Lothian NHS Board

Lothian NHS Board
Mainpoint
102 Westport
Edinburgh
EH3 9DN
Main Switchboard: 0131 242 100

www.nhslothian.scot

Date 09/04/2026
Your Ref
Our Ref 11271R

Enquiries to Richard Mutch
Extension 35687
Direct Line 0131 465 5687
loth.freedomofinformation@nhs.scot
richard.mutch@nhs.scot

Dear

FREEDOM OF INFORMATION REVIEW – SHARED CARE

I write in response to your request for review of NHS Lothian's response to your Freedom of Information request in relation to shared care.

Original Request and Response:
Question:

1. Copies of all risk assessments and policies relating to the disclose of hospital admission records to local authorities/council department.
2. In particular, all risk assessments and policies relating to disclosure of admission and other records from the Royal Infirmary of Edinburgh to East Lothian Council and its Carer departments.
3. Details of processes involved in information sharing of admission records between Royal Infirmary of Edinburgh to East Lothian Council.

Answer:

NHS Lothian (Health) do not directly disclose personal identifiable data on hospital admission and other health records to Local Authorities/Council Department. NHS Lothian, as all Health Boards do have a relationship with IJB/HSCP's, and we have data sharing arrangements jointly signed by all parties for our four Lothian IJB's (including East Lothian).

I would recommend that you contact East Lothian IJB

Integration Joint Boards – NHS Lothian | Our Organisation

East Lothian Council
Corporate Resources,
John Muir House, Haddington,
EH41 3HA
Department: Law and Licensing
foi@eastlothian.gov.uk

Review Request:

- I note from your response that "NHS Lothian, as all Health Boards do have a relationship with IJB/HSCP's, and we have data sharing arrangements jointly signed by all parties for our four Lothian IJB's (including East Lothian)". Given that NHS Lothian is a party to the arrangements, and the hospital compiles and sends lists of admissions, can you please provide copies of those arrangements and any risk assessments in relation to that information sharing?

Review Response:

Further to your correspondence, please find attached the requested Data Sharing Agreements (DSAs) and Data Protection Impact Assessments (DPIAs), which set out the lawful basis for the sharing of personal data between NHS Lothian and the relevant Integration Joint Boards (IJBs) and Health and Social Care Partnerships (HSCPs).

The documents demonstrate that the processing and sharing of personal data is undertaken to support the exercise of statutory health and social care functions and is lawful under **Article 6(1)(e) UK GDPR** (performance of a task carried out in the public interest or in the exercise of official authority). Where special category personal data is processed, reliance is placed on **Article 9(2)(h) UK GDPR (**management of health or social care systems and services), together with the applicable conditions in **Schedule 1, Part 1 of the Data Protection Act 2018.**

The DPIAs address necessity and proportionality, data minimisation, transparency, and the technical and organisational measures in place to safeguard personal data. Where applicable, the arrangements operate consistently with the **Scottish Government's Intra-NHS Scotland Information Sharing Accord,** which provides an agreed governance framework for lawful and proportionate information sharing across NHS Scotland and partner organisations.

On this basis, NHS Lothian is satisfied that the information sharing is compliant with the **UK GDPR**, the **Data Protection Act 2018**, and the **common law duty of confidentiality.**

NHS Lothian has a policy of not releasing the names and detail of staff (and non NHS Lothian staff) below a senior level. This is considered exempt under Section 38(1)(b) of the freedom of information (Scotland) Act 2002 – personal information.

Should you require any further clarification or additional information, please do not hesitate to contact our Interim Information Governance & Security Manager, Elaine Downie - Elaine.Downie@nhs.scot.

If you are not satisfied with this response you still have the right to make a formal complaint to the Scottish Information Commissioner who you can contact at the address below or 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.

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS
Telephone: 01334 464610
Fax: 01334 464611
e-mail: enquiries@foi.scot

Yours sincerely

Freedom of Information Reviewer/
NHS Lothian
cc: Executive Nurse Director
Enc.

V201901

Data Protection Impact Assessment (DPIA) Questionnaire for

DPIA to support HSCP partner staff employed by East Lothian Council to access NHS & NHSL IT systems approved as relevant to fulfil their job role within ELHSCP.

Assessment Date: 12 March 2025
Review Date: March 2027

DOCUMENT CONTROL SHEET

Key Information

Title	*DPIA to support HSCP partner staff employed by East Lothian Council to access NHS & NHSL IT systems approved as relevant to fulfil their job role within ELHSCP*
Date Published/ Issued	02/07/2025
Date Effective From	*02/07/2025*
Version/ Issue Number	0.3
Document Type	DPIA
Document Status	DRAFT
Author	[redacted]
Owner	[redacted]
Approvers	[redacted]
Contact	[redacted]
File Name	DPIA ELHSCP_NHSL

Revision History

Version	Date	Summary of Changes
0.1	November	Initial Draft
	22/11/2024	First IG review
0.2	12/03/2025	Final
0.3	02/07/2025	Approved

Approvals

Version	Date	Name	Designation
[redacted]			

About the Data Protection Impact Assessment (DPIA)

The DPIA (also known as privacy impact assessment or PIA) is an assessment tool which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project that involves the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner's Office (ICO), which can include substantial fines. The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.

A DPIA is not a 'tick-box' exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that your project plan allows for this so that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done.

The ICO code of practice on conducting privacy impact assessments is a useful source of advice.

Is a DPIA required?

If the process or project that you are planning has one or more the aspects listed below then you must complete a DPIA at an early stage.

		YES/NO
1.	The work involves carrying out a ***systematic and extensive evaluation*** of people's personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing. Includes: Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination Excludes: Processing with little or no effect on people	No
2.	The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.*** Includes: • Racial or ethnic origin data • Political opinions data • Religious or philosophical beliefs data • Trade Union membership data • Genetic data • Biometric data for the purpose of uniquely identifying a person • Health data • Sex life or sexual orientation data	Yes

		YES/NO
	• Data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data • Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive <u>To decide whether processing is ***large scale*** you must consider:</u> • The number of people affected by the processing, either as a specific number or as a proportion of the relevant population • The volume of data and/or the range of different data items being processed • The duration or permanence of the processing • The geographical extent of the processing activity	
3.	The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people.	No
4.	The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset.	Yes
5.	The work involves processing personal data about ***vulnerable groups.*** This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data.	Yes
6.	The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of finger print and face recognition for improved physical access control; new "Internet of Things" applications.	Yes
7.	The work involves transferring personal data across borders ***outside the*** countries listed in the ICO website ? ✓ EEA countries ✓ Countries with an 'Adequacy decision' . You can view an up to date list of the countries which have an adequacy finding on the European Commission's data protection website. ✓ covered by the EU-US Privacy Shield framework. check on the Privacy Shield list to see whether the organisation has a current certification; or ✓ Covered by Canada's PIPEDA	No
8.	The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.	No

Step One – Consultation Phase

Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:

- Key service staff e.g. those who will be managing the process.
- Technical support, especially if a new system is involved. This may involve the relevant IT supplier.
- Information governance advisors e.g. Caldicott Guardian, Information Security Officer, Data Protection Officer.

Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS Board, or what information is collected and shared about them.

Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being 'bolted on' shortly before the change is launched.

Step Two- DPIA drafting

The responsibility for drafting a DPIA will normally sit with the service area that 'owns' the change, however, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).

Step Three- Sign-off

[NHS Board may need to also add in here specific, local/ administrative details on how DPIAs should be carried out and recorded in their organisation e.g. links with the Information Asset Register, mailboxes to use etc]

When a DPIA has been fully completed, it must be submitted for formal review by an appropriate IG professional/ the Data Protection Officer. They will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. The Data Protection Officer will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board's Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making.

Once reviewed, the DPIA will need to be signed off by the Information Asset Owner(s) (IAOs), normally a head of service.

1. What are you trying to do and why? – give (or attach separately) a high level summary description of the process, including the nature, scope, context, purpose, assets e.g. hardware, software used, data-flows). Explain the necessity and proportionality of the processing in relation to the purpose(s) you are trying to achieve.

The purpose of the umbrella DPIA is to enable East Lothian Council employees, in job roles held within East Lothian Health & Social Care Partnership, access to NHSL IT and relevant systems. This will support integrated working and ensure relevant staff can deliver the require function of the respective HSCP integrated services. Each application will be approved by their line manager and counter approved by a senior NHSL Manager for example Head of Operations. Each of these NHSL IT systems will have an existing DPIA for each system and operated within those parameters. Each ELC Partnership member of staff will undertake the relevant IT system training, and NHSL Information Governance eLearning.

Individual access is required to each of the systems listed below where job role relevant via NHS Lothian Directory Services Team after completing and submitting an NHSL UserID request form.

Trak - (East Lothian Council employees must have nhs.scot address)

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

Datix – Corporate H&S Risk and Issue management system Docs upload required.

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

Turas – online managers/staff appraisal system for NHS Lothian. Docs upload required.

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

SSTS – includes ESS access which allows for the appropriate recording for line management of staff actions to be recorded. Docs upload required.

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance	See Appendix 1	Partnership colleague, East Lothian Council employee

Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP		working to support delivery of ELHSCP services

eESS - (East Lothian Council employees must have nhs.scot address)

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

Job Train - (East Lothian Council employees must have nhs.scot address) – this is to support recruitment advertising and applicant shortlisting and recruitment and selection process in line with NHS Lothian Policies and Procedures. Docs upload required.

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

NHSL LearnPro/TURAS LEARN – mandatory and PDP learning tool for NHS Lothian staff for all staff cohorts. This is to be replaced by TurasLearn (end of March 2025).

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

Tableau – this is a management dashboard tool that allows for high level staff or departments/service etc overview.

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

NHSL Intranet – all users with NHS Lothian access will have access to the intranet.

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Mental Health & LD	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

NHSL email – all NHSL users that have an account where email is requested will be provided

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

eRostering – this supports the management of bank staff allocation of staff time and wage calculations.

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

BT Cloud Contact: Business Continuity – phone lines

Team/Service	Job Role	Reason for access
East Lothian Rehabilitation Service Planning & Performance Adult Social Care Ongoing & Acute Learning & Disabilities MELDAP	See Appendix 1	Partnership colleague, East Lothian Council employee working to support delivery of ELHSCP services

Each system would be applied following NHSL processes outlined below;-

TRAK	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
NHS L Email	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
Datix	Datix form	Datix - Information Governance
Turas	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
SSTS	User ID Request form	eHealth - Technical Services Policy 005 - NHS

		Lothian User ID Request Form.pdf
Eess	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
Job Train	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
LearnPro / TURAS Learn	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
Tableau	Management Accountant	Management Accountant
Intranet	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
eRostering	eRostering team	eRostering team
BT Cloud Contact	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf

2. What personal data will be used?

Categories of individuals	**Categories of personal data**	**Any special categories of personal data [see Guidance Notes for definition]**	**Sources of personal data**
Staff	Personal details, Training details, Contact Details	No special category data will be processed.	Held on the relevant HR systems, training systems
Patients	Personal details, details relevant to the system design i.e. condition or support/treatment	Health Data (as stored on the patients Medical Record (Trak) or on BT Cloud Connect).	Held on the relevant NHS Lothian systems (e.g. TRAK and BT Cloud Connect).

3. **What legal condition for using the personal data is being relied upon? [see Guidance Notes for the relevant legal conditions]**

Legal condition(s) for *personal data* [see Guidance Notes]	**Legal conditions for any *special categories of personal data* [see Guidance Notes]**
• 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	• 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

4. **Describe how the personal data will be collected, used, transferred and if necessary kept up to date – may be attached separately.**

The data will be collected, used, transferred in identical format as that outlined in each NHSL DPIA specific for the system that they have been granted access to and appropriate approvals given and required system training completed.

East Lothian Council staff will apply for access to the relevant applications, as specified in question 1. Each application will be approved by their line manager and counter approved by a senior NHS Lothian manager (for example the Head of Operations).

5. **What information is being provided to the people to whom the data relate to ensure that they are aware of this use of their personal data? – This is the 'right to be informed' and information such as privacy notices may be included as an attachment.**

East Lothian Council Privacy Notice: How your personal information is used | Privacy and cookies | East Lothian Council

NHS Lothian Data Protection Notice: Data Protection Notice – Your Rights & Privacy

NHS Lothian Staff Data Protection Notice: Data Protection Notice

6. **How will people's individual rights in relation to the use of their personal data be addressed by this process? (Rights are not applicable to all types of processing, and expert advice on this may be necessary.)**

- Right of access: Individuals can make a request for access to information held about them by the organisation by making a request to the relevant department. Patient (SAR Team) and Staff (Information Governance) requests would be handled in line with NHS Lothian's Subject Access Policy (nhslothian.scot).
- **East Lothian Council** – Individuals should contact the Data Protection Officer, Post – John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA, Phone – 01620 827827 or email - sar@eastlothian.gov.uk

- Right to rectification: Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete. Any requests regarding rectification of information that it incomplete / incorrect will be managed by the relevant service with support from the Information Governance department if required.
- **East Lothian Council** – Individuals should contact the Data Protection Officer, Post – John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA, Phone – 01620 827827 or email - sar@eastlothian.gov.uk

- Right to object (where applicable): Individuals have the right to object to processing of personal data in certain situations. This right Is not absolute, and NHS Lothian may continue to use the data if we can demonstrate compelling legitimate grounds.
- **East Lothian Council** – Individuals should contact the Data Protection Officer, Post – John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA, Phone – 01620 827827 or email - sar@eastlothian.gov.uk

- Right to restrict processing (where applicable): If an individual objects to processing which is necessary for the performance of NHS Lothian's tasks in the public interest or for the purpose of legitimate interest, we will restrict our processing while we consider whether our legitimate ground override your individual interests, rights and freedoms.
- **East Lothian Council** – Individuals should contact the Data Protection Officer, Post – John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA, Phone – 01620 827827 or email - sar@eastlothian.gov.uk

- Right to data portability (where applicable): The right to data portability only applies when the individual has submitted their personal information directly, through electronic means, to NHS Lothian.
- **East Lothian Council** – Individuals should contact the Data Protection Officer, Post – John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA, Phone – 01620 827827 or email - sar@eastlothian.gov.uk

- Right to erasure (where applicable): NHS Lothian has a legal obligation to retain a full and complete medical record for all their patients, as such data collected for healthcare purposes cannot be erased until its retention period has passed.

When using personal information, our legal basis is usually that its use is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us under the NHS Scotland Act. This means that in most circumstances NHS Lothian will refuse requests for erasure.

- **East Lothian Council** – Individuals should contact the Data Protection Officer, Post – John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA, Phone – 01620 827827 or email - sar@eastlothian.gov.uk

- Rights in relation to automated decision-making and profiling (where applicable): Individuals have the right not to be subjected to a decision, based solely on automated processing, including profiling. NHS Lothian do not currently process any personal or company data in this way.
- **East Lothian Council** – Individuals should contact the Data Protection Officer, Post – John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA, Phone – 01620 827827 or email - sar@eastlothian.gov.uk

7. For how long will the personal data be kept?- refer to our Document Storage Retention and Disposal Policy for advice

Information kept on NHS Lothian systems will be kept in accordance with NHS Lothian's Records Management policy which is in line with the Scottish Government Code of Practice for Health and Social Care 2024.

Information kept on East Lothian council systems will be kept in accordance with East Lothian Council's retention policy.

8. Who will have access to the personal data?

Relevant East Lothian Council staff working across East Lothian Health and Social Care Partnership.

9. Will the personal data be routinely shared with any other service or organisation? – if yes, provide details of data sharing agreement(s) and any other relevant controls. Advice on data sharing requirements is in the Scottish Information Sharing Toolkit.

Yes, information will regularly be shared between NHS Lothian and East Lothian Council as part of the East Lothian Health and Social Care Partnership. The current DSA between NHSL and ELC was Signed off in 2013. Copy can be provided.

10. **Will the personal data be processed internally by an internal Data Processor or externally by an external Data Processor e.g. an IT services provider? – [see Guidance Notes for the definition of Data Processor]. Provide details of contractor selection criteria, processing instructions and contract (may be attached separately).**

Personal data will be processed internally.

11. **Describe what *organisational* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary.)**

Type of Control – examples	Description
Information security and related policy(ies)	As per existing board policies; IT Security, Records Management, Confidentiality, Information Governance. Data Sharing Agreement,
Staff training	Mandatory Information Governance LearnPro modules.
Adverse event reporting and management	NHS Lothian adverse event reporting system, Datix. All incidents logged and investigated by the relevant service / department and Information Governance.
Physical access and authorisation controls	Access restricted to authorised staff.
Environmental controls	As per NHS Lothian IT Security policy.
Information asset management including management of backups and asset disposal	NHS Lothian Information Asset Register managed and reviewed by the NHS Lothian Information Governance department. Relevant systems have been registered on the IAR.
Business continuity	Each service has robust Business Continuity plans in place, and the specific system i.e. eESS, TRAK etc will have NHSL wide Business Continuity and Resilience Plans in place that will be communicated in the event of business/system failures.
Data Backup	Information stored on NHS Lothian systems will be backed up by NHS Lothian. Information stored on East Lothian Council systems will be backed up by East Lothian Council.
Add others where applicable	

12. **Describe what *technical* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary).**

Type of Control – examples	Description
System access levels and user authentication controls	As per existing board policies.
System auditing functionality and procedures	As per existing board policies.
Operating system controls such as vulnerability scanning and anti-virus/anti-malware software	As per existing board policies, Cisco Systems, Ivanti, Nessus.
Network security such as firewalls and penetration testing	As per existing board policies, NHS Lothian firewalls, Nessus.
Encryption of special category personal data	As per existing board policies.
Cyber Essentials compliance(if applicable)	
System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)	SOP's and SSP's are in place for each system used by each organisation
Details of ISO27001/02 accreditation and scope (if applicable)	
Add others where applicable	

13. **Will personal data be transferred to outside the European Economic Area (EEA) or countries without an European Commission-designated adequate level of protection? – if yes, provide details of the safeguards that will be in place for the transfer(s).**

No, no information will be transferred outwith the UK.

14. **Describe who has been consulted in relation to this process – e.g. subject matter experts, service providers, service users.**

[redacted]

[redacted]

15. <u>In light of what is proposed, indicate what level of risk has been identified in relation to the following data protection principles:</u>

Principle	***Low/ Green***	***Medium/ Amber***	***High/ Red***
Personal data is processed in a fair, lawful and transparent manner	X		
Personal data is collected for specific, explicit and legitimate purposes	X		
Personal data is adequate, relevant and limited to what is necessary	X		
Personal data is accurate, and kept up to date	X		
Personal data is kept no longer than necessary	X		
Personal data is processed in a manner that ensures adequate security	X		

16. **Risks and actions identified [see Guidance Notes for more information]. List all that you have identified and ensure that these integrate properly with our NHS Board's risk management process:**

Description	Likelihood	Consequence	Overall Risk rating (LxC)	Mitigation/ Actions	Residual Risk	Risk Owner	Date
Inappropriate access to information.	Unlikely	Major	MR	Access requests approved by staff line manager/senior manager. Access restricted to authorised staff from NHS Lothian and East Lothian Council.	LR	Operational Business Manager, East Lothian HSCP	07/04/2025
Data Breach	Possible	Major	MR	Access restricted to authorised staff. An NHSL Data Breach is reported into Datix, and investigated in accordance with NHSL Data Breach Policy. ELC Data Breaches are reported to the Data Protection Officer/Team for investigation.	LR	Operational Business Manager, East Lothian HSCP	07/04/2025
Information kept longer than required.	Unlikely	Moderate	LR	Data is managed in accordance with NHSL or ELC Records and Retentions Schedules.	LR	Operational Business Manager, East Lothian HSCP	07/04/2025
Staff retaining accounts after leaving the department / organisation.	Possible	Moderate – Major	MR	Service Managers will arrange for accounts to be closed as appropriate after the individual has left their	MR	Operational Business Manager, East	07/04/2025

				department / the organisation.		Lothian HSCP	

17. **Review and Sign-Off**

Role	Advice/ Action/ Sign-Off	Date
IG/ Data Protection (DPO) Advice	[redacted]	02/07/2025 02/07/2025
Information Security Officer Advice (questions 11 and 12)	N/A	
Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO)	N/A	
DPO opinion on whether residual risks need prior notification to the ICO		
Project Lead Sign Off	[redacted]	02/07/2025
Information Asset Owner(s) (IAO(s)) Sign Off	[redacted]	02/07/2025

18. Recommended Review Date: July 2028

GUIDANCE NOTES

Question 2 - Special category personal data

The special categories of personal data are specified in Article 9 of the General Data Protection Regulation and include data about:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a person
- health
- sex life or sexual orientation.

Personal data relating to criminal convictions and offences should be regarded as having the same special nature as those in the categories listed above.

Question 3 – Legal condition

It is illegal to process personal data without meeting adequately a legal condition.

For personal data which does not relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list. Please note that 'data subject' means the person to whom the personal data relates.

- 6(1)(a) – Consent of the data subject
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) – Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject**.**

In NHS Scotland, in many cases condition 6(1)(e) will be the most relevant.

For personal data which relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

In NHS Scotland, in many cases condition 9(2)(h) will be the most relevant.

The Information Commissioner's Office (ICO) advises that public authorities will find using consent as a legal basis difficult. So if the proposed processing is to use consent as its legal basis you need to indicate why this is necessary and seek the advice of an appropriate IG professional.

Question 10 – Data Processor

Article 4 of the General Data Protection Regulation defines a Data Processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller. In practice it includes organisations and companies that provide services such as records storage, transport and destruction and IT services, where we ask them to carry out specific tasks using personal data on our behalf. IT suppliers, even if only accessing data/systems for support issues or bug fixes, are legally defined as a Data Processor. Data Processors may only be used to process personal information where they have provided sufficient guarantees to implement appropriate technical and organisational measures to comply with the law.

Question 16 – Risk Assessment

ASSESSING THE LEVEL (GRADE) OF THE RISK

1. Determine the **Likelihood (L)** of recurrence for the event using **Figure 1** (see below).

   When determining the likelihood you should consider:

   - The frequency of any previous occurrences e.g. How many times a data breach was reported due to this type of issue (e.g. lost records or records accessed without authorisation) in the last month ? in the last year? In the last 5 years?
   - You may need to check the Information Governance, Data Protection and Information Security incidents reported in your organisation in order to assess the likelihood.

   Figure 1: Likelihood of Recurrence definitions

Descriptor	Remote	Unlikely	Possible	Likely	Almost Certain
Likelihood	Can't believe this event would happen – will only happen in exceptional circumstances (5-10 years)	Not expected to happen, but definite potential exists – unlikely to occur (2-5 years)	May occur occasionally, has happened before on occasions – reasonable chance of occurring (annually)	Strong possibility that this could occur – likely to occur (quarterly)	This is expected to occur frequently / in most circumstances – more likely to occur than not (daily / weekly / monthly)

2. Determine the **Consequence (C) rating** using **Figure 2 (see below)**

   Look at **events** that **could lead** to the consequence, **not the consequence itself**

   e.g. Examples of **Events:**

- Records lost in transit (e.g. paper records sent by post)
- Information recorded inaccurately or not recorded in the record
- Data not available due to ransom-ware attack
- Data lost due to error in IT systems – no useful backup available.
- Confidential personal data sent by email to wrong addressee
- Confidential personal data made available to external people due to poor role access definition and testing
- New system or changes in a system went live without appropriate change management (new or changes in data processing started without IG approval)

Examples of Consequences

- Only 1 data subject affected but significant or extreme consequences e.g. missed vital treatment as a consequence of information not being issued to the patient or health professional leading to death or major permanent incapacity
- very sensitive data being exposed to people who don't need to know causes extreme distress (could be patient or staff data)
- Large amount of non-sensitive but personal identifiable data lost in the wind when in transit causing organisational embarrassment in the news for a week
- Staff snooping on neighbours medical records
- Excessive health data shared with social worker (husband under domestic abuse investigation) causing direct threats and stalking.
- Personal health data shared by a charity with private business for commercial/marketing purposes causing unwanted disturbance.
- Reportable data breach to ICO causing monetary penalty.
- Complaint from patient to ICO results in undertaking for better access to health records.
- 1.6 million patients in Google Deepmind affected by the processing
- Compliance Audit recommended
- DC action required
- Undertaking served
- Advisory Visit recommended
- Improvement Action Plan agreed
- Enforcement Notice pursued
- Criminal Investigation pursued
- Civil Monetary Penalty pursued

When considering the consequences of a data breach in your proposed service/system which consequence should you opt for?

Don't choose the worst case scenario or the most likely scenario, but opt for the **"Reasonably foreseeable, worst case scenario"** where if you got a phone call to tell you it had happened, you wouldn't be surprised.

Figure 2: Consequence Table

Descriptor	Negligible	Minor	Moderate	Major	Extreme
Objectives / Project	Barely noticeable reduction in scope / quality / schedule of an eHealth innovation (e.g. new system)	Minor reduction in scope / quality / schedule	Reduction in scope or quality, project objectives or schedule	Significant project over-run	Inability to meet project objectives, reputation of the organisation seriously damaged (e.g. Care Data)
Injury (Physical and psychological) to patient / visitor / staff. e.g. issues with data quality, availability or confidentiality with physical or psychological consequence for the data subject.	Adverse event leading to minor injury not requiring first aid (e.g. data quality issues on instruction to patient re prescription)	Minor injury or illness, first aid treatment required	Agency reportable, e.g. Police (violent and aggressive acts) Significant injury requiring medical treatment and/or counselling. e.g. Staff member who attempted suicide, privacy compromised as A&E shared details beyond "need-to-know".	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.	Incident leading to death or major permanent incapacity (e.g. health records not released on time for making treatment decision causing death or major injury).
Patient Experience e.g. poor access to my records or difficulties to exert data protection rights.	Reduced quality of patient experience / clinical outcome not directly related to delivery of clinical care	Unsatisfactory patient experience / clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience / clinical outcome, short term effects – expect recovery <1wk	Unsatisfactory patient experience / clinical outcome, long term effects – expect recovery - >1wk	Unsatisfactory patient experience / clinical outcome, continued ongoing long term effects
Complaints / Claims e.g. Complaints due to data protection issues	Locally resolved verbal complaint	Justified written complaint peripheral to clinical care	Below excess claim. Justified complaint involving lack of appropriate care	Claim above excess level. Multiple justified complaints	Multiple claims or single major claim
Service / Business Interruption e.g. from constant small interruptions of ICT systems to big Business Continuity issues due to cyberattacks or core data centre being down beyond	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service	Short term disruption to service with minor impact on patient care	Some disruption in service with unacceptable impact on patient care Temporary loss of ability to provide service	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.	Permanent loss of core service or facility Disruption to facility leading to significant "knock on" effect

acceptable levels.					
Staffing and Competence e.g. Poor data protection, confidentiality and ICT security training	Short term low staffing level temporarily reduces service quality (less than 1 day) Short term low staffing level (>1 day), where there is no disruption to patient care	Ongoing low staffing level reduces service quality Minor error due to ineffective training / implementation of training	Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training / implementation of training Ongoing problems with staffing levels	Uncertain delivery of key objective / service due to lack of staff. Major error due to ineffective training / implementation of training	Non-delivery of key objective / service due to lack of staff. Loss of key staff. Critical error due to ineffective training / implementation of training
Financial (including damage / loss / fraud) e.g. derived from compensation rights as per DPA, ICO or NIS fines, ransomware, etc.	Negligible organisational / personal financial loss (£<10k)	Minor organisational / personal financial loss (£10k-100k)	Significant organisational / personal financial loss (£100k-250k)	Major organisational / personal financial loss (£250 k-1m)	Severe organisational / personal financial loss (£>1m)
Inspection / Audit e.g. ICO or NIS interventions	Small number of recommendations which focus on minor quality improvement issues	Recommendations made which can be addressed by low level of management action.	Challenging recommendations that can be addressed with appropriate action plan.	Enforcement action. Low rating Critical report.	Prosecution. Zero rating Severely critical report.
Adverse Publicity / Reputation e.g. media attentions due to data breaches or cybersecurity attacks	Rumours, no media coverage Little effect on staff morale	Local media coverage – short term. Some public embarrassment. Minor effect on staff morale / public attitudes.	Local media – long-term adverse publicity. Significant effect on staff morale and public perception of the organisation	National media / adverse publicity, less than 3 days. Public confidence in the organisation undermined Use of services affected	National / International media / adverse publicity, more than 3 days. MSP / MP concern (Questions in Parliament). Court Enforcement Public Enquiry
Privacy	Negligible harm to the individual arising from disclosure of confidential or sensitive information.	Minor harm to the individual arising from disclosure of confidential or sensitive information. Uncomfortable situation with no material detrimental effect on the person. Minor impact on dignity.	Moderate harm to the individual arising from disclosure of confidential or sensitive information e.g. damage to personal relationships and social standing arising from disclosure of confidential or sensitive information	Major harm to the individual arising from disclosure of confidential or sensitive information e.g. ID theft with potential adverse effect to the individual for which the person is likely to recover	Extreme harm to the individual arising from disclosure of confidential or sensitive information e.g. ID theft with financial loss extreme adverse effect or losing a job or

				overtime or significant loss of personal autonomy detrimental impact on dignity	Extreme risk to life or health

Based on: Australian/New Zealand Standard: Risk Management (AS/NZS4360:2004) Risk Management Standard), (2004) Standards Australia/Standards New Zealand

Clinical Governance and Risk Management Standards (2005), NHS Quality Improvement Scotland

3. Use the risk matrix shown in **Figure 3** below to determine the risk grading for the risk. **L x C =R**

Figure 3: Risk Assessment Matrix

Likelihood	**Consequence**				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Almost certain	LR	MR	HR	HR	HR
Likely	LR	MR	MR	HR	HR
Possible	VLR	LR	MR	MR	HR
Unlikely	VLR	LR	LR	MR	MR
Remote	VLR	VLR	VLR	LR	LR

In terms of grading risks, the following grades have been assigned within the matrix.

- Very Low Risk (VLR)
- Low Risk (LR)
- Moderate Risk (MR)
- High Risk (HR)

DATA SHARING AGREEMENT

Between

and

East Lothian Council

Version 0.4

Date: May 2025

Review Date: May 2028

Contents

1 Parties, Scope and Purpose

1.1 Name and details of the parties who agree to share information

Legal name of parties to DSA
NHS Lothian
East Lothian Council

1.2 Business and legislative drivers.

1.2.1 Purpose of the information sharing

Purpose description	Primary or secondary purpose
This agreement covers both East Lothian Council and NHS Lothian employees, in job roles held within East Lothian Health and Social Care Partnership (ELHSCP), accessing relevant and appropriate East Lothian Council and NHS Lothian IT software and systems. This will support integrated working and ensure relevant Health and Social Care Partnership staff deliver the required function of their respective HSCP integrated service. All relevant software and systems will be detailed within the appendix. Access to the software and systems by appropriate East Lothian Council and NHS Lothian staff will only be permitted if it is deemed required for their job role. All relevant job roles will be listed in the appendix. If any further job roles are highlighted this DSA will be reviewed and updated accordingly.	Primary

Indicate how the data controllers will decide upon changes in the purposes of the sharing	Jointly or independently
	Separately East Lothian Council and NHS Lothian will act as separate Data Controllers In the event that either Party wishes to modify the purposes of processing in relation to data controlled by the **other** Party, these changes will be agreed between the Parties subject to the terms of this Agreement

1.2.2 Legal basis for the processing and constraints

If sharing personal data:	
Under the UK General Data Protection Regulations:	
• 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	• 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis,

	the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

2 Description of the information to be shared

In the table below, NHS Lothian will be the Data Controller for data held on NHS-owned systems, and East Lothian Council will be the Data Controller for data held on Council-owned systems.

Data category	Data Controller status	PD* / SPD*
NHS Lothian Patients Personal Details (inc. Name, Address, Date of Birth etc.)	Sole – NHS Lothian	PD
NHS Lothian Patients Health Data (as stored on Trak or BT Cloud Connect)	Sole – NHS Lothian	SPD
NHS Lothian Staff Personal Details (inc. Name, Address, Date of Birth etc.)	Sole – NHS Lothian	PD
NHS Lothian Staff Training Details	Sole – NHS Lothian	PD
NHS Lothian Staff Contact Details (inc. Work Phone Number, Work email address etc.)	Sole – NHS Lothian	PD
East Lothian Council clients' personal details (inc. Name, Address, Date of Birth, etc.)	Sole – East Lothian Council	PD
East Lothian clients' social work data	Sole – East Lothian Council	SPD
East Lothian Council staff personal details (inc. Name, Address, Date of Birth etc)	Sole – East Lothian Council	PD
East Lothian Council staff training details	Sole – East Lothian Council	PD
East Lothian Council staff contact details (inc. Work phone number, Work email address etc.)	Sole – East Lothian Council	PD

(*) PD – Personal Data as defined within the Data Protection Act 2018 (Part 1, s.3(2))

(*) SPD – Special Category Personal Data as defined within the Data Protection Act 2018 (s.2).

The parties agree this is the minimum amount of data needed to properly fulfil the purposes of this agreement.

3 Description and manner of information sharing

3.1 Data flows

All information will be stored on the relevant NHS Lothian or East Lothian Council systems. If access to these systems is deemed relevant and required for NHS Lothian or East Lothian Council staff (working as part of East Lothian Health and Social Care Partnership), then requests for access to the appropriate systems will be made in accordance with the table below.

TRAK	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf

NHS Lothian Email	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
Datix	Datix form	Datix - Information Governance
Turas	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
SSTS	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
Eess	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
Job Train	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
LearnPro / TURAS Learn	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
Tableau	Management Accountant	Management Accountant
Intranet	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf
eRostering	eRostering team	eRostering team
BT Cloud Contact	User ID Request form	eHealth - Technical Services Policy 005 - NHS Lothian User ID Request Form.pdf

LIST OF ELC SYSTEMS TO BE ADDED AFTER REVIEW WITH JOYCE RUSSELL

ELC IT User Access	East Lothian H&SCP Shared Services NHS employee access to ELC IT Request Form	ELC Policy
MOSAIC etc	Same as above	ELC Policy

Each application for access will be approved by either the NHS Lothian or East Lothian Council member of staff's line manager and counter approved by a senior NHS Lothian manager for example the Head of Operations. Applications for NHS Lothian employees to access East Lothian Council systems are currently signed off by the employees line manager and counter approved by the Chief Social Work Officer in East Lothian Council.

The NHS Lothian or East Lothian Council staff, working as part of the East Lothian Health and Social Care Partnership, who may require access to NHS Lothian systems or East Lothian Council systems, will be working as part of one of these Health and Social Care Partnership teams:

- East Lothian Rehabilitation Service;
- Planning & Performance;
- Adult Social Care;

- Ongoing & Acute;
- Learning & Disabilities; and

Each of these teams will develop and maintain a Standard Operating Procedure (SOP) that will include how they will manage accounts for new joiners, leavers and movers.

For each East Lothian Council staff member that is given access to NHS Lothian systems, and each NHS Lothian staff member given access to East Lothian Council systems, it will be the responsibility of their direct line manager to ensure the staff member is accessing information and systems appropriately. If any inappropriate access is discovered this will be managed through the appropriate organisational policies and procedures relevant to the staff member's employing organisation.

3.2 How data/information is to be accessed, processed and used

Data use description	Associated work instructions, policy or procedure If applicable
All information will be stored on the relevant NHS Lothian or East Lothian Council systems. Data will be collected, used, transferred and kept up to date as appropriate for each system and outlined within the relevant system DPIA.	Policies: • Board local policies on Information Governance and Security • Confidentiality policy • Safe email transmission • East Lothian Council Information Governance and IT Security policies. For further information regarding relevant policies, contact dpo@eastlothian.gov.uk and / or itservicedesk@eastlothian.gov.uk
Each application for access will be approved by the member of staff's line manager and counter approved by the relevant senior manager for example the Head of Operations or East Lothian Council CSWO .	
It is the responsibility of each member of staff to ensure they only access such information and systems as is relevant and necessary to their role . If any inappropriate access is discovered this will be managed through the appropriate organisational policies and procedures relevant to the staff members employing organisation.	

4 Impact assessments and preparatory work

Data Protection Impact Assessment completed and approved May 2025 by NHS Lothian; approved August 2025 by East Lothian Council.

4.1 Actions and countermeasures agreed from the impact assessment and preparatory work.

Information Governance training is provided to all NHS Lothian staff via NHS e-learning modules on Data Protection & Confidentiality, IT Security and Records Management. This

training is completed as part of the corporate induction programme and updated every 18 months.

East Lothian Council staff will complete mandatory e-learning modules on data protection and information security as well as ad hoc e-learning via Metacompliance software and in-person training where appropriate.

5 Fair processing

5.1 List of relevant Fair Processing Notice(s)

NHS Lothian Data Protection Notice: Data Protection Notice – Your Rights & Privacy (nhslothian.scot)

NHS Lothian Staff Data Protection Notice: Data Protection Notice

East Lothian Council Privacy Notice: How your personal information is used | Privacy and cookies | East Lothian Council

East Lothian Council Service-specific Privacy Notices

5.2 Impact on people interests

Impact description	Control measure
Inappropriate access to information	Access requests approved by staff line manager and senior manager. Access restricted to authorised staff from NHS Lothian and East Lothian Council. It is the responsibility of each member of staff to ensure they only access such information and systems as is relevant and necessary to their role. If any inappropriate access is discovered this will be managed through the appropriate employer policies and procedures.
Data Breach	Access restricted to authorised staff. Any breach of NHS Lothian-controlled data will be reported on the Datix system and investigated in accordance with NHS Lothian Data Breach Policy. Any breach of East Lothian Council-controlled data will be reported to the Data Protection Officer / Data Breach Team for investigation.
Information kept longer than required	NHS Lothian-controlled data is managed in accordance with NHS Scotland Records Management Code of Practice. East Lothian Council-controlled data is managed in line with the Council's Retention Schedule, its Information and

	Records Management Policy and its Data Protection Policy.
Staff retaining accounts after leaving the department / organisation	Each service will develop and maintain a Standard Operating Procedure that details the process for new starts gaining accounts and also the process for ensuring accounts for staff that have left their team / the organisation are closed as appropriate.

5.3 Consent decisions

- For the purposes of this data sharing agreement consent will not be required from data subjects.
- Section 1.2.2 of the DSA details the legal basis which is 6(1)(e) – Public Task and 9(2)(h) – Health and Social Care.
- If there is a significant change in the use of information this agreement will be reviewed, updated and re-approved by both parties (NHS Lothian and East Lothian Council).

6 Accuracy of the information

6.1 Agreed steps to ensure the accuracy of any data shared.

- Each Party to this agreement is responsible for the quality of the data under its control.

6.2 Agreed arrangements for any challenges to the accuracy of information

- If a complaint is received about the accuracy of personal data which affects datasets shared with partners in this agreement, the Party that receives the complaint will report the issue to the relevant Data Controller. The relevant Data Controller will replace the out-of-date data with the revised data.

7 Data retention

7.1 Retention periods and purpose.

- Partners to this agreement undertake that information shared under the agreement will only be used for the specific purpose for which it was shared, in line with this agreement. It must not be shared for any other purpose outside of this agreement.
- In each case, the organisation that owns the system on which the data is held remains the Data Controller and record keeper for the information that is shared.
- The retention period for NHS Lothian-controlled information will be in line with local Board policies and procedures and the NHS Scotland Code of Practice for Records Management.
- The retention period for East Lothian Council-controlled information will be in line with the Council's Retention Schedule, and in any case it shall be no longer than is necessary for the purposes of the processing.
- Neither Party shall release information controlled by the other Party to any third party without obtaining the express written authority of the Data Controller.
- In the event that either Party engages a Data Processor and sub-processors to process the information under their control, they warrant to each other that they shall impose terms and conditions on that Data Processor and sub-processors that are no less onerous than the terms of this Agreement.

7.2 Secure disposal of information

- The following destruction processes will be used when the information is no longer required:

Confidentially and securely destroyed in line with each Party's policies and procedures.

- For NHS Lothian-controlled data, electronic files will be kept accurate and up-to-date in in line with the NHS Scotland Records Management Code of Practice.; During the annual data cleansing process information held will be audited and deleted if no longer required to be maintained in line with Data Protection legislation compliance.
- For East Lothian-controlled data, information will be regularly reviewed and disposed of in line with Service's routine operating procedures.

8 The rights of individuals

8.1 Subject access request, FOIs and Objection to processing

Freedom of Information (Scotland) Act – Information Requests

Both Parties are Scottish public authorities for purposes of the Freedom of Information (Scotland) Act 2002 and must respond to any request for recorded information made to them in a permanent form (such as letter or email). This would include an obligation to respond to requests about information sharing practices and procedures such as the arrangements under this Protocol. It should be noted that the actual personal information exchanged between the Parties will, in almost every case, itself be exempt from disclosure under the freedom of information legislation.

Each Party shall be separately responsible for responding to any Freedom of Information requests relating to data under its control. Any request for information submitted to either Party will be processed under the Party's existing FOISA handling procedures, passing up through the organisation's internal review process where appropriate.

Data Protection Act – Objection to processing

Individuals can object where the use of their personal data is causing them substantial, unwarranted damage or distress. This can be an objection to a specific use of information about them or to the fact that either or both parties hold any information at all on that individual.

If this objection is put in writing by the individual (often referred to as a 'section 10 notice') then the relevant Data Controller is obliged to reply in writing within 21 days. This reply should either confirm that the party intends to comply with the request to stop processing data in the manner specified and the timescale within which this will be done, or should confirm that they find the request unreasonable and do not intend to comply, in which case they must state reasons.

Each Party shall have procedures in place to deal with such requests.

A person who wishes each of the parties to cease processing information held on them must be advised that this can only be done by submitting separate written notifications, one addressed to each Party.

Under UK GDPR;

Art. 15 GDPR Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
    - the purposes of the processing;
    - the categories of personal data concerned;
    - the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
    - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
    - the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    - the right to lodge a complaint with a supervisory authority;
    - where the personal data are not collected from the data subject, any available information as to their source;
    - the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Art. 16 GDPR Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Art. 21 GDPR Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning

him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

8.2 Direct Marketing

Direct marketing is not involved in this agreement.

8.3 Automated decisions

No automated decisions are involved in this agreement – in the context of this agreement, "Automated decisions" refer to decisions made using shared information with no human intervention.

9 Security

- only authorised individuals can access, alter, disclose or destroy data. This is achieved through the work instructions, policies and procedures held by each Party.

- authorised individuals act only within the scope of their authority. This is achieved through the work instructions, policies and procedures held by each Party.

  The Parties shall take all reasonable measures to protect against the accidental loss, alteration, or destruction of data. This is achieved through the work instructions, policies and procedures held by each Party.

- Breaches of security leading to Accidental, Unlawful destruction, Loss, Alteration, Unauthorised disclosure of or access to NHS Lothian personal data transmitted, stored, or otherwise processed must be reported within 72 hours of the breach being identified in line with each partner organisations' incident reporting procedures and Data Protection regulations.
- Breaches of security relating to personal data controlled by East Lothian Council must be reported to the Council's Data Breach Team within **24 hours** of any employee's becoming aware of the breach, in line with the Council's Data Breach Procedure.

- Significant data breaches involving personal information provided by partners under this ISP should be notified to the partner that originally provided the information.

- All signatories must have appropriate technical and organisational measures in place to ensure that any personal data shared between partners is handled and processed

in accordance with the requirements of the Data Protection Act 2018, Privacy and Electronic Communication Regulations (PECR) as well as ePrivacy enforceable law.

The security controls applicable by each organisation will be:		Jointly agreed between the parties
	X	Independently decided by each party

10 International transfers of personal data

Personal data shared in line with this agreement will be transferred to		UK countries only
		Out with UK
	X	Will not be transferred outside the UK

10.1 List of countries where the data will be transferred to (if applicable).

N/A

10.2 Reasons for transferring personal data outside the UK.

N/A

10.3 Exceptions

None

	Consent
	Contract performance or it is in the interest of the individual
	Substantial public interest
	Vital interests
	Public registers
	Legal proceedings or advice

11 Implementation of the data sharing agreement

11.1 Dates when information sharing commences/ends

- Will effect from the date of last signature of this agreement.
- Review date of Agreement May 2028.

11.2 Training and communications

- All staff who have an authorised job related purpose to obtain access to either one or both NHS Lothian IT systems and/or East Lothian Council systems must complete both :
    - Mandatory safe information handling training via TURAS e-learning training packages.
    - All staff must complete mandatory East Lothian Council Information Governance / Data Protection training.

11.3 Information sharing instructions and security controls

- Robust SOP's must be in place with each service prior to Data Sharing Agreement being agreed.

11.4 Publication and transparency

- The data collected will not be published. Fully anonymised compliance reports may be generated and published on the basis of the shared data.
- This agreement is available on request
- NHS Lothian's Privacy statement can be found on the NHSL website
- East Lothian Council's generic privacy statement can be found on the Council website.

11.5 Monitoring, review and continuous improvement

- Regular data cleansing according to each Party's local policies and procedures.
- DSA will be audited regularly or when changes are made to the way data is being processed.

11.6 Sharing experience and continuous improvement

- This will be reviewed by NHS Lothian and East Lothian Council on an annual basis.

12 Sign-off and responsibilities

12.1 Name of accountable officer(s)

Accountable Officer Name	Post title	Organisation
[redacted]	[redacted]	East Lothian Health and Social Care Partnership
[redacted]	[redacted]	East Lothian Council
[redacted]	[redacted]	NHS Lothian

Senior Information Risk Owner Name	Post title	Organisation
[redacted]	[redacted]	NHS Lothian
[redacted]	[redacted]	East Lothian Council

12.2 Lead practitioner

Lead IG Practitioner Name	Post title	Organisation

[redacted]	[redacted]	NHS Lothian
[redacted]	[redacted]	East Lothian Council

12.3 Signatories

Name of Parties to DSA	NHS Lothian	
Authorised signatories to DSA	Title /Name	[redacted]
	Role	[redacted]
Board HQ Address	Mainpoint, 102 Westport, Edinburgh, EH3 9DN	
Signature	[redacted]	
Date	22/05/2025	

Name of Parties to DSA	East Lothian Council	
Head Office address	Title /Name	[redacted]
	Role	[redacted]
Head Office address	[redacted]	
Signature	[redacted]	
Date	22/05/2025	

Appendix 1 - All relevant NHS Lothian software and systems that East Lothian Council staff, working as part of East Lothian Health and Social Care Partnership will require access to.

- TRAK – Electronic Patient Records system.
- Datix – Corporate H&S Risk and Issue management system.
- TURAS – Online managers / staff appraisal system for NHS Lothian.
- SSTS – includes eEss access which allows for the appropriate recording for line management of staff actions.
- eEss
- Job Train – This is to support recruitment advertising and applicant shortlisting and recruitment and selection process in line with NHS Lothian Policies and Procedures.
- TURAS Learn – Mandatory Personal Development Plan (PDP) and eLearning tool for NHS Lothian staff.
- Tableau – Management dashboard tool that allows for high level overview of departments / services within ELHSCP
- NHS Email
- eRostering – Supports the management of bank staff allocation of staff time and wage calculations
- BT Cloud Contact – Online Telephone Call system

Appendix 2 – List of ELC IT systems – following review with [redacted]

Appendix 3 – List of East Lothian Health and Social Care Partnership job roles that may require access to NHS Lothian systems. If any further job roles are highlighted this DSA will be reviewed and amended accordingly.

Adult Social Work	Include in DPIA
Community Care Worker	Where required following assessment by General Manager (GM) / Team Manager (TM)
Community Justice Lead Officer	Where required following assessment by GM/TM
Community Payback Work Supervisor	Where required following assessment by GM/TM
General Manager	Y
Mental Health Officer	Y
Senior Practitioner	Y
Service Manager - Adult Social Work	Y
Service Manager - Justice & MHO Services	Where required following assessment by GM/TM
Social Work Assistant - Justice Social Work	Where required following assessment by GM/TM
Social Worker	Y
Social Worker - Justice	Where required following assessment by GM/TM
Team Leader - Community Payback Work	Where required following assessment by GM/TM
Team Leader - Justice	Where required following assessment by GM/TM
Team Manager	Y
Support Plan Broker	Where required following assessment by GM/TM
Senior Support Plan Broker	Where required following assessment by GM/TM
East Lothian Rehabilitation Service	
Community Care Worker	Where required following assessment by GM/TM
Driver/Technican	Y
Main Grade Occupational Therapist	Y
Senior Business Support Administrator	Y
Senior Business Support Assistant	Y
Senior Practitioner - Occupational Therapy Service	Y
Team Manager - Occupational Therapy	Y
Team Manager - TEC	Y
TEC Officer	Y
Learning Disabilities, MH & SUS	
Adult Community Resource Manager	Where required following assessment by GM/TM
Caretaker	N
Community Care Worker	Where required following assessment by GM/TM
Day Service Officer	N
Day Service Officer - Secondment	N
Senior Business Support Assistant - Resource Centre	N
Senior Day Service Officer	N
Senior Practitioner	Where required following assessment by GM/TM
Service Manager - Adult Community Resources	Y

Shared Lives Co-ordinator	N
Social Worker	Where required following assessment by GM/TM
Team Manager - Registered Adult Learning Disability Services	Where required following assessment by GM/TM
Team Manager - Health & Social Care	Y
Ongoing & Acute	
Activity Leader	Where required following assessment by GM/TM
Assistant Manager	Y
Assistant Unit Manager	Where required following assessment by GM/TM
Care Coordinator	Y
Care Support Co-ordinator	Y
Care Support Organiser	Y
Care Support Worker	Where required following assessment by GM/TM
Community Care Worker - Care Homes	Where required following assessment by GM/TM
Day Service Officer	Where required following assessment by GM/TM
Emergency Care Support Worker	Where required following assessment by GM/TM
Emergency Care Worker	Where required following assessment by GM/TM
Finance Assistant - Social Care	Where required following assessment by GM/TM
Housekeeper - Crookston	Where required following assessment by GM/TM
Senior Business Support Assistant	Y
Senior Care Support Co-ordinator	Where required following assessment by GM/TM
Senior Practitioner - Care Homes	Where required following assessment by GM/TM
Senior Social Care Worker	Where required following assessment by GM/TM
Senior Social Care Worker - Days	Where required following assessment by GM/TM
Senior Social Care Worker - Nights	Where required following assessment by GM/TM
Service Manager - Ongoing Care	Y
Social Care Assistant	N
Social Care Assistant - Day	N
Social Care Assistant - Days	N
Social Care Assistant - Nights	N
Social Care Assistant - Nights (T)	N
Social Care Worker	Where required following assessment by GM/TM
Social Care Worker - Days	Where required following assessment by GM/TM
Social Care Worker - Nights	Where required following assessment by GM/TM
Social Worker - Care Homes	Where required following assessment by GM/TM
Team Manager -ECS	Y
Unit Manager	Where required following assessment by GM/TM
Unit Manager - Eskgreen RHOP	Where required following assessment by GM/TM
Planning & Performance	
Business Support Administrator	Where required following assessment by GM/TM
Content Officer	Where required following assessment by GM/TM
Equalities and Engagement Officer	Where required following assessment by GM/TM
General Manager - Planning & Performance	Y
Information Systems Administrator	Where required following assessment by GM/TM
Management Information Officer	Where required following assessment by GM/TM

Organisational & Workforce Development Manager	Y
Planning & Performance Manager	Y
Planning & Performance Officer	Where required following assessment by GM/TM
Senior Business Support Administrator	Where required following assessment by GM/TM
Senior Business Support Assistant	Where required following assessment by GM/TM
Senior Business Support Assistant (Corporate Appointeeship)	Where required following assessment by GM/TM
Senior Communications Advisor	Where required following assessment by GM/TM
Strategy Officer	Where required following assessment by GM/TM
Strategy Officer - Carers	Where required following assessment by GM/TM
Strategy Officer - H&SC	Where required following assessment by GM/TM
Workforce Development Officer	Where required following assessment by GM/TM

PAN-LOTHIAN AND BORDERS PARTNERSHIP

Pan-Lothian Framework
to facilitate lawful information sharing amongst partners

Parties to the framework

NHS Partners

Organisation	Address	ICO Reference
Lothian NHS Board	Waverley Gate 2-4 Waterloo Place Edinburgh EH1 3EG	Z5757124
Borders NHS Board	Borders General Hospital Melrose TD6 9BS	Z772810X

Local Authority Partners

Organisation	Address	ICO Reference
City of Edinburgh Council	8 East Market Street Edinburgh EH8 8BG	Z5545409
Midlothian Council	Midlothian House 40 - 46 Buccleuch Street Dalkeith Midlothian EH22 1DN	Z6284453
West Lothian Council	West Lothian Civic Centre Howden South Road Livingston EH54 6FF United Kingdom ICO REF: Z6925127	Z6925127
East Lothian Council	John Muir House, Brewery Park, Haddington, EH41 3HA	Z5759571
Scottish Borders Council	Council HQ, Newtown St Boswells, Melrose, TD6 0SA	Z5573350

Integrated Joint Boards

Organisation	Address	ICO Reference
Borders Integration Joint Board	Council HQ, Newtown St Boswells, Melrose, TD6 0SA	Z5573350

Edinburgh Integration Joint Board	8 East Market Street Edinburgh EH8 8BG	ZB127030
East Lothian Integration Joint Board	East Lothian HSCP, John Muir House, Brewery Park, Haddington, East Lothian, EH41 3HA	ZA259857
Midlothian Integration Joint Board	Fairfield House 8 Lothian Road Dalkeith Midlothian EH22 3AA	
West Lothian Integration Joint Board	West Lothian Civic Centre Howden South Road Livingston West Lothian EH54 6FF	ZA256125

Police

Organisation	Address	ICO Reference
Police Service of Scotland	Tulliallan Castle, Kincardine, Fife. FK10 4BE	Z3611656

Document History

This document will be signed by all Parties providing an e-signature. Each party will keep its own copy, including historical versions as required by each organisation's record retention policy.

Version Control

Date	Version	Summary of Changes	Changes Section
May 2022	0.1	Initial draft of a new document revising the Pan-Lothian and Borders Partnership General Protocol v.5.10	All
June 2022	0.2	Tracked changes and comments from partners	All
June 2022	0.3	Tracked changes and comments from ZR & CD	All
June 2022	0.4	Updated to reflect changes agreed at the meeting 21.06.2022, and further changes made for consideration by partners following further discussion.	All
January 2024	0.5	Updated to reflect changes agreed at meeting on 17/01/2024	All

February 2024	0.6	Updated to reflect changes agreed at meeting on 21/02/2024	All

Purpose of the agreement

The purpose of this framework is to set out the standards under which the Parties agree to develop safe, secure and compliant data sharing practices through governance arrangements. By endorsing this framework, the Parties agree to adhere to the expected standards and baseline compliance measures it describes.

The framework will cover all data sharing until superseded by new agreements and will not contradict any Party's internal policies. Any subsequent versions of this framework must be endorsed by all Parties.

Purposes for data sharing

All Parties recognise that effective data sharing is essential for the delivery of efficient public services. Information sharing activities facilitated by this framework will support:

- Health and social care functions
- Delivery of certain integrated services
- Management and planning of services
- Improvement of service delivery
- Achievement of better outcomes for individuals in contact with services
- Safety and well-being of individuals who may be in need of care or protection
- Streamlining of data collection so that individuals are not repeatedly asked the same questions
- Investigation, prevention and detection of crime, and management of offenders
- Preservation of personal and community safety
- Assessment of need at individual and community level

Legislative context

This framework sets out high level principles and measures that apply to data sharing among the Parties to support compliance with data protection law, namely the UK GDPR, the Data Protection Act 2018, and its successive legislation.

In recognition that data protection legislation does not apply to information relating to the deceased, adherence to this framework will additionally support compliance with the Human Rights Act 1998 or the Access to Health Records Act 1990.

Individual data sharing activities will be designed to meet the requirements of a range of applicable legislation.

Routine information sharing versus one-off requests

The Parties acknowledge that personal data will be shared between them as a result of 'routine' data sharing activities formally entered into by the Parties, and also in response to 'one-off' requests received for information they hold.

Under this framework, 'routine' data sharing will be established via Data Sharing Agreements between the relevant Parties. For instances of 'one-off' data sharing, Parties will follow their own procedures for ensuring personal data is shared in accordance with the law.

Routine information sharing

To ensure compliance with data protection law, the Parties commit to the following controls, and agree to document them within a Data Sharing Agreement and supporting compliance documentation in accordance with their organisation's own procedures:

- Parties will assess the data sharing activity in accordance with their own policies and procedures. A Data Protection Impact Assessment (DPIA) will be completed in relation to all data sharing activities which meet the criteria for one.
- Parties will identify the lawful basis for processing which supports their involvement in the data sharing activity. Parties recognise that 'consent' will rarely be applicable to data sharing activities arranged under this framework.
- Parties will agree responsibilities for providing privacy information to data subjects, so they are reasonably made aware of the data sharing activity.
- Parties will consider and assess the general fairness and privacy impact relating to the data sharing activity.
- Parties will identify and agree appropriate limitations around the use of data shared under the activity.
- Parties will agree the minimum information required to be shared in order to meet the purpose of the data sharing activity and will not engage in excessive data sharing.
- Parties will agree responsibilities for ensuring information is accurate, and a mechanism for amending it if necessary.
- Parties will agree the retention period(s) which they will apply to the shared data. It is recognised that Parties may apply their own retention rules independently as appropriate depending on their statutory and business need.
- Parties will agree appropriate organisational measures expected to be in place to support the data sharing activity. As a minimum this will include relevant training and procedure documentation to ensure that data is handled consistently when shared as a result of the activity.
- Parties will ensure appropriate physical and technical security measures are applied to the data sharing activity in accordance with their local policies and procedures.
- Parties will agree how data protection breaches will be reported and handled.
- Parties will agree how statutory information requests (e.g.: subject access requests, objections, rectification requests, requests for erasure and freedom of information requests) will be handled.
- Parties will identify and agree how concerns stemming from the data sharing activity can be escalated and resolved if necessary.
- Parties will identify and record any information risk associated with the data sharing activity in accordance with their own policies and procedures.

When entering into data sharing activities under this framework, the Parties recognise that where they will be acting as Controllers in their own right, Data Sharing Agreements will reflect the Controller-to-Controller relationship. Where there is a requirement for a Processor to Controller relationship a Data Processing Agreement will be put in place.

It is recognised that the above controls can be reasonably met in a variety of ways. The Parties shall refer to guidance issued by the Information Commissioner's Office (ICO) when making arrangements for data sharing, including the Data Sharing Code of Practice. Further advice should be sought from local Data Protection Officers, Information Assurance Teams, or equivalents, if needed.

'One-off' requests to share information

The Parties additionally commit to facilitating the exchange of personal data in relation to 'one-off' requests when it is assessed lawful to do so. To ensure accountability in relation to individual instances of data sharing, the Parties commit to ensuring that:

- The Parties will establish and follow their own procedures for requesting and processing 'one-off' requests for personal data (excluding Subject Access Requests).
- The Parties will document why the personal data is required and identify the lawful basis which permits the data to be shared. Requests for information will specify the information which is required and the reason for which it is needed. A record will be retained of the information which is, or is not, shared in the circumstances.
- The Parties will request the minimum personal data necessary for their purpose and will engage constructively with each other when queries or challenges arise.
- The requesting Party shall provide sufficient detail within the request to allow the disclosing Party to assess the necessity and proportionality of the data disclosure.
- Data shall only be shared where there is confidence that to do so complies with the Data Protection Principles.
- The Parties will consider whether it is within the reasonable expectations of the data subject that their personal data will be shared in the way proposed. The Parties will only handle people's data in ways they would reasonably expect or will be able to explain why any unexpected processing is justified. Where the Parties have Privacy Notices in place addressing the data sharing, this will be considered to address the data subject's reasonable expectations.
- Where there is doubt around whether personal data can be lawfully shared, the Parties will consult the relevant Data Protection Officers or Information Assurance Teams or equivalents as detailed in Schedule 1.
- The Parties will ensure that the mechanism for sharing information is secure.

Neither this framework nor any data sharing agreement created as part of it creates or implies any obligation to share information.

Use of statistical & anonymous data.

Organisations in receipt of statistical data from partner organisations must request permission from the Disclosing Party (the data owner) if they wish to use that information for any purpose other than that for which the information was originally provided.

For the avoidance of doubt, 'anonymised data' refers to data that cannot be used in any circumstance to re-identify an individual. 'Pseudonymised data' refers to data that substitutes identifiers (e.g. numbers) for personal information, but might be used in combination with other data (e.g. a key held on another system) to identify individuals. Anonymised data **is not** personal data; pseudonymised data **is** personal data.

Precautions will be taken against the possible identification of individuals by the accrual of datasets. These measures might include (but are not limited to):

- Anonymising data
- Pseudonymising data
- Mapping data flows to reduce duplication
- Regular data cleansing/deletion

Any Party that wishes to submit or circulate reports or articles beyond the Parties to this framework which incorporate statistics or other data supplied by another Party, will ensure that the data owner has the opportunity to view and comment on the report prior to its release.

Procedure for raising concerns / variations / escalation process

Any disputes arising from this framework, or in relation to data sharing arrangements put in place as a result, should in the first instance be referred to the Parties' relevant Data Protection Officers, Information Assurance Teams, or equivalents. Individuals in these roles are authorised to progress and agree minor amendments or technical updates to this framework as and when required.

Review

This agreement will be formally reviewed every five years.

Signatories to the framework

As this agreement governs any data sharing activity entered into between the parties, it should be signed by Chief Executives (or equivalent).

Name	Title	Signature	Date of Issue	Version
Ralph Roberts	Chief Executive, NHS *B*orders			
Calum Campbell	Chief Exec*u*tive, NHS Lothian			

Andrew Kerr	Chief Executive, City of Edinburgh Council		29/02/2024	
Monica Patterson	Chief Executive, East Lothian Council			
Dr Grace Vickers	Chief Executive, Midlothian Council			
Graham Hope	Chief Executive, West Lothian Council			
David Robertson	Chief Executive, Scottish Borders Council			
Andrew Hall	For the Chief Officer Edinburgh Integrated Joint Board		29-01-25	
Fiona Wilson	Chief Officer East Lothian Integrated Joint Board			
Morag Barrow	Chief Officer Mid Lothian Integrated Joint Board			
Alison White	Chief Officer West Lothian Integration Joint Board			

	Chief Officer Borders Integrated Joint Board			
	ACC Local Policing East, Police Service of Scotland			

SCHEDULES

SCHEDULE 1 – Contacts

Organisation	Escalation Contact	Data Protection Officer (if different)
East Lothian Council	Zarya Rathé, Team Manager-Information Governance dpo@eastlothian.gov.uk	See escalation contact
NHS Lothian	Tracey McKinley Information Governance & Security Manager Loth.Dpo@nhs.scot	See escalation contact
NHS Borders	Susie Thomson Borders General Hospital Melrose TD6 9BS dpo@borders.scot.nhs.scot.uk	See escalation contact
Police Scotland	Information Assurance Information.assurance@scotland.police.uk	See escalation contact
City of Edinburgh Council	Kevin Wilbraham Information Governance Manager and Data Protection Officer dataprotection.officer@edinburgh.gov.uk	See escalation contact
Midlothian Council		
West Lothian Council	Carol Dunn Records Manager carol.dunn@westlothian.gov.uk	See escalation contact
Scottish Borders Council	Jenna Paterson Information Manager dataprotection@scotborders.gov.uk	Nuala McKinlay

SCHEDULE 2 – DSA Templates

Contacts regarding Data Sharing templates

2.1 Data sharing activities between any of the Parties (excluding NHS) and Police shall use the template produced by Police Scotland as a guide for agreeing specific data sharing terms.

Contact: Information.assurance@scotland.police.uk

2.2 Data sharing activities between any of the Parties (excluding Police) and NHS shall use the template produced by NHS Central Legal Office as a guide for agreeing specific data sharing terms.

Contact: Loth.Dpo@nhs.scot

2.3 Data sharing activities between NHS and Police shall use either of the templates set out at sections 2.1 or 2.2 above as a guide for agreeing specific data sharing terms. The template used shall be agreed between the Parties on a case-by-case basis.

Appendix

Freedom of Information Act 2002 / Environmental Information (Scotland) Regulations 2004

As Public Authorities, the Parties might receive requests for information under the Freedom of Information (Scotland) Act 2002 (FOISA) or the Environmental Information (Scotland) Regulations 2004 (EISRs) that address information shared between the Parties. In these circumstances, the Party that receives the request shall seek the views of the Party(ies) that created and/or originally shared the information prior to issuing a response to the requester.

Notwithstanding the above, the sole discretion regarding whether to disclose the information or apply an exemption shall rest with the Party that receives the request.

In addressing requests under FOISA and the EISRs, advice should be sought from the Party's Freedom of Information officer(s) or equivalent.

Public Records (Scotland) Act 2011

As named Authorities under the Public Records (Scotland) Act 2011 (PRSA), all Parties shall create and maintain Records Management Plans ('RMPs') addressing the management of records generated and shared between the Parties. The Parties shall ensure that their RMPs remain relevant and up to date with reference to the Keeper of the Records of Scotland's Model RMP.

Advice and guidance should be sought from the Records Manager or equivalent named within Element 2 of the Party's RMP.