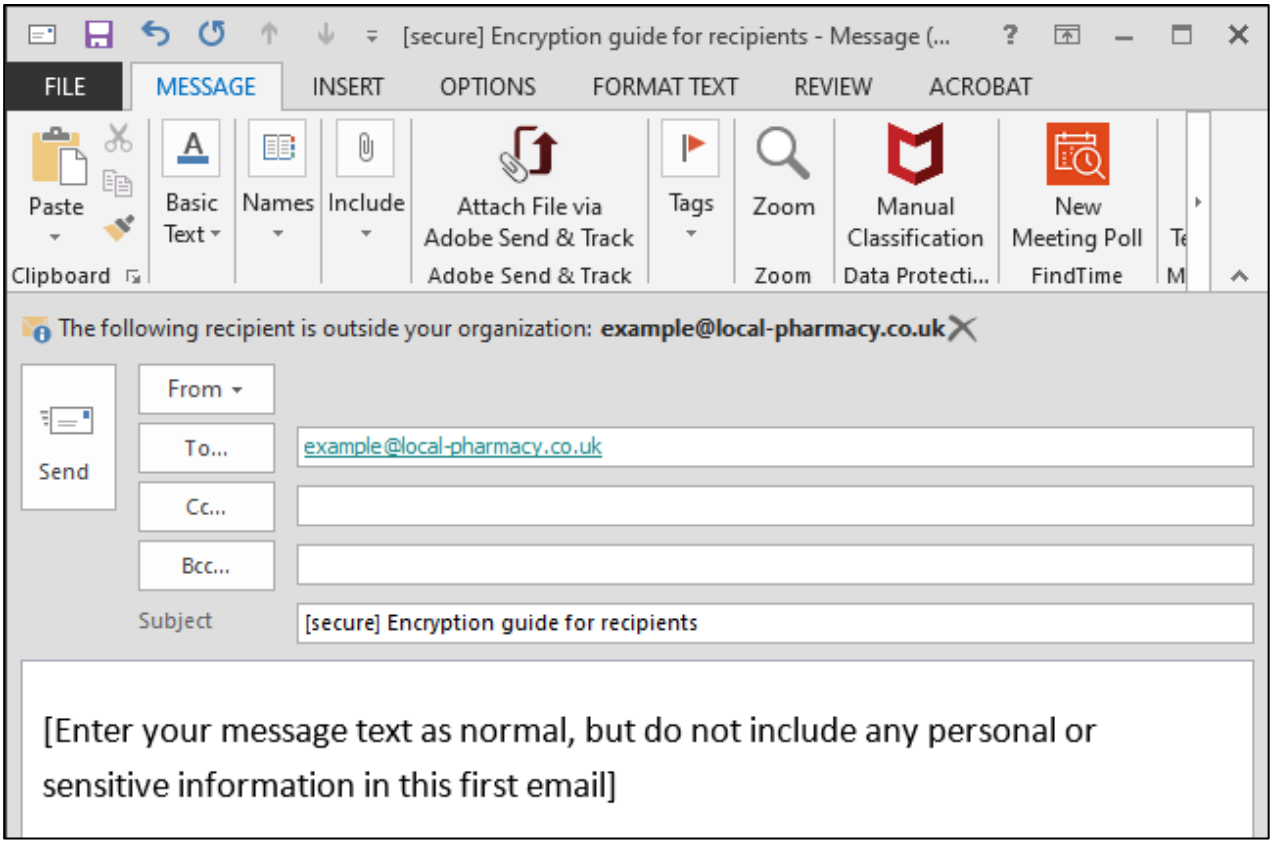
- Send the recipient the **Accessing encrypted emails – guide for non-O365 email users**. This guide will give instructions on what to expect the first time an encrypted email is received.
- Send the recipient an initial encrypted email (as per the instructions in section 5.1) but do not include patient or sensitive information the first time. This first email is to set-up the secure channel of communication and ensure the correct person has received the 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 from within the nhs.scot email service as an email or as an attachment, subject to local governance policies. Please be aware the user cannot register for the service until they have received an encrypted email.

### 5.1. Procedure to send an encrypted email

Follow the steps below 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.

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




5. Compose your message as normal, but do not include personal or sensitive information in this first email.
6. Send the message as normal; 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 any attachments.

The service will then encrypt messages and deliver them 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.

## 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 policies and procedures.

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, the email will not be sent and you will receive an 'undeliverable message' alert.

## 7. Data protection

It is the user's responsibility and legal duty under the Data Protection Act 2018, on behalf of NHS Shetland, to safeguard any data sent to another organisation in line with the data protection and information governance requirements agreed between NHS Shetland and the receiving organisation. If required, you should retain unencrypted copies of any encrypted email received in your local information repositories in accordance with local information management policies and processes and the Scottish Government Records Management Health and Social Care Code of Practice.

## 8. Help and further guidance

For help and further guidance, you can contact:

- NHS Shetland IT Service Desk http://intranet/departments/it/index.html
- National O365 Support (NOS) Team helpdesk on the ServiceNow Portal http://nhsnss.service-now.com/teams
- National Services Scotland (NSS) Information Technology (IT) customer support desk by telephone (0131 275 7777 and option 1)

**End of document**