# Information Security Policy

## Email Acceptable Usage

<table>
<thead>
<tr>
<th>Author:</th>
<th>Information Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Lead Executive Director:</td>
<td>Director of Information and Digital Technology</td>
</tr>
<tr>
<td>Endorsing Body:</td>
<td>Healthcare Quality Assurance and Improvement Committee</td>
</tr>
<tr>
<td>Governance or Assurance Committee</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Implementation Date:</td>
<td>September 2010</td>
</tr>
<tr>
<td>Version Number:</td>
<td>2.6.10</td>
</tr>
<tr>
<td>Review Date:</td>
<td>September 2020</td>
</tr>
</tbody>
</table>
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
17. Instructions on How to Send Sensitive Information using email to a Patient – APPENDIX 2

18. Advisory Leaflet for Patients – Using Email to Communicate with NHS Lanarkshire – APPENDIX 3

19. Reporting Unsolicited Email (SPAM) – APPENDIX 4

CONSULTATION AND DISTRIBUTION RECORD

| Contributing Author / Authors | • Alan Ashforth, Information Security Manager, eHealth |
| Consultation Process / Stakeholders: | • Donald Wilson, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) |
| Distribution: | • All staff |

CHANGE RECORD

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Change</th>
<th>Version No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2006</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Mar 2007</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>1.0</td>
</tr>
<tr>
<td>Sept 2010</td>
<td>A Ashforth</td>
<td>Revised in view of new policy template</td>
<td>2.0</td>
</tr>
<tr>
<td>Sept 2012</td>
<td>A Ashforth</td>
<td>Revised in view of comments</td>
<td>2.1</td>
</tr>
<tr>
<td>May 2013</td>
<td>C Tannahill</td>
<td>Revised in view of comments</td>
<td>2.2</td>
</tr>
<tr>
<td>May 2014</td>
<td>A Ashforth</td>
<td>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</td>
<td>2.3</td>
</tr>
<tr>
<td>Aug 2014</td>
<td>A Ashforth &amp; C Tannahill</td>
<td>Minor change – Reference appendix updated and some rewording throughout</td>
<td>2.4</td>
</tr>
<tr>
<td>Aug 2015</td>
<td>A Ashforth</td>
<td>Minor change – Reference appendix</td>
<td>2.5</td>
</tr>
<tr>
<td>Sept 2015</td>
<td>A Ashforth</td>
<td>Minor change – Section 4 added gov.scot email domain</td>
<td>2.5.1</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>A Ashforth</td>
<td>Minor changes – Section 4 Red reference to allow sensitive email to send from lanarkshire.scot.nhs.uk to northland.gov.uk Amber reference to BCC and CC, and Section 5 Recall external email and Mail Merge</td>
<td>2.5.2</td>
</tr>
<tr>
<td>Jun 2016</td>
<td>A Ashforth</td>
<td>Minor change – Section 4 Red reference to</td>
<td>2.5.3</td>
</tr>
<tr>
<td>Date</td>
<td>Author</td>
<td>Description</td>
<td>Version</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>July 2016</td>
<td>A Ashforth</td>
<td>A Minor change – Section 4 Red reference to allow sensitive email to send from lanarkshire.scot.nhs.uk to orthland.gcsx.gov.uk</td>
<td>2.5.4</td>
</tr>
<tr>
<td>April 2017</td>
<td>A Ashforth</td>
<td>A Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.</td>
<td>2.5.6</td>
</tr>
<tr>
<td>April 2018</td>
<td>A Ashforth</td>
<td>Reviewed in line with General Data Protection Regulation (GDPR)</td>
<td>2.6</td>
</tr>
<tr>
<td>June 2018</td>
<td>A Ashforth</td>
<td>Updated to show new director of information and digital technology</td>
<td>2.6.1</td>
</tr>
<tr>
<td>July 2018</td>
<td>A Ashforth</td>
<td>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)’</td>
<td>2.6.2</td>
</tr>
<tr>
<td>Aug 2018</td>
<td>A Ashforth</td>
<td>Updated reference to Data Protection Act 2018</td>
<td>2.6.3</td>
</tr>
<tr>
<td>Sept 2018</td>
<td>A Ashforth</td>
<td>Data protection statement added into Section 3 – Stakeholders</td>
<td>2.6.4</td>
</tr>
<tr>
<td>Oct 2018</td>
<td>A Ashforth</td>
<td>Adapt IS policy for use in General Practice</td>
<td>2.6.5</td>
</tr>
<tr>
<td>Dec 2018</td>
<td>A Ashforth</td>
<td>Identify South Lanarkshire council email domains ‘southlanarkshire.gov.uk’ and ‘southlanarkshireleisure.co.uk’ as Gsi equivalent for sending red sensitive email using NHSmail</td>
<td>2.6.6</td>
</tr>
<tr>
<td>Jan 2019</td>
<td>A Ashforth</td>
<td>Replace last two bullets of ‘Insecure – Amber’ item in classification of sensitivity table with:- All Sensitive information including a patient’s</td>
<td>2.6.7</td>
</tr>
</tbody>
</table>
## Information Security Policy – Email Acceptable Usage

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Description</th>
<th>Version No.</th>
</tr>
</thead>
</table>
| 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      |
| May 2020   | K. Torrance  | Extended until September 2021 (COVID-19)                                                                                                                                                                     | 2.6.10      |
1. **Introduction**

This policy relates to Email Usage and forms part of the overall Information Security policy for NHS Lanarkshire (NHSL).

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 eHealth 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 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 your 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 your information, please visit the Data Protection Notice on our website at [www.nhs lanarkshire.scot.nhs.uk](http://www.nhs lanarkshire.scot.nhs.uk) or ask a member of staff for a copy of our Data Protection Notice.

### 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, 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

<table>
<thead>
<tr>
<th>Classification of Sensitivity</th>
<th>Handling of email</th>
</tr>
</thead>
</table>
| **Secure - Red** (Person Identifiable Information and Commercially Sensitive Information) | **Email Address:**
|   | ✓ Send from/to NHS Scotland *(NHSmail (nhs.net), lanarkshire.scot.nhs.uk, ggc.scot.nhs.uk etc.)*
|   |   e.g. Tim.Kit@lanarkshire.scot.nhs.uk to Henry.Smit@ggc.scot.nhs.uk
|   |   Tim.Kit@lanarkshire.scot.nhs.uk to Henry.Smit@nhs.net
|   |   Tim.Kit@nhs.net to Henry.Smit@nhs.net
|   | ✓ Send from **lanarkshire.scot.nhs.uk** to **northlan.gov.uk** and **culturenl.co.uk**
|   |   e.g. Tim.Kit@lanarkshire.scot.nhs.uk to SmythA@northlan.gov.uk
|   |   Tim.Kit@lanarkshire.scot.nhs.uk to Smarty@culturenl.co.uk
|   | ✓ Send from **lanarkshire.scot.nhs.uk** to **southlanarkshire.gov.uk** and **southlanarkshireleisure.gov.uk**
|   |   e.g. Tim.Kit@lanarkshire.scot.nhs.uk to GregA@southlanarkshire.gov.uk
|   |   Tim.Kit@lanarkshire.scot.nhs.uk to BobC@southlanarkshireleisure.co.uk
|   | ✓ Send to GSI Equivalency partner from NHSmail (nhs.net) ONLY
|   |   ✓ *.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
| **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 e.g. hotmail, gmail etc. |   |
Information Security Policy – Email Acceptable Usage

<table>
<thead>
<tr>
<th>Secure - Red (Person Identifiable Information and Commercially Sensitive Information)</th>
<th>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 consent from the Head of Health Records.</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Lost or Sent to the Wrong Recipient:</td>
<td>Email Address:</td>
</tr>
<tr>
<td>✓ Could cause distress</td>
<td>✓ Send from NHSmail (nhs.net) to a patient’s personal email address using NHSmail Encryption Feature using “[secure]” at the start of the subject line</td>
</tr>
<tr>
<td>✓ Could identify individuals</td>
<td>Handling Instructions for emailing patients sensitive information when using NHSmail Encryption Feature:</td>
</tr>
<tr>
<td>✓ Could undermine confidence in service</td>
<td>✓ Patient has given consent to emailed communication</td>
</tr>
<tr>
<td>✓ Could release commercially sensitive information</td>
<td>Must send an introductory email to the patient including Appendix 3 which has instructions on how to enrol for the service and advice over the security of the service and the implications and their responsibilities when using the service</td>
</tr>
<tr>
<td></td>
<td>✓ Check the patient responds indicating they have enrolled for the service</td>
</tr>
<tr>
<td></td>
<td>✓ Verify that it is the correct patient and corresponding email address</td>
</tr>
<tr>
<td></td>
<td>✓ Must send a test secure message by adding “[secure]” to the start of the subject line</td>
</tr>
<tr>
<td></td>
<td>✓ One email = one patient, under no circumstances should the blind copy (bcc) or copy (cc) be used to send to a patient.</td>
</tr>
<tr>
<td></td>
<td>✓ Use the check list given in the ‘Patient Mailing Policy’ to verify that the intended content is appropriate and authorised to be sent to the patient</td>
</tr>
<tr>
<td></td>
<td>✓ Agree purpose:</td>
</tr>
<tr>
<td></td>
<td>✓ Subject Access Reports</td>
</tr>
</tbody>
</table>

See Appendix 2 for detailed instructions on how to send sensitive Information using email to a patient.

<table>
<thead>
<tr>
<th>Insecure - Amber (With consent of Individual or Patient)</th>
<th>Email:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Lost or Sent to the Wrong Recipient:</td>
<td>SMS:</td>
</tr>
<tr>
<td>✓ Could cause distress</td>
<td>Reply to email sent by patient or verify address prior to sending.</td>
</tr>
<tr>
<td></td>
<td>Reply to SMS sent by patients or verify number</td>
</tr>
</tbody>
</table>

Insecure - Amber (With consent of Individual or Patient)

If Lost or Sent to the Wrong Recipient:

✓ Could cause distress
### 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

### Handling Instructions:

- Any

### Email: SMS:

- 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.
Information Security Policy – Email Acceptable Usage

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

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ACTION]</td>
<td>Action Required/For Action</td>
</tr>
<tr>
<td>[ACT]</td>
<td></td>
</tr>
<tr>
<td>[FOR INFO]</td>
<td>For Your Information</td>
</tr>
<tr>
<td>[FYI]</td>
<td></td>
</tr>
<tr>
<td>[REMINDER]</td>
<td>Reminder</td>
</tr>
<tr>
<td>[REQUEST]</td>
<td>Request</td>
</tr>
<tr>
<td>[REQ]</td>
<td></td>
</tr>
<tr>
<td>[URGENT]</td>
<td>Urgent - use sparingly considering the importance to person you are sending the email to</td>
</tr>
<tr>
<td>[URG]</td>
<td></td>
</tr>
<tr>
<td>[SOCIAL]</td>
<td>e.g. department night out</td>
</tr>
<tr>
<td>[SOC]</td>
<td></td>
</tr>
<tr>
<td>[EOM] (suffix)</td>
<td>End of Message - for example Fire Alarm today at 3pm saves recipient opening full email.</td>
</tr>
</tbody>
</table>

For Example: **Subject:** [FOR INFO] Fire Alarm test today at 11am Law House [EOM]

- **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
  - **X** 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
  - **X** Don’t keep emails longer than required
Information Security Policy – Email Acceptable Usage

- 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 IT 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
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;
Information Security Policy – Email Acceptable Usage

- 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 eHealth IT 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.

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 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 an eHealth 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, eHealth
Executive Director: Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body: Information Governance 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.

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:

- General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- May 2014 Using Email in NHSScotland: A Good Practice Guide
- May 2012 Frequently Asked Questions on new guidance for email in NHSScotland
- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- NHSL Risk Management Strategy 2016
- 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
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Information Security Policy – Email Acceptable Usage

17. Instructions on How to Send Sensitive Information using email to a Patient - APPENDIX 2

How to send an encrypted message
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 and prepares the recipient for receiving the encrypted email:

1. Send the recipient the NHSmail guidance for opening encrypted email, so they can register for the service.
2. 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 an email or as an attachment, subject to local governance policies.
3. 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.

To send an encrypted email:
4. Log in to your NHSmail account (either via an email client such as Outlook or via the web portal at www.nhs.net).
5. Create a new email message in the normal way.
6. Ensure the recipient’s email address is correct.
7. 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.
8. Type the message.
9. 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 providing NHSmail is used to do this and the subject field of the email has the text [secure] before the subject of the message.

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 NHSmail.

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

**Only email sent from NHSmail with [secure] at the start of the subject line will be encrypted.**

**Limitations**
The NHSmail Encryption Feature will allow sensitive email to be opened by patients that use their own email system to receive the email and enroll, 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.

NHSmail operates a maximum 35 MB email message size.

For more information please see the [NHSmail guidance for encrypted email](#).
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 emails 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 use NHSMail and while they are in transit within the Scottish NHS network they 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 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 will 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, follow the NHSmail guidance for opening encrypted email, so they can register for the service.

Replying to secure email sent from the NHS
You should take care when replying to secure email sent from the NHS, as your reply will only be secure when replying within the Trend Micro Private Post website. Merely replying to the email which stated “You have received an email message secured by Private Post. Please open the file called Encrypted_Message.htm to read the message” will NOT be sent securely. For further details please see the link to the NHSmail guidance above regarding ‘Replying to’ encrypted emails. 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.
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 the NHSmail helpdesk as well as the NHS Lanarkshire IT 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 required blocked.**

In order for the NHSmail service to efficiently process your spam report please ensure that you have attached a copy of the offending email in .eml or .msg format. This must be attached directly from your mailbox **(not from a forward or copy)**. The guidelines below explain how to do this.

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 the NHSmail service and may still affect other staff.

If you have already attached a copy of the spam mail in the correct format, and it has been taken directly from the recipient’s mailbox, then it will be uploaded to the spam filters for blocking. Please allow up to 48 hours for this blocking process to take effect. No further correspondence will be required.

**Reporting email threats with Microsoft Outlook**

Forward the email to spamreports@nhs.net and 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 spamreports@nhs.net and spamreports@lanarkshire.scot.nhs.uk in the ‘To field’.
4. Click **Send**.

**Staff using NHSmail can report email threats with Outlook Web App (www.nhs.net)**

Follow the instructions below to save a copy of the email you suspect is spam in Outlook Web App

1. Click on the Spam Email in the reading pane to select it
2. Click on the **New mail icon** in the top left of the screen
3. Drag and drop the spam email from the email list into the body of the new blank email
4. Type spamreports@nhs.net and spamreports@lanarkshire.scot.nhs.uk into the To: field
5. Enter the appropriate subject text a. Note: It is recommended that you use spam, phishing or malicious depending on the type of email you are reporting
6. Click **Send**

For more advice on reporting email threats see NHSmail Cyber Security Guide.