Information Security Policy
Email Acceptable Usage

Author:	**Information Security Manager**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Quality Assurance and Improvement Committee**
Governance or Assurance Committee	**Information Governance and Cyber Assurance Committee**
Implementation Date:	**September 2010**
Version Number:	**2.6.15**
Last Review Date:	**Nov 2023**
Review Date:	**Nov 2026**

CONTENTS

i) Consultation and Distribution Record
ii) Change Record

1. INTRODUCTION

2. AIM, PURPOSE AND OUTCOMES

3. SCOPE
   3.1 Who are the Stakeholders

4. INFORMATION SECURITY

5. EFFICIENT COMMUNICATION

6. SMS COMMUNICATION

7. MANAGERIAL AUTHORITY

8. EXTRA BITS AND BOBS

9. EXTERNAL CONTRACTORS AND THIRD PARTIES

10. ROLES AND RESPONSIBILITIES

11. RESOURCE IMPLICATIONS

12. COMMUNICATION PLAN

13. QUALITY IMPROVEMENT – MONITORING AND REVIEW

14. EQUALITY AND DIVERSITY IMPACT ASSESSMENT

15. SUMMARY OF POLICY / FAQS

16 REFERENCES – APPENDIX 1

17. Advisory Leaflet for Patients – Using Email to Communicate with NHS Lanarkshire – APPENDIX 2

18. Instructions on How to Send Sensitive Information using email to a Patient – APPENDIX 3

19. Reporting Unsolicited Email (SPAM) – APPENDIX 4

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Alan Ashforth, Information Security Manager
Consultation Process / Stakeholders:	• Donald Wilson, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance and Cyber Assurance Committee
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
Mar 2006	A Ashforth	Revised in view of new policy template	1.0
Mar 2007	A Ashforth	Revised in view of new policy template	1.0
Sept 2010	A Ashforth	Revised in view of new policy template	2.0
Sept 2012	A Ashforth	Revised in view of comments	2.1
May 2013	C Tannahill	Revised in view of comments	2.2
May 2014	A Ashforth	Section 4 – sub-section Steps for Sending Information by email New labelling for sensitive email sent to partner organisations Section 4 – Sensitive email – new point – There is no requirement to use password protection of attached documents	2.3
Aug 2014	A Ashforth & C Tannahill	Minor change – Reference appendix updated and some rewording throughout	2.4
Aug 2015	A Ashforth	Minor change – Reference appendix	2.5
Sept 2015	A Ashforth	Minor change – Section 4 added gov.scot email domain	2.5.1
Mar 2016	A Ashforth	Minor changes – Section 4 Red reference to allow sensitive email to send from lanarkshire.scot.nhs.uk to 3orthland.gov.uk Amber reference to BCC and CC, and Section 5 Recall external email and Mail Merge	2.5.2

Jun 2016	A Ashforth	Minor change – Section 4 Red reference to allow sensitive email to send from lanarkshire.scot.nhs.uk to 4orthland.gcsx.gov.uk	2.5.3
July 2016	A Ashforth	Minor change – Section 4 Red reference to allow sensitive email to send from lanarkshire.scot.nhs.uk to culturenl.co.uk	2.5.4
Oct 2016	A Ashforth	Reviewed in line with SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)	2.5.5
April 2017	A Ashforth	Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.6
April 2018	A Ashforth	Reviewed in line with General Data Protection Regulation (GDPR)	2.6
June 2018	A Ashforth	Updated to show new director of information and digital technology	2.6.1
July 2018	A Ashforth	Section 5: Added additional email housekeeping tips as well as email etiquette for improved productivity. Section 4: Included summary advice on General Data Protection Regulation (GDPR), Freedom of Information (FOI), Subject Access Request (SAR). Section 4: Added new guidance for sending information categorized as 'red' sensitive to patients using NHSmail Encryption Feature. See 'Handling Instructions for emailing patients sensitive information when using NHSmail Encryption Feature' Added new Appendix 2 'Instructions on How to Send Sensitive Information using email to a Patient' Added new Appendix 3 'Advisory Leaflet for Patients – Using Email to Communicate with NHS Lanarkshire' Section 5: Added new SPAM reporting process in Appendix 4. Added new Appendix 4 'Reporting Unsolicited Email (SPAM)'	2.6.2
Aug 2018	A Ashforth	Updated reference to Data Protection Act 2018	2.6.3
Sept 2018	A Ashforth	Data protection statement added into Section 3 – Stakeholders	2.6.4
Oct 2018	A Ashforth	Adapt IS policy for use in General Practice	2.6.5
Dec 2018	A Ashforth	Identify South Lanarkshire council email domains 'southlanarkshire.gov.uk' and 'southlanarkshireleisure.co.uk' as Gsi equivalent for sending red sensitive email using NHSmail	2.6.6

Jan 2019	A Ashforth	Replace last two bullets of 'Insecure – Amber' item in classification of sensitivity table with:- All Sensitive information including a patient's Health Record must be treated according to 'Secure – Red (Personally Identifiable Information)' classification of sensitivity Provided examples of approved email methods for RED sensitive email. Changes to 'Appendix 3 – Advisory Leaflet for Patients – Using Email to Communicate with NHS Lanarkshire' to make the leaflet easier to understand including new para on "Replying to secure email sent from the NHS"	2.6.7
March 2019	A Ashforth	As a result of the decommissioning of GSI/GCSX email domains by March 2019, the gsi.gov.uk, gsx.gov.uk, gcsx.gov.uk, gse.gov.uk, scn.gov.uk email domains have been replaced with *.gov.uk, and a further email domain *.parliament.uk added, as safe government email domains when sending from NHSmail. Also, removed all other references to GCSX email domains. See section 4 'Secure – Red (Personally Identifiable Information)' classification of sensitivity, as follows:- *.gov.scot for Scottish Government *.gov.uk for Local & Central Government *.pnn.police.uk for Police *.cjsm.net for Criminal Justice *.mod.uk for Ministry of Defence *.parliament.uk for Parliament	2.6.8
June 2019	A Ashforth	Identify South Lanarkshire council email domains 'southlanarkshire.gov.uk' and 'southlanarkshireleisure.co.uk' as approved for sending red sensitive email using 'lanarkshire.scot.nhs.uk' email	2.6.9
Nov 2019	A Ashforth	Change all references to NHSmail/nhs.net to NHSmail (nhs.net). Also, changed order of sending sensitive email table to use 'lanarkshire.scot.nhs.uk' email for sending to NHS domains and NHSmail (nhs.net) and NLC and SLC then use NHSmail (nhs.net) to send to central and other local government organizations.	2.6.10
June 2021	A Ashforth	Scheduled review including updated UK GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section. Added SWAN SFT alternative to Email for sending documents.	2.6.11
June 2021	A Ashforth	Reviewed in relation to migration to Microsoft 365 Email such that all references to sending	2.6.11

		[SECURE] email using NHSmail is replaced with the process of doing so using M365 providing the sending lanarkshire.scot.nhs.uk mailbox has been migrated to M365. Section 4 - 'STEPS for Sending Information by email' - 'Secure - Red' - changed government secure email boundary • remove all council email domains non-gov.uk in line with M365 safe domains • remove Scot.gov and CJSM.net but provide note on use of M365 Email Encryption Feature for sending red sensitive email to these domains. Section 4 - 'STEPS for Sending Information by email' - 2nd page of 'Secure - Red (Person Identifiable Information and Commercially Sensitive Information)' - added SWAN SFT as safe alternative to email at bottom of 2nd page. General – Replaced all references of 'NHSmail Email Encryption Feature' to 'M365 Email Encryption Feature'. General - Remove all references to sending email using NHSmail and replaced with @lanarkshire.scot.nhs.uk email. Section 5 - Added link to Email Etiquette guidance on Firstport. Section 5 - 'Unsolicited Email (Junk and Phishing)' changed to reference guide 'Managing and Reporting Junk and Phishing email' hosted on Firstport. Appendix 1 – Added links to NHSS M365 secure email policy and governance framework hosted on Firstport. Appendix 2 – Added 'Opening Email Replies from a Patient' and 'Replying to a Patient'. Appendix 2 – Referred to national and local guidance on M365 Email encryption hosted on Firstport. Appendix 2 & 3 - Removed the process for recipients to enroll with a third party such as Egress to read encrypted email.	

		Appendix 4 - Updated Appendix 4 for reporting SPAM.	
Jan 2022	A Ashforth	Section 4 (page 10) - 'STEPS for Sending Information by email' - 'Secure - Red' - changed government secure email boundary • change CJSM.net to safe domain for sending red sensitive email to this domain. • Send from nhs.scot to viatris.com	2.6.12
Mar 2022	A Ashforth	Section 4 (page 10) - 'STEPS for Sending Information by email' - 'Secure - Red' – added @scotland.police.uk for Police Scotland domain	2.6.13
Oct 2022	A Ashforth	Missing label for 'Insecure – Amber' in 'STEPS for Sending Information by email' table on page 11 reinserted to table	2.6.14
Nov 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. Page 11 *.gov.scot is now a secure domain. Page 11 removed 'See next section for more details on how to check that your mailbox has been migrated to M365 and how to send using M365 Email Encryption Feature.' As all mailboxes cloud based. References Appendix 1 – updated including all links to NHSS M365 documents on Firstport. Page 23 – Appendix 3 – removed 'Check your mailbox has been migrated to M365'. Page 25 – Appendix 4 – removed all references to checking your mailbox has been migrated to M365'. Added Leavers section to 7. Managerial Authority.	2.6.15

1. Introduction

This policy relates to Email Usage and forms part of the overall Information Security policy for NHS Lanarkshire (NHSL). NHSL are currently in a transition to Microsoft 365 (M365), so some elements of the policy have been modified to cover this transition.

2. Aim, Purpose and Outcomes

- To ensure that INFORMATION SECURITY is maintained
  - Ensure that confidentiality and integrity of personal and sensitive information is maintained
  - Ensure that information is available to ***authorised*** users
  - Ensure that information is not disclosed to ***unauthorised*** people
  - To prevent ***destruction*** of information
  - Risks associated with email use are reduced.

- To ensure that email communication is as EFFICIENT as possible
  - To ensure that NHSL activities are not disrupted by poor email use
  - To ensure that email is used cost-effectively
  - To describe the ***appropriate*** use of email

- To establish MANAGERIAL AUTHORITY over NHSL email communications

This policy forms part of the Information Security Management System (ISMS) and should be read in conjunction with all the IS policies.

This policy has been written in line with the best practice for information security standards ISO 27001 and ISO 27002 and the policy will be reviewed to meet future changes to this standard.

This policy has been written to comply with current legislation and the policy will be updated appropriately to suit new and/or modified legislation. The references appendix (Appendix 1) will be updated to reflect this legislation.

3. Scope

This policy is intended for all NHS Lanarkshire staff to maintain information security. In the interests of clarity all references to 'staff' includes all staff within NHS Lanarkshire and all staff who are employed, engaged or partners within each GP practice (contracted to NHS Lanarkshire).

3.1 Who are the Stakeholders?

All staff.

NHS Lanarkshire take care to ensure personal information is only accessible to authorised people. Our staff have a legal and contractual duty to keep personal health information secure, and confidential. In order to find out more about current data protection legislation and how we process information, please visit the Data Protection Notice on our website at www.nhslanarkshire.scot.nhs.uk.

4. Information Security

All data hosted by NHS Lanarkshire including email is subject to the same data protection laws as other communication systems.

- General Data Protection Regulation (**GDPR**) requires strong security in place to protect person identifiable information held in email, information that needs to be accurate. Out of date or irrelevant information could breach **GDPR** and result in NHSL being fined.

- Freedom of Information (**FOI**) and Subject Access Request (**SAR**), relevant information may be reported under **FOI** or current data protection legislation in the form of a **SAR**. Staff should think about the content of the emails they send as these could be disclosed to a requester.

NHS Lanarkshire does not perform automatic archiving of emails, so it is necessary for staff to keep relevant emails in line with appropriate legislation and retention policies.

- Protect Access to your mailbox:
  - ✓ Staff must take precautions to ensure that other staff cannot access their emails.

- If you're going to be away from your computer:
  - ✓ Lock it

- If you're going to be away for one or more days:
  - ✓ Staff can give delegated access to their email
    - ✗ but other staff do not require your user ID and password
  - ✓ Staff may auto-forward emails to other staff members if they are going to be away,
    - ✗ but not to a non-NHS email address

STEPS for Sending Information by email

Classification of Sensitivity	Handling of email
Secure - Red **(Person Identifiable Information and Commercially Sensitive Information)** **If Lost or Sent to the Wrong Recipient:** ✓ **Could cause distress** ✓ **Could identify individuals** ✓ **Could undermine confidence in service** ✓ **Could release commercially sensitive information**	**Email Address:** ✓ Send from **lanarkshire.scot.nhs.uk** or **nhs.scot** to domains within government secure email boundary ✓ ***.scot.nhs.uk** ✓ **@nhs.scot** ✓ **@nhs.net** ✓ ***.gov.uk for local & central Government** ✓ ***.gov.scot** ✓ ***.cjsm.net** ✓ **@scotland.police.uk & *.pnn.police.uk for Police** ✓ ***.mod.uk for Ministry of Defence** ✓ ***.parliament.uk for Parliament** e.g. Tim.Kit@lanarkshire.scot.nhs.uk to Henry.Smit@ggc.scot.nhs.uk Tim.Kit@lanarkshire.scot.nhs.uk to Torvil.Hand@nhs.scot Tim.Kit@lanarkshire.scot.nhs.uk to Henry.Smit@nhs.net Torvil.Hand@nhs.scot to Henry.Smit@ggc.scot.nhs.uk Tim.Kit@lanarkshire.scot.nhs.uk to SmythA@northlan.gov.uk Tim.Kit@lanarkshire.scot.nhs.uk to GregA@southlanarkshire.gov.uk ✓ Send from **nhs.scot** to **viatris.com** ✓ Send from **lanarkshire.scot.nhs.uk** to an email domain accredited to the NHS Digital secure email standard as listed in NHS Digital DCB1596, such as a care home or another 3rd party supplier **Handling Instructions:** ✓ There is a legitimate need to access/share information ✓ Check recipient addresses carefully ✓ One email = one patient, under no circumstances should the blind copy (bcc) or copy (cc) be used to send to a patient. ✓ Do not include personal details in the subject line ✓ You must add "**OFFICIAL - SENSITIVE**" to the subject line when emailing external partner agencies ✓ There is no requirement to use password protection of attached documents ✓ Never send to unconnected organisation, patients or wider public ✓ Never send from personal email account hotmail/gmail

Secure - Red (Person Identifiable Information and Commercially Sensitive Information) **If Lost or Sent to the Wrong Recipient:** ✓ **Could cause distress** ✓ **Could identify individuals** ✓ **Could undermine confidence in service** ✓ **Could release commercially sensitive information**	**The following process can be used to respond to Subject Access Requests by General Practice. Any other service wishing to use the process below must seek approval from the Head of Health Records or Information Governance Team.** **Email Address:** ✓ Send from NHS Lanarkshire to a patient's personal email address using M365 Email Encryption Feature using "[secure]" at the start of the subject line **Handling Instructions for emailing patients sensitive information when using M365 Encryption Feature:** ✓ Patient has given consent to emailed communication ✓ Must send an introductory email to the patient including **Appendix 2** which has advice over the security of the service and the implications and their responsibilites when using the service ✓ Check the patient responds indicating they are happy to participate in the service ✓ Verify that it is the correct patient and corresponding email address ✓ Must send a test secure message by adding **"[secure]"** before the subject of the email ✓ One email = one patient, under no circumstances should the blind copy (bcc) or copy (cc) be used to send to a patient. ✓ Use the check list given in the 'Patient Mailing Policy' to verify that that the intended content is appropriate and authorised to be sent to the patient ✓ Agree purpose: ✓ Subject Access Reports See **Appendix 3** for detailed instructions on how to send sensitive Information using email to a patient. Safe alternative to email is to use the SWAN Secure File Transfer Service, see SWAN SFT user manual on Firstport.
Insecure - Amber (With consent of Individual or Patient) **If Lost or Sent to the Wrong Recipient:**	**Email:** **SMS:** Reply to email sent by patient or verify address prior to sending. Reply to SMS sent by patients or verify number

✓ **Could cause distress** ✓ **Could identify individuals**	**Handling Instructions:** ✓ Must add "**OFFICIAL**" to the subject line when emailing external partner agencies ✓ Patient has given consent to emailed communication ✓ One email = one patient, under no circumstances should the blind copy (bcc) or copy (cc) be used to send to a patient ✓ Emails are professional (not personal) ✓ Agree purpose: ☑ Record agreement within health record ☑ Keeping in touch ☑ Appointments ☑ Emailing a relative abroad about patient status ☑ Reply to complaints and FOI requests ✗ All Sensitive information including a patient's Health Record must be treated according to Secure - Red (Personally Identifiable Information) classification of sensitivity
Insecure - Green (Unclassified) **If Lost or Sent to the Wrong Recipient:** ✓ Will not cause distress ✓ Will not breach confidence ✓ Will not cause financial or other harm ✓ Does not refer to person's physical or mental state	**Email:** **SMS**: Any **Handling Instructions:** No specific handling instructions Send to anyone with a legitimate need to see information

5. Efficient Communication

Every email sent creates a recorded profile of the sender and the organisation, therefore email correspondence must conform to expectations for professional business conduct. All staff should be familiar with, and comply with the NHSL Email Usage Policy.

Email should be used judiciously and in the first instance consideration should be given as to whether it is the best medium for achieving an objective. Emails should be succinct and have a clear message and clear expectation on whether a response or specific action is required from the recipient.

NHSL has introduced a prefix standard for the Subject Line in emails. This indicates the purpose of the email and the expected response (or not). This will help everyone manage and prioritise their e-mails. See the examples for the prefixes you can use.

NHS Email Etiquette: Improving Productivity and Managing Risks			
The prefixes adopted are listed opposite:	**Prefix**		**Description**
	[ACTION]	[ACT]	Action Required/For Action
	[FOR INFO]	[FYI]	For Your Information
	[REMINDER]		Reminder
	[REQUEST]	[REQ]	Request
	[URGENT]	[URG]	Urgent - use sparingly considering the importance to person you are sending the email to
	[SOCIAL]	[SOC]	e.g. department night out
	[EOM] (suffix)		End of Message - for example Fire Alarm today at 3pm saves recipient opening full email.
For Example:	Subject:	[FOR INFO] Fire Alarm test today at 11am Law House [EOM]	

See Email Etiquette poster for more details on Firstport

- Kinds of activities
  - ✓ NHSL Email must be used to support NHSL ***business activities***
  - ✓ NHSL emails sent to people outside NHSL must be for ***legitimate business purposes***
  - ✓ Personal use is permitted as long as it is reasonable
  - ✗ NHSL Email may not be used for ***illegal*** activities

- Use Do's and Don'ts:
  - ✓ Before sending email, consider whether email is the best way to communicate for the purpose. Sometimes it is better to phone or speak to someone directly (especially when the information is required at short notice e.g. late cancellation of a meeting).
  - ✓ Keep emails professional, short and concise
  - ✓ Do take care on the content of emails as they may be disclosed in an FOI or a Subject Access Report
  - ✓ Minimise small talk;
  - ✓ Be courteous
  - ✓ Use descriptive words
  - ✓ Use the subject line to highlight the email purpose and content
  - ✓ Do re-read your message before you send it and use spell check
  - ✓ Use the out of office facility
  - ✓ Do take responsibility for letting the senders of routine e-mails know if you no longer require them
  - ✓ Do update distribution lists
  - ✓ Do give some thought before attaching "emails to emails"
  - ✓ Do use common sense and respect for busy colleagues
  - ✗ Don't keep emails longer than required

- ✗ Don't keep emails that are inaccurate or not relevant as they may be reported may breach current data protection legislation or provide misleading information if disclosed in a SAR
- ✗ Don't copy to everyone. Think about who will have to deal with this email and don't waste people's time.
- ✗ Records should not be kept only in emails. Store them in a central space where other staff members can access them
- ✗ Don't customise email format so that it creates additional effort to read
- ✗ DON'T USE CAPITALS TO WRITE AN EMAIL: THIS IS SEEN AS SHOUTING!
- ✗ Don't use multiple addresses cc and bcc "*just to be safe*"
- ✗ Don't mark an email urgent unless it is
- ✗ Don't print off all emails
- ✗ Don't send to a group e-mail address unless appropriate. Send group e-mail only when it's useful to every person
- ✗ Don't allow email to control your day

- Be careful:
  - ✗ Don't use sharp comments. Remember that the person only sees the words, and not your facial expression, so don't be too informal
  - ✗ Don't react to email comments in the heat of the moment. Breathe, read it again, and then reply
  - ✗ Don't make derogatory comments
  - ✗ Don't reply to "**all**" - consider who needs to see reply
  - ✗ Don't reply to out-of-office messages
  - ✗ Don't send offensive emails and report any you receive
  - ✗ Don't send, copy or forward anything that could be libelous (untrue/false), sensitive or offensive
  - ✗ Don't send an e-mail if the wording could be considered rude or offensive
  - ⚠ Requesting a delivery report increases email traffic so use this option only when you need to.
  - ⚠ Emails can be forwarded but only if you have permission from the sender to do so
  - ⚠ Once you click on the "Send" button you have no further control over the email, in particular the recall function is not possible for emails sent outside the organisation
  - ⚠ Use mail merge to send the same email to a list of recipients, one recipient at a time, please contact the Service Desk for advice on the use of mail merge

- Space saving
  - ✓ Do undertake routine housekeeping and clear out old messages that are no longer required
  - ✗ Don't send huge files as attachments

- Unsolicited Email (Junk and Phishing)

All inbound emails to NHS Lanarkshire's corporate email system 'lanarkshire.scot.nhs.uk' are filtered in a number of stages. However, some unsolicited email may still be delivered.

- ✓ Staff are asked to report Junk and Phishing emails to improve detection.
- ✓ If your mailbox has been migrated to M365, use the guide Managing and Reporting Junk and Phishing email to report this to Microsoft. Verify if your mailbox has been migrated to M365, use the instructions **'Check your mailbox has been migrated to M365'** in **Appendix 3**.
- ✓ Otherwise, report to Microsoft by forwarding the original email as an attachment to junk@office365.microsoft.com for Junk mail or to phish@office365.microsoft.com for PHISHING mail. Also, add in spamreports@lanarkshire.scot.nhs.uk.
- ✓ See **Appendix 4 'Reporting Unsolicited Email (SPAM)'** for more details on this process.

6. SMS Communication

- ⚠ SMS is NOT normally considered a secure service for red sensitive information, an alternative method must be used unless the service has been risk assessed, approved for use and explicit consent has been obtained from the patient
- ⚠ SMS is not reliable
- ✓ Make a note in the patient's record when an SMS is sent
- ✓ Message should be maximum 20 words long
- ✓ Stick to alphanumeric text (no special characters)
- ✓ Request Delivery Receipt

7. Managerial Authority

- Legal
  - ⚠ Emails can be used as evidence in a court of law
  - ⚠ Email can be released under the Freedom of Information act (this excludes clinical data unless it is specifically pertinent to an investigation)
- Privacy
  - ✓ Emails will be filtered by software to detect viruses and SPAM. Emails may be quarantined if the screening software considers them risky
  - ⚠ NHSL email is not private
  - ⚠ Email will be monitored by NHSL technical staff and managers (authorized at a senior level)
  - ⚠ Email usage will be monitored and audited
- The emailing software will add a disclaimer to all outgoing emails
- Administrators can remove emails if they consider this action necessary

There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example sick leave. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the current data protection legislation;
- Freedom of Information requests
- Evidence in legal proceedings
- Line of business enquiry
- Conducting an investigation which may result in disciplinary action according to local disciplinary procedures.

Where it is not possible to ask the permission of the member of staff whose mailbox needs to be accessed, the procedure for gaining access to their mailbox is:

- Gain authorisation from the Head of Department
- Submit a request to the Service Desk
- A record will be made of the reason for accessing the mailbox together with the names of the people involved
- Inform the person whose mailbox was accessed

Leaver Process

- ⚠ Your manager must alert the ServiceDesk to disable your network account (and disable access to all clinical access) from your contract end date.
- ⚠ When you leave the board you will have no further access to your mailbox within the Board.
- ⚠ If your mailbox has important information not recorded on departmental folders or clinical system then this data will need reviewed by yourself and your manager before you leave, so that this data can be transferred to internal systems.
- ⚠ The board will NOT normally transfer the contents of the mailbox to another board due to legislation such as FOI. The only exception to this would be a service migrating to the other board with an understanding that the recipient board will be responsible for retrospective FOI and other legislation implications when the staff member transfers.
- ⚠ The board will NOT export the mailbox to external media or cloud storage etc – if you have your own personal information or professional development information within your mailbox then this needs to be filed elsewhere before you leave, and no personally identifiable information must leave the Board.
- ⚠ The board will NOT allow other board staff access to the mailbox after you leave as normally the mailbox will be deleted promptly.

8. Extra Bits and Bobs

- ✓ Problems Emailing:
  - ✓ If an email bounces, investigate yourself before raising the matter with support. It could be as simple as a misspelled email address
  - ✓ If an email bounces back because someone has run out of space, contact them by phone to let them know.
  - ✓ Add an automatic signature to your emails:
    - Click on Tools, Options, General, Email Options: then insert your name, designation, postal address and telephone number.

✗ If you inappropriately send emails from another user's email address it could lead to disciplinary action according to local disciplinary procedures.

9. External Contractors and Third Parties

External Contractors and Third Parties

✓ are expected to fully comply with the terms and conditions of this document whilst using any equipment connected directly or indirectly to NHSL's networking infrastructure.

⚠ Failure to comply or a show of disregard for the terms and conditions of this document may be interpreted as a threat to compromise the security of NHSL's computer network.

⚠ In such an event a Digital representative would

- inform the respective Line Manager of the situation.
- If the matter is not subsequently resolved NHSL would reserve the right to terminate the individuals' access to NHSL's networking infrastructure and computer network *with immediate effect.*

10. ROLES AND RESPONSIBILITIES

Authors/Contributors:	Information Security Manager
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance and Cyber Assurance Committee

11. RESOURCE IMPLICATIONS

None

12. COMMUNICATION PLAN

This policy will be managed through the Corporate Policies intranet site and will be announced through the staff briefing.

13. QUALITY IMPROVEMENT – Monitoring and Review

To be reviewed at regular intervals by Information Security Manager.

14. EQUALITY AND DIVERSITY IMPACT ASSESSMENT

This policy meets NHS Lanarkshire's EDIA. X

(tick box)

15. Summary of Policy/Frequently Asked Questions (FAQs)

N/A

16. REFERENCES

APPENDIX 1

The principal Acts of Parliament, Scottish Government circulars, and internal guidance documents relevant to this policy are:

- UK General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- National Cyber Security Centre Cyber Assurance Framework
- Scottish Government Public Sector Cyber Resilience Framework
- May 2014 Using Email in NHSScotland: A Good Practice Guide
- May 2012 Frequently Asked Questions on new guidance for email in NHSScotland
- CEL 25 (2012) NHS Scotland Mobile Data Protection Standard
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- MEL 2000 (17) Data Protection Act 1998
- NHSL Risk Management Framework
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012
- SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

NHS Scotland (NHSS) now utilises Microsoft 365 (M365) to host mailboxes and as such a number of NHSS M365 Email documents now exist detailing the governance structures & processes in place, as well as the technologies & standards used. These also include an acceptable use policy and more procedural guides such as how to use the M365 Email Encryption Feature.

The NHSS M365 documents exist on Firstport as follows:-

- V1.0 M365 Overarching Email Policy for the M365 Email Governance Framework
- V1.0 M365 Secure Email Policy
- V1.0 M365 Email Acceptable Use Policy
- V2.0 M365 Retention Policy User Guide v02.0
- V1.0 M365 Email Incident Management policy
- V1.0 M365 GDPR Transparency Information for M365 Email
- V1.0 M365 Sending Secure Email User Encryption Guide
- V1.0 M365 Accessing Encrypted Emails Guide for non-M365mail users
- V1.0 M365 Email Access to Data Procedure
- V1.0 M365 Access to Data Request Form
- V1.0 M365 Secure Email Connectors
- V1.0 M365 Secure Email Controls
- V1.0 M365 Microsoft Exchange Online Secure Email Configuration Guidance
- M365 Intune Device Management and App Protection (MDM APP) End user guide

Also, see the SharePoint site for Information Security & Governance for Office 365 email.

17. Advisory Leaflet for Patients - Using Email to Communicate with NHS Lanarkshire

APPENDIX 2

Advisory Leaflet for Patients

The Risks

This leaflet is to provide you, as an NHS Lanarkshire Patient, with information about the risks of receiving and sending emails from/to NHS Lanarkshire from/to your own email address. These e-mails could possibly contain sensitive medical information about you.

Once you have read and understood the risks described in this document, you should be able to make an informed decision on whether or not to use email to communicate with the NHS, especially if they contain personal information.

Emails from NHS Lanarkshire while they are in transit within the Scottish NHS network are secure from interception and hacking.

If an email is sent from the NHS network to you and you have an email like Gmail, Yahoo, Hotmail etc it will enter the internet (otherwise known as the world wide web (www)) – emails are not that safe on the WWW.

The risks to your personal information could be that:

- the information is intercepted and hacked;
- it is not delivered;
- is not delivered promptly;
- it is identified as spam and not put into your inbox;
- the wrong email address is used and it is sent to another person in error (this is the most frequent risk);
- the computer being used to access the email has a virus that allows access to the information provided;
- the internet email provider is hacked and the information is stolen;
- the information is transferred outwith the UK to a country which does not have the same level of privacy laws;
- NHS Lanarkshire will only use your personal information for the purposes of medical care, but if your information gets into the public domain there is a risk that it may be used for other purposes, such as direct marketing or identify theft.

If any of the above examples happen, it could have a serious impact on your privacy and potentially your ongoing health and wellbeing (e.g. you don't get a treatment you need because the email went to your spam folder and you didn't notice). If medical information about you is released into the public domain, it could cause embarrassment, invasion of your privacy and possible consequences regarding, for example, health or life insurance.

NHS Lanarkshire will try to take what steps it can to reduce these risks, however human error and technical glitches may make them ineffective.

Written consent

If you wish to accept the risks stated above and decide to receive information about you your health care provider will ask what types of information you wish to have sent by e-mail and you must give written consent.

You have the right to withdraw your consent at any time and no further e-mails will then be sent to you. To withdraw consent, you should speak to your health care provider, or e-mail or write to them. Communications by email will continue to happen until your health care provider replies, in writing, to your request to withdraw.

You will be asked to renew your consent for e-mails at regular intervals so that our records are kept up to date.

Procedure for e-mails

If you consent to receive e-mails, NHS Lanarkshire will use a procedure for sending encrypted e-mails to you and you will be given instructions on what to do when you receive them, and how to reply securely.

Once you have received the e-mail and attachments you have been sent, it becomes your own responsibility to safeguard the contents.

If you save it to your PC or other device, you will increase the chances of it being hacked, particularly if your device is set to backup data to the internet (Cloud, Dropbox etc). It is also recommended that you delete the e-mail and attachment as soon as you no longer need it, to reduce the risk of loss or hacking.

NHS Lanarkshire will keep the e-mails we have received from and sent to you according to our policy for retention of e-mails.

Receiving secure email from the NHS

After you have given your written consent to receive e-mails:

- You may be asked to email your health care provider first – this should not contain any personal information – it is only completed as a test to ensure your health care provider gets your correct e-mail address.
- You will receive a return e-mail from your health care provider with “[secure]” in the subject heading of the e-mail.
- To open the secure e-mail simply open the email, you may need to click on a link in the email then asked to re-authenticate with your email provided to verify it is you who is opening the email.
- Depending on the email system you use and its compatibility with Microsoft you may be offered to either authenticate or sign in with a One-time passcode. Select the account to be used.
- If you opt to use a one-time pass code a screen will appear informing you that the pass code has been sent to your e-mail address. Follow the instruction to access the encrypted e-mail.

- Check your e-mail for the one-time pass code, enter it on the notification Email and you will then have access to the encrypted e-mail.

Replying to secure e-mail sent from the NHS

You should take care when replying to secure e-mail sent from the NHS. You should be able to make an informed decision on whether or not to you are happy to send sensitive personal information by email to the NHS.

18. Instructions on How to Send Sensitive Information using email to a Patient

APPENDIX 3

How to send an encrypted message?
Before sending patient or other sensitive data via the encryption service, it is good practice to set up the 'encrypted channel' which helps verify the correct recipient and prepares the recipient for receiving the encrypted email:

1. Send the recipient 'Advisory Leaflet for Patients - Using Email to Communicate with NHS Lanarkshire - APPENDIX 2'.
2. 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. If it is an incorrect recipient, data has not been compromised.
3. Create a new email message in the normal way.
4. Ensure the recipient's email address is correct.
5. 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 may potentially be exposed to interception or amendment.
6. Type the message.
7. Click on **send** to send the message. An unencrypted copy will be saved in your **sent items** folder.

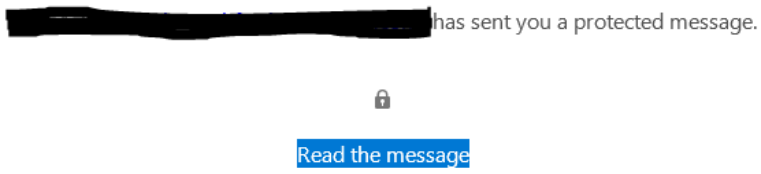
Once the initial process has taken place, you can then send other emails with required attachments providing the **subject** field of the email has the text **[secure]** before the subject of the message.

It should be noted that for the purposes of sharing information in documents it would normally be best to convert these to PDF and send the PDF version instead of Word, Excel and PowerPoint, this is so that the recipient is able to open and read the document, and potentially file it or print it. Unfortunately, if the document is in Word, Excel and PowerPoint format then this document is protected in such a way that it can be previewed only, but not opened and cannot be printed. To export a Microsoft document, open the document then click on File, Export, Create PDF/XPS.

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.

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

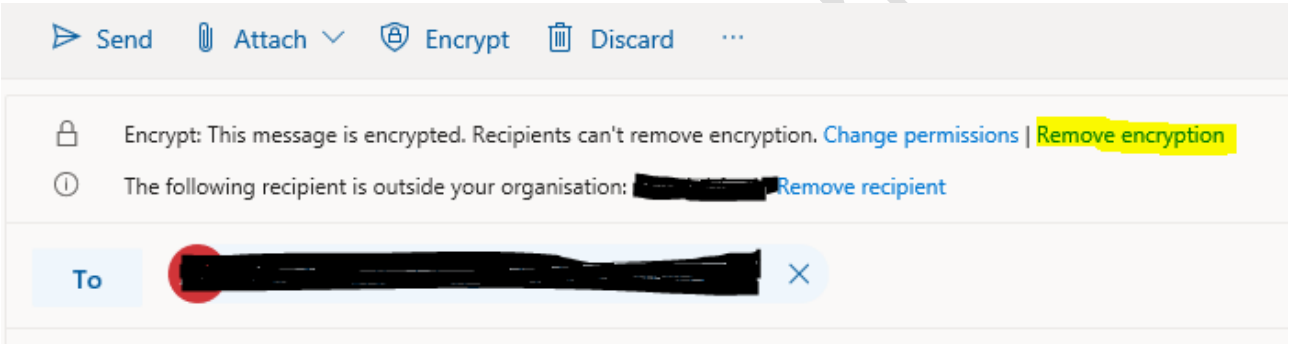
Opening Email Replies from a Patient
All replies received will be retain the encryption and won't be displayed until a link marked 'Read the message' is clicked, on see example reply.



After click on the link, a browser session will be presented and you may be asked to authenticate with Microsoft with secondary authentication (usually a code on your mobile). After being successfully authenticated the email and contents should be presented.

Replying to a Patient
In order to reply to this email (reply to patient), click on 'Reply' in the browser window for the received email.

NB is crucial to retain the secure email channel created earlier by not removing the encryption that was set earlier. See example reply email dialogue in browser window.



DO NOT CLICK ON 'REMOVE ENCRYPTION' as highlighted, as it is essential for the encryption to continue for all of the email conversation.

Limitations
The M365 Encryption Feature will allow sensitive email to be opened by patients that use their own email system to receive the email, however if you engage with someone passing themselves off as another person the process will still work fully but by NHS Lanarkshire sending the sensitive information to an imposter, NHSL will breached current data protection legislation. Always verify the recipient email address is the actual patient concerned.

For the purpose of Subject Access Requests the email address of the patient must be obtained through the request process and validated.

See national guidance V1.0 M365 Sending Secure Email User Encryption Guide and local guidance M365 Email Encryption feature for more details.

19. Reporting Unsolicited Email (SPAM)

APPENDIX 4

Reporting email threats

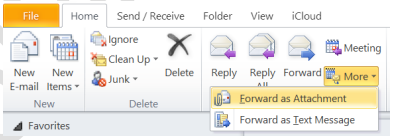
If you receive an email that you suspect to be spam, or suspect may be an attempt to spoof or phish your account, it is extremely important that you report this to Microsoft as well as the NHSL Cyber Security Team (the latter will be used to monitor trends like a targeted Spam/Phishing attack on NHSL). *There is no requirement to raise an IT ServiceDesk call unless the issue is more serious such as persistent abusive senders etc which require to be blocked.*

If you choose to simply mark an email as junk in Outlook, the sender's emails will no longer arrive in your inbox but the threat will not have been reported to Microsoft and may still affect other staff.

Use the guide Managing and Reporting Junk and Phishing email to report this to Microsoft using the new buttons within Outlook.

Alternatively, forward the email to junk@office365.microsoft.com for Junk mail or to phish@office365.microsoft.com for PHISHING mail, and the NHSL Cyber Security Team spamreports@lanarkshire.scot.nhs.uk as an attachment for virus analysis and central trend monitoring:

1. Select the suspect email from your email list
2. In the Outlook ribbon in the respond area, select '**More**' and then select '**Forward as Attachment**'.



3. In the email window that opens add junk@office365.microsoft.com for Junk mail or to phish@office365.microsoft.com for PHISHING mail, and spamreports@lanarkshire.scot.nhs.uk as the recipient in the 'To field'.
4. Click **Send**.