Accessing encrypted emails – guide for non-O365 email users

Approval date:	**March 2021**
Version number:	**1.0**
Author:	**Sam Collier, Senior IG Officer and Deputy DPO** **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: HRGUI003

NHS Shetland Document Development Coversheet*

Name of document	Accessing encrypted emails – guide for non-O365 email users		
Document reference number	HRGUI003	**New or Review?**	New
Author	Sam Collier, Senior IG Officer and Deputy DPO NHS Scotland Office 365 Cloud and Computing Programme, 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
25/02/2021	Document adapted from NSS original. Changes made to formatting for accessibility and compliance with Framework for Document Development. Screenshots replaced and alt-text added. Some minor errors corrected. Saved as version 0.1
09/03/2021	Approved at IGSG and saved as version 1.0

Contents

1. Introduction 5
2. Purpose of the document 5
3. How encryption is applied 5
4. Receiving an encrypted email 6
Option 1 – sign in to the email account to which the encrypted email was sent 6
Option 2 – one-time passcode 7

1. Introduction

This guide is specific to the NHS Scotland Office 365 email service. It does not replace any NHS Scotland or NHS Shetland policies.

This guide is part of the NHS Scotland Office 365 Email Governance Framework (OEGF). It is a supporting document to the overarching NHS Scotland Office 365 Email Policy.

This document provides guidance for recipients of encrypted emails which have been sent from an O365 email account. It explains how to open and read encrypted emails ensuring sensitive information that has been received remains secure.

O365 email is a national secure collaboration service for health and social care, designed to enable the secure exchange of information. O365 email users can send secure, encrypted emails to any free global hosted email services such as Gmail / Hotmail and other privately-run email services.

Please note, it is not possible for anyone other than an O365 email user to initiate an encrypted email exchange using the O365 email encryption feature.

2. Purpose of the 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 recipients of email from NHS Shetland O365 email and gives information on how to use the encryption feature.

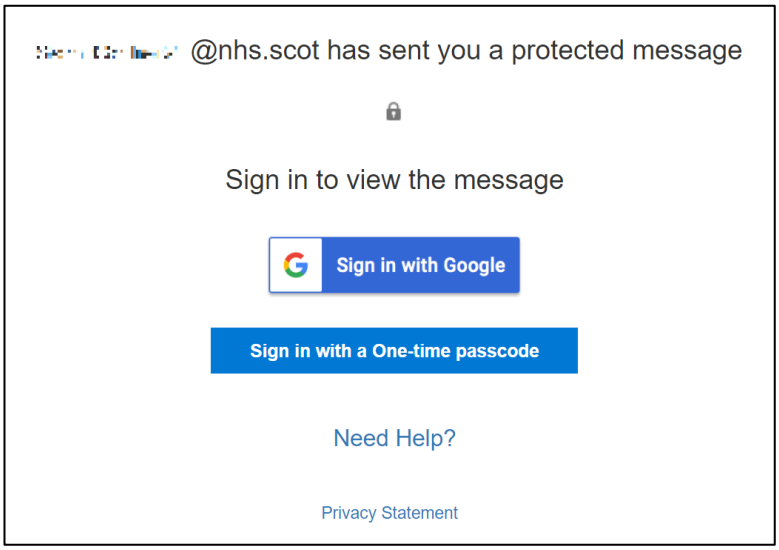
3. How encryption is applied

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. Receiving an encrypted email

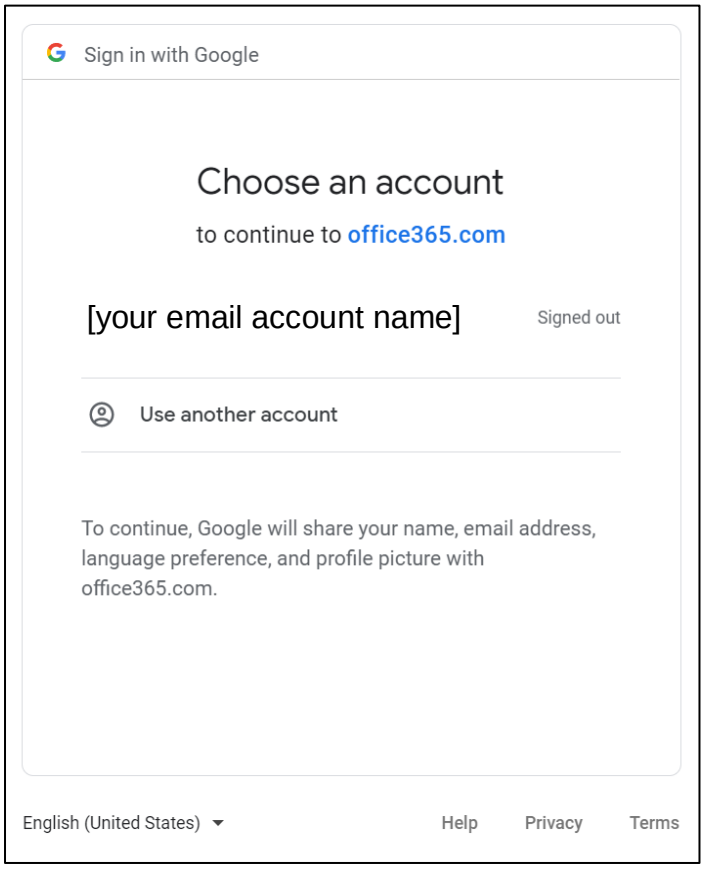
An encrypted email sent from an O365 email address (ending @nhs.scot or @nhs.net) will contain a link to access the encrypted message. Clicking on the link will take you a page with two options to access the encrypted email:



This screenshot is from Gmail, but other email systems such as Yahoo, Hotmail, Outlook, Zoho or iCloud will have a similar page including both options.

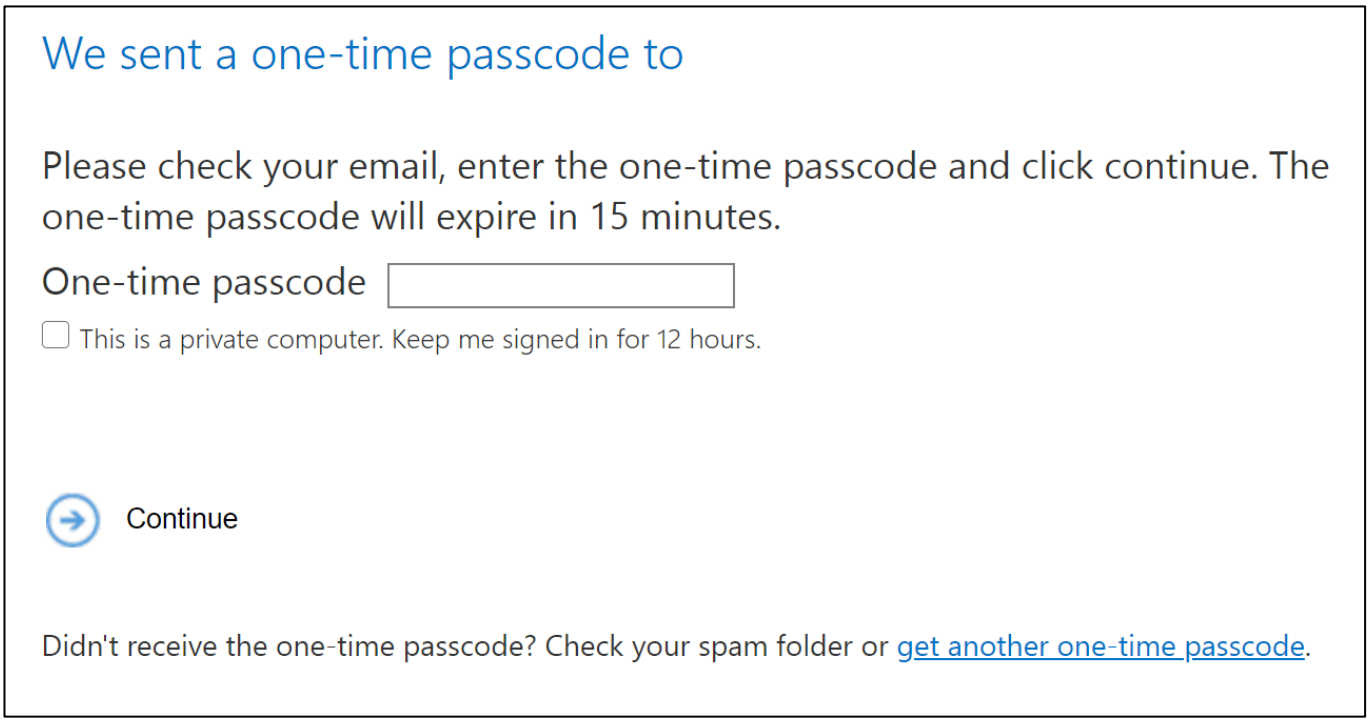
Option 1 – sign in to the email account to which the encrypted email was sent

Selecting the first option ('Sign in with Google' in the screenshot above) should display a page where you can select your account, sign in and then read the encrypted email:

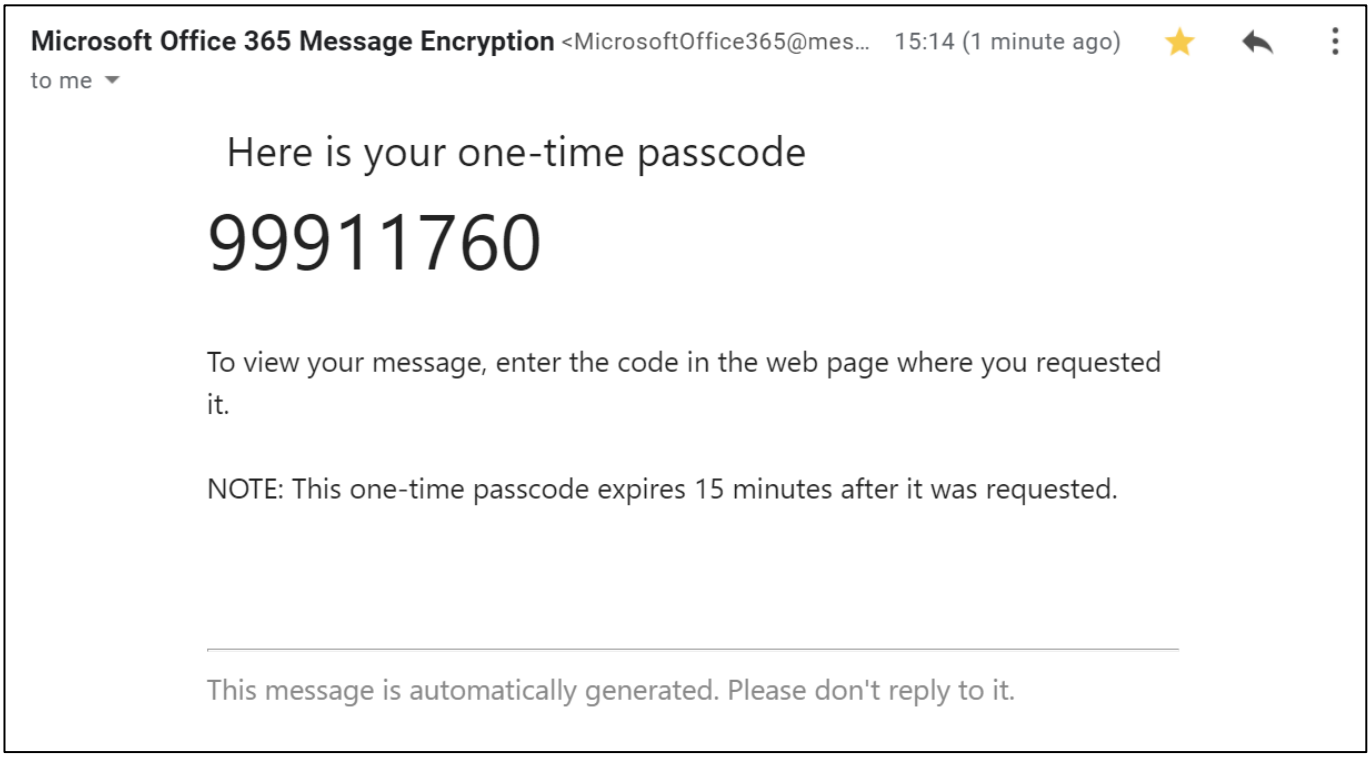


Option 2 – one-time passcode

If you opt for using a one-time passcode, the following screen will appear informing you that the passcode has been sent to your email address:



You will need to check your email for the one-time passcode – the email will look like this:



Follow the instructions and enter the passcode to access the encrypted Email.

End of document