

# Safe Email Transmission

## Standard Operating Procedure (SOP)

This guidance applies to NHS Lothian staff, independent contractors and partner agency staff or organisations with an NHS Lothian provided email address. Council and partner agency staff using their own employers email service must follow the guidance issued by their own employer and not assume that the detail within this guidance applies to them.

1. NHS Lothian email is secure to send and receive sensitive, confidential information between NHS Lothian email addresses and those listed in the grid below. It is also very important to ensure that only the correct recipients are selected when composing email, as there are instances of there being more than one person with the same name in the global address book.

The safe email transmission grid in the following pages give instruction as to the method of email communication that should be used for information of different security classification levels.

Security classifications are as follows:

- Confidential or Sensitive data (including person identifiable data)
- General work or related, but **not** Confidential or Sensitive data including person identifiable
- Non work related.

Confidential or sensitive data (including person identifiable information) must at all times only be sent in accordance with the email grid.

Email communications with patients containing Confidential or Sensitive data is prohibited as email does not provide adequate security for confidential correspondence. However exceptions can be sought by application for approval to the Caldicott Guardian with provision of a risk assessment and procedure for review.

3. NHS Lothian has secured email links with a number of partner agencies. This enables NHS Lothian staff to send sensitive, confidential information with these partners and the following guidance must also be followed.
  - The 'reply to all' function should not be routinely used, as it is bad practice to assume that all recipients have 'safe' email addresses.
  - Where smartphones are used for email, the data contained on these devices can be remotely wiped immediately in the event of loss or theft. These devices must be protected with an additional password or pin and encryption, and when being used should be held in such a way as to prevent any onlookers from viewing sensitive or confidential data.
4. Before sending any email containing personal data, staff must double-check that they have addressed the email to the correct recipient. It is very easy for an email message to be forwarded on to additional recipients who were not on the original distribution list, without your knowledge or consent, so care must be taken with the overall content and confidentiality of the topics being discussed. **STOP AND CHECK** and, only then, **SEND**.
5. Any personal, sensitive or confidential information should not be shared by email unless appropriate confidentiality and security procedures are used. Before sending any confidential material you must ensure that you have read, understand and abide by the NHS Lothian Digital

and IT Security policy. This is contractual obligation of your NHS Lothian network and email access.

6. Before sending an email containing personal data you must ask yourself:
  - Is email the appropriate, and most secure, communication method?
  - Do you have a justified purpose for using this confidential information?
  - Do you need to seek advice or authorisation?
  - Are you using it because it is absolutely necessary to do so?
  - Are you using the minimum information required, including an anonymous email header?
  - Are you allowing access to this information on a strict need-to-know basis only?
  - Can you encrypt the message contents?
    - (Outlook= New message > Options > Permissions > Encrypt)
    - (OWA Webmail = New message > Encrypt button)
7. Staff must not encourage email communication, which may involve the transfer of personal data, with private individuals or external companies into NHS Lothian. The email matrix below defines those partner agencies with which NHS Lothian has secure email links. Addresses which do not appear on this list, constitute a significant risk when transferring personal data. The sending of email containing Confidential or Sensitive data to non-approved external addresses is not secure and should not be used for this data. All mail is filtered to prevent junk email and to reduce the risk of personal data being sent via an insecure channel.
8. If you have any doubts or queries as to whether an email address is safe, presume it is not and **STOP AND CHECK** with IT Security. **DO NOT** use external email accounts for the transfer of personal data.
9. Misuse of email may contravene one or more legislative frameworks, including (but not limited to) the Data Protection Act 2018, Computer Misuse Act 1990, Electronic Communications Act 1990, Freedom of Information (Scotland) Act 2002, Copyright, Design and Patents Act.
10. NHS Lothian may develop further secure email links when technically possible. Key staff will be informed of any such developments, and the grid below will be updated and published as and when this happens.

### Safe Email Transmission Grid

Applies to all Confidential or Sensitive data including Personally Identifiable Information (PII)

To:	<b>SECURED</b> @nhslothian.scot.nhs.uk @*.scot.nhs.uk @nhs.net @nhs.scot @phs.scot @*.nhs.uk @*.gov.uk @*.mod.uk @*.cjsm.net @*.pnn.police.uk @*.parliament.uk @westlothian.org.uk @*.elcschool.org.uk @*.edin.sch.uk @brookhouseinquiry.org.uk @ipco.org.uk @fshc.co.uk @brighterkind.com @huntercombe.com @fshcgroup.com	<b>INSECURE</b> All email addresses not listed <b>SECURED</b> including but not exhaustively; @outlook.com @*.ed.ac.uk @hotmail.com @gmail.com @btinternet.co.uk @children1st.org.uk @doctors.org
From:		
1 @nhslothian.scot.nhs.uk	Yes	No
2 @nhs.net	Yes	No