Lothian NHS Board

Mainpoint
102 West Port
Edinburgh
EH3 9DN

Telephone: 0131 536 9000
www.nhslothian.scot.nhs.uk

Date: 08/04/2026
Our Ref: 11230
Enquiries to loth.freedomofinfomation@nhs.scot

Dear

FREEDOM OF INFORMATION – PATIENT EMAIL POLICY

I write in response to your request for information in relation to NHS Lothian's patient email policy.

Question:

Please provide all information held relating to the policy expressed on the East Lothian GIRFEC website (https://sites.google.com/edubuzz.org/girfecineastlothian/neurodiversity) about the inability of NHS Lothian to respond via email to parent/carer queries.

Without prejudice to the generality of this request, please include all information relevant to the discharge of the Public Sector Equality Duty, the Fairer Scotland Duty and duties under the UNCRC (Incorporation) (Scotland) Act 2024, including but not limited to impact assessments and relevant legal responsibilities/guidance which have led to the conclusion that NHS Lothian cannot rather than will not reply.

Answer:

NHS Lothian's policy is not to communicate with patients using insecure email addresses. This is because the communication is likely to include individual patient information which is subject to rules for storage and transfer under the Data Protection Act. Transfer of information by insecure email addresses risks the exposure of this information. In order to send information to patient by email, a Caldicott exemption approval is required.

I have enclosed the relevant policies and standard operating procedures:

Data Protection Policy
Safe Transfer of Health Records SOP
Safe Email Transmission SOP

I hope the information provided helps with your request.

If you are unhappy with our response to your request, you do have the right to request us to review it. Your request should be made within 40 working days of receipt of this letter, and we will reply within 20 working days of receipt. If our decision is unchanged following a review and you remain dissatisfied with this, you then have the right to make a formal complaint to the Scottish Information

Commissioner within 6 months of receipt of our review response. You can do this by using the Scottish Information Commissioner's Office online appeals service at https://www.foi.scot/appeal. If you remain dissatisfied with the Commissioner's response you then have the option to appeal to the Court of Session on a point of law.

If you require a review of our decision to be carried out, please write to the reviewer at the address at the top of this letter. The review will be undertaken by a Reviewer who was not involved in the original decision-making process.

FOI responses (subject to redaction of personal information) may appear on NHS Lothian's Freedom of Information website at: https://org.nhslothian.scot/FOI

Yours sincerely

ALISON MACDONALD
Executive Director of Nursing Midwifery and AHPs
Cc: Chief Executive
Enc.

Data Protection Policy

Title: **Data Protection Policy**			
Date effective from:	October 2025	**Review date:**	October 2028
Approved by:	Policy Approval Group		
Approval Date:	30 September 2025		
Author/s:	NHS Lothian Data Protection Manager		
Policy Owner:	Information Governance and Security Manager		
Executive Lead:	Executive Medical Director		
Target Audience:	All NHS Lothian staff		
Supersedes:	Data Protection Policy v3.1 (2018)		
Keywords (min. 5):	Data, protection, information, records, breach, Caldicott, legal, controller		

Data Protection Policy

Version Control

Date	Author	Version	Reason for change
Jan 2018	NHS Lothian Data Protection Manager	v3.1	Approved by Information Governance Sub-Committee
June 2022	NHS Lothian Data Protection Manager	v4.0	Approved by the Policy Approval Group
June 2025	NHS Lothian Data Protection Manager	v4.1-2	Under review.
Sept 2025	NHS Lothian Data Protection Manager	v5.0	Approved by the Policy Approval Group

Executive Summary

NHS Lothian is required to process a large variety of personal data in order to carry out its statutory functions. NHS Lothian processes patient and carer data for healthcare related purposes, including provision of care, administration of healthcare services, teaching and research. Personal data is also held on current, past and prospective employees, suppliers, and others with whom it communicates. All such this policy outlines NHS Lothian intention to process personal data professionally and securely regardless of how the data is collected, recorded and used – whether on paper, in a computer system or recorded on other media.

NHS Lothian will ensure appropriate Data Protection Impact Assessment(s) are completed with any new use of personal data is proposed. This will ensure all aspects of the processing are considered and risks are documented and where necessary address before the commencement of processing.

When data sharing is necessary NHS Lothian will ensure appropriate Data Sharing or Data Processing Agreement are in place documenting the processing taking place.

NHS Lothian complies with Data Protection legislation and will ensure all data is processed respectfully and in accordance with the law.

Data Protection Policy

Contents

1.0 Purpose

The purpose of this policy is to detail how NHS Lothian needs to process a variety of personal data in order to carry out its statutory functions. NHS Lothian processes patient and carer data for a variety of healthcare related purposes including provision of care, administration of healthcare services, teaching and research. Personal data is also held on current, past and prospective employees, suppliers, and others with whom it communicates. All such personal data will be dealt with properly and securely no matter how it is collected, recorded and used – whether on paper, in a computer system or recorded on other media.

NHS Lothian will observe the requirements of Data Protection Legislation when processing personal data. NHS Lothian will ensure that the organisation continues to treat personal data with due care and diligence.

2.0 Policy statement

NHS Lothian will:

- Observe, fully the conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply checks to determine the length of time information is held.
- Ensure that the rights of people about whom personal data is held can be fully exercised under the Act. These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information.
- Ensure Data Protection Impact Assessment(s) are undertaken when any new use of personal identifiable data is proposed.
- Where necessary ensure appropriate Data Sharing and Data Processing Agreements are in place with trusted partners.
- Ensure that personal data is not transferred out with the UK without suitable safeguards.
- Take appropriate technical and organisational security measures to safeguard personal data.
- All Information Assets should be logged in the organisations Information Asset Register.

2.1 Organisational Issues

- NHS Lothian will ensure that a full, correct and up-to-date notification is lodged in its name with the Information Commissioner.
- The Data Controller for NHS Lothian will be the Chief Executive, who will delegate day-to-day responsibility for the operational application of the Data Protection Legislation to the Executive Medical Director.
- NHS Lothian will observe the Caldicott principles and ensure that there is a nominated Caldicott Guardian.
- NHS Lothian employ a Data Protection Officer suitably qualified with specific responsibility for advising on, and monitoring data protection practice in the organisation.
- NHS Lothian will ensure that:
- Everyone processing personal data understands that they are contractually responsible for following good data protection practice is appropriately trained to do so and provided with appropriate support.
- Anyone wishing to make enquiries about processing personal data knows whom to approach.
- Enquiries regarding processing personal data are timeously dealt with in line with Data Protection Legislation.
- Methods of processing personal data are clearly defined and reviewed regularly to ensure best practice guidance is followed within the organisation.
- A regular review and audit are made on the ways data are processed.
- When sharing information with Public Authority or voluntary partners, or when required for statutory purposes, this is managed in accordance with the NHS Lothian Information Sharing Protocols. Where deemed appropriate by managers, breaches of the Data Protection Act 2018 and associated policy may result in action being taken through the current Disciplinary Policy.

3.0 Scope

This policy applies to all staff working for or on behalf of NHS Lothian. Temporary and agency staff, volunteers, contractors, students and work experience personnel will also be expected to ensure compliance with this policy.

The Data Protection Policy covers the following areas to set out the approach to Information Governance in NHS Lothian:

- Statement of intent
- Responsibilities for Information Governance
- Guidance to all aspects of data processing

4.0 Definitions

Information Governance Principles:

NHS Lothian recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. NHS Lothian fully supports the principles of corporate governance and recognises its public accountability but equally places importance on the confidentiality and security of personal information regarding patients, staff and the population, and commercially sensitive information.

NHS Lothian also recognises the need to share patient information with other healthcare organisations and outside agencies in a controlled manner which is consistent with the interest of individual patients, the health of the people of Lothian and, in some circumstances, the public interest.

NHS Lothian believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are four key inter-linked strands to Information Governance:

- Openness
- Confidentiality
- Information Security
- Quality assurance

5.0 Implementation roles and responsibilities

5.1 Chief Executive

This policy is authorised by the Chief Executive as the officer responsible for the duties of the employer under legislation

The Chief Executive has overall responsibility for ensuring that an organisational structure and effective arrangements exist to ensure the compliance of data protection legislation

This will include responsibility for:

- The staff employed within NHS Lothian
- The work processes, activities and systems performed within NHS Lothian

5.2 Executive Medical Director

The Executive Medical Director is responsible for the following:

- Ensuring that the provisions of this policy are implemented throughout the organisation.

- Ensuring through the various line management structures and the NHS Lothian Staff Governance Committee that the NHS Lothian Board is meeting all its legal obligations.

5.3 Senior Information Risk Owner

NHS Lothian's Senior Information Risk Owner will implement and lead the information governance risk assessment and management processes and advise the Board on the effectiveness of information risk management across the organisation.

5.4 Digital Department

Implementation of this policy will follow continued good practice as outlined in the appendices. NHS Lothian Digital Department will provide a compliance and advice to support the organisation, this will include the statutory requirement of a Data Protection Officer post and service

5.5 Line Managers

All line managers should have local dissemination and implementation plans in place to ensure all staff who need to interact with identifiable data, manual, IT or other electronic equipment are familiar and adhere to all aspects of this policy.

All line managers should have local dissemination and implementation plans in place to ensure all staff are familiar with and adhere to all aspects of this policy. This includes non-clinical areas and non-clinical staff at all locations within NHS Lothian.

5.5.1 Good Practice for Managers

Has identified the staff in his or her area to whom this policy applies and has given the policy (or selected excerpts) to them.

Has assessed the impact of the policy on current working practices and has an action plan to make all necessary changes to ensure that his or her area complies with the policy.

Has set up systems to provide assurance to him or her that the policy is being implemented as intended in his or her area of responsibility.

5.6 All staff

Information Governance and Security training will be provided as part of the mandatory induction program for new NHS Lothian employees.

All staff must attend mandatory updates every 24 months. Included in this is the Information Governance module, which ALL staff must complete.

Unauthorised breaches of IT security policy will be taken very seriously and may result in an investigation into the alleged breach, and may result in disciplinary action in accordance with NHS Scotland Workforce Conduct Policy

5.6.1 Good Practice for Employees

Has read the policy (or selected excerpts) and considered what it means for him or her, in terms of how to conduct his or her duties.

Has completed any mandatory education or training that may be required as part of the implementation of the policy.

Has altered working practices as they expected by the policy

5.7 Records Management Plan

NHS Lothian has a Records Management Plan, and the Corporate Records Manager will submit to The Keeper of the Records when required. This plan sets out the overarching framework for ensuring that NHS Lothian's records are managed and controlled effectively, and commensurate with the legal, operational and information needs of the organisation.

6.0 Associated materials

In conjunction with the Data Protection Legislation, NHS Lothian will apply the Principles of Caldicott, IT Security, Information Sharing, Confidentiality, Social Media, and Records Management, as defined in their supporting policies and protocols to meet the Information Governance standards as prescribed by Scottish Government.

Subject Access Policy, approved by the Policy Approval Group, September 2025

Access to Health Records further guidance

Parental Responsibility

Processing Access Requests

Staff files process

Safe Transfer of Health Records

Consent to Process Personal Data

Personal Data Breach Flowchart

Warnings and Alerts Policy approved by the Policy Approval Group, September 2025 (available on the NHS Lothian intranet)

Data Protection Impact Assessment Form/Guidance

Data Sharing and Data Processing Agreements/Guidance

7.0 Evidence base

Access to Health Records Act 1990

Data Protection Act 2018

UK General Data Protection Directive (GDPR) 2016

Human Rights Act 1998

Computer Misuse Act 1990

Network and Information Systems regulation 2018

Public Records (Scotland) Act 2011

Disposal of Records (Scotland) Regulations 1992

Freedom of Information (Scotland) Act 2002

Scottish Government Records Management Health and Social Care Code of Practice 2024

Scottish Health Memorandum 60 of 1958 (SHM58/60)

MEL (1993)152 – Guidance for Retention and Destruction of Medical Records

NHS (Scotland) HDL (2006) 41 - NHS Scotland Information Security Policy

The Management, Retention and Disposal of Administrative Records HDL (2006) 28

8.0 Stakeholder consultation

NHS Lothian consultation groups for this policy will be Information Governance Working Group and Digital & IT Executive Team.

A draft version of this policy was placed on the NHS Lothian Consultation Zone to give all NHS Lothian staff the opportunity to provide comment/feedback.

9.0 Monitoring and review

The strategic direction for Information Management and Information Governance will be set out in the Information Governance Working Group and Digital & IT Executive Team. The Digital Portfolio Group, accountable to NHS Lothian Board will have overarching responsibility for monitoring the strategy and for ensuring that NHS Lothian has effective policies and management arrangements in place, which cover all aspects of Information Governance.

Assessments of compliance with relevant information governance standards will be undertaken each year, and an appropriate information governance improvement plan will be produced as a result. Delegated responsibility for overseeing the Information Governance Strategy, Policy and Implementation plan sits with the NHS Lothian Digital Portfolio Group chaired by the Director of Digital. This group will secure the necessary resources to implement the Information governance action plan and will monitor activities and annually report progress to The Healthcare Governance Committee. Full terms of reference will be available on NHS Lothian Intranet.

The Executive Medical Director and Caldicott Guardian, is the named executive director on the Board with responsibility for Information Governance. The Director of Public Health & Health Policy is the designated interim Senior Information Risk Owner (SIRO)

delegated responsibility for implementation and monitoring of the Information Governance Action plan which sits with the Information Governance and Security Manager.

Regular monitoring of compliance with this policy will be performed via National and local audits both internally and also by external contractors.

The effectiveness of this policy may also be monitored and evaluated using outputs from the following:

- IT Security investigations
- SAE reviews
- DATIX investigations
- Complaint investigations
- Regularly scheduled internal and external audits
- Staff feedback via conversations, queries, compliments & complaints
- Information Governance Working Group and also the Digital & IT Executive Team.
- Post training feedback from staff

This policy, and its associated materials, will be reviewed every 3 years, as a minimum, or as a result of any changes in legislation, guidance, as the result of inspection or audit, or any other factors which may render the policy in need of earlier review.

Safe Email Transmission Grid

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.

2. 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. Staff have the option to turn off AutoComplete in Outlook, which may reduce the risk of inadvertently including previously used email addresses, thus resulting in a data breach.
   To turn off AutoComplete in outlook, go to File>Options>Mail, then scroll down to the 'Send messages' section and untick the option 'Use Autocomplete List to suggest names when typing

6. 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 a contractual obligation of your NHS Lothian network and email access.

7. 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)

8. 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.

9. 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.

10. 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 Patients Act.

11. 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

FROM	SECURED ✓	SECURED ✓ (Care Homes)	INSECURE ✗
@nhslothian.scot.nhs.uk @nhs.scot	@nhs.net @nhs.scot @nhslothian.scot.nhs.uk @*.cjsm.net @*.edin.sch.uk @*.elcschool.org.uk @*.gov.uk @*.mod.uk @*.nhs.uk @*.parliament.uk @*.police.uk @*.scot.nhs.uk @bupa.com @cabedinburgh.org.uk @care4carers.org.uk @chas.org.uk @chss.org.uk @crew2000.org.uk @dadsrock.org.uk @disclosurescotland.gov.scot @elcap.org @enjoyleisure.com @gov.scot @gpplus.com @health-in-mind.org.uk @hscni.net @igpr.co.uk @mariecurie.org.uk @meld-drugs.org.uk @mndscotland.org.uk @musselburghcab.org.uk @penicuikcab.org.uk @phs.scot @salvationarmy.org.uk @sightscotland.org.uk @spacescot.org.uk @vocal.org.uk @westlothian.org.uk @westlothianleisure.com	@abercorncare.com @almondvalleycare.co.uk @amicura.co.uk @astleyhousenursinghome.co.uk @aurem-care.com @barchester.com @bekkacare.com @belgravelodge.co.uk @blackfauldshouse.com @braeburnhome.co.uk @brighterkind.com @cameronpark.co.uk @carberryresidentialhome.co.uk @careuk.com @caringhomes.org @claremontparknursinghome.co.uk @coel.org.uk @colintoncare.co.uk @croftheadcarehome.co.uk @crossreach.org.uk @eildoncare.co.uk @elder-homes.co.uk @erskine.org.uk @fairview.care @florabank.co.uk @fshc.co.uk @fshcgroup.com @grandlodgescotland.org @gilmertoncare.co.uk @guthriehousecare.co.uk @haddingtoncare.co.uk @hc-one.co.uk @huntercombe.com @lammermuirhousecare.co.uk @lindemann.healthcare @livingstoncare.co.uk @manorgrangecare.co.uk @mc1.org @meadowvalecare.co.uk @moraruk.co @nazarethcare.com @northcare.co.uk @peacockmedicare.com @randolphhill.com @renaissance-care.co.uk @sanctuary.co.uk @stannesmusselburgh.co.uk	All email addresses not listed as **SECURED,** including but not exhaustively: @*.ed.ac.uk @aol.com @btinternet.co.uk @children1st.org.uk @doctors.org @gmail.com @hotmail.com @icloud.com @outlook.com @sky.com @yahoo.com

		@stcolumbashospice.org.uk @stmargaretscare.co.uk @struanlodgecare.com @trinityhousecare.com @viewpoint.org.uk @walkerhealthcare.co.uk	

Safe Transfer of Health Records

1. Information taken away from Hospital premises

All staff must seriously consider the need for taking patient/client/staff records out of their base with them on a visit. This should only happen when absolutely essential and there is no other method available for accessing/recording the information required. Staff must not carry around more information than is necessary.

It is recognised that health professionals may find it necessary to remove patient records from their base, to assist their daily practice of seeing patients in community settings. The guidelines below should be followed to reduce the risk of the records being accessed by an unauthorised person, lost or stolen. These guidelines are also applicable to HR staff transporting staff records.

- When removing notes for home visits ensure that you take only for those visits that are pre booked.
- Consider whether you need the notes to carry out the visit?
- Records should not be removed for general administration purposes, e.g. writing routine reports.
- Record the removal and return of files taken away from the workplace.
- Records should be stored and carried in a secure bag/case.
- Records should not be carried 'loosely' as this increases the risk of dropping them and losing something.
- Where confidential information is being transported by both internal and external mail, it is important to ensure that it is securely packaged and that the word 'Confidential' is clearly displayed. Where information is being sent to locations out with those covered by the van service, recorded delivery (signed for and special delivery guaranteed or trusted courier) should be utilised. Lockable, traceable, tamper proof bags should be used.
- If the member of staff is not returning to their base at the conclusion of their visits the records must be stored in the bag/case used and taken out of the car overnight into their home. Care must be taken in order that members of the family or visitors to the house cannot gain access to the records. This practice should only occur if the member of staff is not returning to their base after the working day or the records are required for the next working day. Staff must have the agreement of their manager if it is necessary for them to work in this way.
- Records should not be away from base for more than one working day i.e. if a member of staff is not returning to base at the conclusion of their working day, the records taken out on visits must be returned on their next normal working day.

There may be exceptional circumstances that mean this is not possible i.e. if a member of staff goes off sick before returning the notes. In this situation the records should be returned as soon as is practically possible. Managers may have to make arrangements to retrieve records if they are required whilst the member of staff is off for a period of time.

2. Transfer of records to other bases in NHS Lothian

- Where the record is related to significant events (e.g. complaints, legal action, access to records requests, serious incidents); or where the person holding the record or the person asking for it thinks that the record is particularly sensitive for other reasons, it should be delivered in person wherever possible.
- Loose identifiable information should not be handed to another person for delivery simply because they are going to the designated department.
- When records are sent in the internal post an assessment must be made as to the risk of loss. If the loss of those records could compromise patient care or create a serious breach of confidence the following procedure must be followed. It must be followed in all cases where whole patient records are being sent.
- Records must be transferred in an envelope which can be securely sealed, be clearly addressed to a named individual including their title and location and be marked Private and Confidential. If an envelope is reused cross out the previous address. NEVER reuse an envelope with a business reply service number. The records will be sent to the address registered to the business reply service and not to the address you have written.
- Where bulk transfers (50 records or more) are used the number of items in transit must be recorded with a method to identify any records that are transferred.
- The sender must add their name, title and location to the back of the envelope. A note should be attached to the records asking the recipient to contact the sender to acknowledge receipt. This can be done via e mail, telephone or by a return receipt. Alternatively, an e mail can be sent to the recipient telling them the records are in transit and to contact the sender if they do not arrive within three days.
- If the sender has heard nothing after three working days, they should contact the person the records were addressed to, to check receipt.
- If possible, staff should nominate a colleague to open mail containing service user records when on planned or unplanned leave. Such records should be kept secure until the member of staff returns from leave.
- If staff need to send records urgently then they should contact the intended recipient in advance to ensure that they are not on leave or working away from their base.
- Information should not be regularly faxed, where possible alternative secure methods must be used. NHS Lothian permit faxing where authorisation has been given by the Caldicott Guardian and an exemption application must be completed.
    - No new fax service or business process to be implemented - this is against NHS Lothian Policy
    - Existing Fax services must be locally reviewed for more suitable methods and an action plan of a move to more secure methods of transferring information established (e.g. secure email and provision is NHS.net addresses

- In emergency Fax Guidance in NHS MEL (1997)45 must be followed (excerpt Sub Appendix 1)
- NHS MEL (1997)45 is due to be replaced with stricter controls following several miss-dial fax data breach incidents that have resulted in monetary fines by the Information Commissioner, and this guidance will be updated and replaced.

Faxing should only be used in an emergency situation.

3. External post - Royal Mail

- When records are sent in the external post an assessment must be made as to the risk of loss. If the loss of those records could compromise patient care or create a serious breach of confidence the following procedure must be followed. It must be followed in all cases where whole patient records are being sent.
- External post should be avoided in most circumstances for sending clinical records out with NHS Lothian (use internal mail, or physical handover). Where original records or copies have to be sent to organisations outside NHS Lothian, they should be securely sealed and addressed as above and should be sent using Royal Mail's Recorded Delivery service which provides a tracking and tracing service.
- Lockable, traceable tamperproof bags/containers must be used for anything bulkier than an individual letter.
- Where bulk transfers (50 records or more) are used the number of items in transit must be recorded with a method to identify any records that are transferred. In addition to the secure method of transfer used, records must be transferred in an envelope which can be securely sealed, be clearly addressed to a named individual including their title and location and be marked Private and Confidential.

4. Tracking Records

When an assessment has been made as to the risk of loss and the loss could compromise patient care or create a serious breach of confidence the following procedure must be followed. It must be followed in all cases where whole patient records are being sent so that their whereabouts are known at all times.

The person responsible for sending or taking records must log:

- The name and type of records removed, including any unique identifying number,
- The reason for removal and whether likely to be temporary or permanent if known,
- The date of removal,
- The person the record is being sent/handed over to,
- Method of transfer
- The date notified that the records have arrived at their destination including name of person confirming receipt, if appropriate.
- The date records return to base, if appropriate.

Where data is received in an insecure manner from another part of NHS Lothian i.e. does not follow this policy, the recipient should notify the sender and request that any future

information must be sent securely. A DATIX incident report should be completed on any such incidents.

5. Transportation of Health Records, Out of Hours

Between 9am and 5pm on weekdays, Medical Records personnel are available to assist with the tracking and transportation of health records between hospital departments if required. If a set of case notes is needed out of hours, then the case notes will be retrieved by the Reception or Nursing staff (who are trained to use the tracking system) are also authorised to track and transport case notes out of hours – the procedural rules apply to both core working hours and 'out of hours'

6. Health Records Guidance

Further Guidance can be sought from NHS Lothian Health Records Department who have a more local policy on how to transfer Health Records, this can be found on the intranet, Health Records Policy PP34-Transporting Casenotes (available on NHS Lothian intranet)

7. Email

Email of personally identifiable information should be in compliance with safe email transmission . Safe Email Transmission Standard Operating Procedure (available on NHS Lothian intranet)

Appendix 1

NHS MEL (1997) 45 Guidance on the use of facsimile transmissions for the transfer of Personal Health Information within the NHS in Scotland

1. No named data should be sent by fax. If it is essential, clinical information can be sent with a suitable identifier (e.g. the CHI number) and the name and address and identifier conveyed by post or telephone. Where the transmission of named data is established practice and where discontinuation of this practice would cause disruption to patient services, it is therefore essential that best practice (as described below) is followed and that a confidentiality notice used as described below in paragraph 9. In these circumstances Health Boards and Trusts should plan to switch such data exchange to the NHS Mail which is being established as a secure, private network at the earliest opportunity. You should refer to NHS MEL(1996)80 for information about NHS Mail and how to connect to it.
2. It is imperative that fax machines which are used for the transmission or receipt of confidential information are placed in a secure location. The machines should be operated only by authorised users and these users should fully understand their responsibilities for maintaining confidentiality.
3. The room housing the fax machine must be locked whenever unattended. If the office is in general use, consideration must be given to ensuring that unauthorised individuals are unable to read, accidentally or otherwise, faxes which are arriving or have recently arrived.
4. Where the fax machine used for confidential information is located in a safe area (e.g., a "safe haven" in a Health Board) and is the only fax machine in use by tile organisation, the safe haven staff should forward any faxes not intended for their area.
5. A particular problem relates to faxes arriving outside normal hours which could be seen by cleaners or other personnel. Options to combat this include a blanket ban on transmissions outside office hours, switching machines off overnight if they are not secured and, possibly (if it does not constitute a fire hazard), locking machines (while switched on) into a cupboard. A further option involves the use of a computer to receive and store faxed data; whereby the information cannot be extracted without a password.
6. One of the most important risks with fax machines is misdialling, although most models display the number dialled. This can lead to faxes not arriving at all or arriving in an unintended location. In the latter case, there can be serious implications if non-coded confidential information is on the fax. Consideration should be given to the use of encryption between two safe havens, in appropriate cases. Best practice involves always checking the safe haven fax number before dialling; never dial from memory. Valid sources would include a locally compiled safe haven directory of a national directory, but not a general directory; alternatively, a telephone call to the safe haven should be used.
7. It is good practice to always precede the fax transmission by a telephone call to the recipient to confirm the fax number, to ensure that someone will be on hand at the machine to receive the fax and to seek confirmation from the intended recipient that the fax has been received.

8. It is good practice to identify frequently used numbers and program these into a fax machine's "memory dial" facility; equally, computer dialling facilities may be used where available. However, numbers must be tested in conjunction with a telephone call before using them for confidential information. Furthermore, the use of "memory dial" codes should be limited to safe haven numbers; this will prevent code mis- dialling having serious consequences.
9. If, in extreme circumstances where the above guidelines cannot be followed completely, non-totally anonymised patient information requires to be faxed, the fax should be preceded by a Confidentiality Notice such as: -

This facsimile transmission is intended only for the use of the individual or entity to which it is addressed and may contain confidential information belonging to the sender which is protected by the physician- patient privilege. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this transmission in error, please notify this office by telephone to arrange for the return of the documents