Data Protection Policy

Introduction

This policy sets out the commitment of the Scottish Land Commission (The Commission) to exercise best practice when processing personal data, to comply with the data protection law, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) and the Data (Use and Access) Act 2025 (DUAA).

Data protection law and principles

Data protection law governs the processing of personal data by a data controller, or by a data processor on their behalf. It sets out obligations for organisations processing personal data, and rights for individual data subjects. Scottish Land Commission acts a s both a data controller and a data processor in the course of its activities.

The UK GDPR sets out seven key principles for the processing of personal data, these are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Lawfulness, fairness and transparency

The Commission will process all personal data in line with a lawful purpose, as set out in the UK GDPR, and will record the purpose in its record keeping process.

The Commission seeks to help individuals understand how it processes their personal data through clear, transparent communications such as the privacy statement on the Commission's website and other information provided to individuals at the point of data collection.

Purpose limitation

The Commission will process personal data for specified, explicitly and limited purposes, and will not further process that data for incompatible purposes. Processing of personal data beyond the purpose for which it was originally collected will be risk assessed/reviewed via the DPIA process to ensure that it complies with the data protection principles.

The Commission will often rely on 'legal obligation' to process personal data in relation to case work. This is because we are under a legal obligation to inquire into alleged

breaches of the Tenant Farming Commissioner's codes of practice as stipulated in the Land Reform (Scotland) Act 2016.

Data minimisation

The Commission will process personal data which is adequate, relevant and limited to what is necessary for its purpose. The DPIA process ensures that data collection will be risk assessed to ensure that excessive or unnecessary data is not processed.

Anonymisation of data will be considered and applied where appropriate to ensure that individuals are identified only where necessary.

Accuracy

The Commission will process personal data which it understands to be accurate, complete, up-to-date, and relevant to its purpose. Where inaccuracies are found, these will be addressed prior to further processing, or the data deleted. The Commission will take all reasonable steps to ensure that personal data remains accurate over time.

Storage limitation

The Commission will retain personal data only for as long as is necessary to its purpose and will apply clearly defined rules governing retention and disposal of data, as per the relevant completed DPIA. Destruction of personal data will be carried out securely and in line with ICT protocols.

Where exception to these rules are necessary, reasons for this will be recorded on the relevant DPIA, and steps taken to ensure that personal data is adequately protected.

The Commission will continually develop and implement safeguards to protect personal data, ensuring these remain in line with developments in technology and the threat landscape, applying them consistently and proportionately based on risk. Regular reviews of safeguarding effectiveness will be carried out.

Security and data breaches

The Commission will implement appropriate organisational and technical measures to protect personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Such measures will protect the confidentiality, availability and integrity of personal data at all times.

The Commission will operate appropriate procedures for managing any information security incident that constitutes a personal data breach, including notification to the Information Commissioner's Office (ICO) if required. Assessment of data breaches and, where appropriate reporting, is the responsibility of the Data Protection Officer.

Accountability

The Commission will put adequate resources in place to ensure, and evidence, compliance with the data protection principles and data protection law. These will include:

- Appointment of a DPO

- Implementation of DPIA's
- Maintenance of detailed records of processing activities
- Maintenance of appropriate consent and contract documentation
- Regular training for staff
- Regular testing and review of its controls to privacy.

Special category and criminal offence data

Data protection legislation defines categories of personal data which require additional conditions to be met for their processing to be fair and lawful. The Commission will process such data in accordance with the data protection principles, and in accordance with this policy.

DPIA's are required to detail whether any processing of special category or criminal offence data alongside the purpose and lawful basis for doing so.

Individuals' rights

The Commission will fulfil its obligations to uphold individuals' rights and will operate procedures to appropriately manage requests received from individuals to exercise their rights. These requests will be managed by the DPO.

Data sharing and disclosure to third parties

Personal data will be disclosed to third parties appropriately and governed by data sharing agreements and data processor contracts which will provide for appropriate safeguards. Disclosure will be in line with a specific and lawful purpose which will be identified prior to disclosure.

Where the Commission transfers personal data beyond the UK, including to its data processors, it will do so in line with a relevant condition as set out in data protection legislation, and with any required contractual clauses in place, thereby providing an appropriate level of protection for personal data. Such transfers will be risk assessed and the relevant condition recorded in our record of processing.

Data Protection Impact Assessments (DPIAs)

The Commission is committed to the consistent use of DPIAs which are mandatory in certain circumstances, to improve the early identification and mitigation of privacy risk and to ensure we meet our obligations in respect of data protection law.

DPIAs will be considered wherever there is significant change to the way personal data is processed. The DPO will advise as to whether a DPIA is required, including whether a statutory requirement to conduct a DPIA exists. The DPO will notify the ICO of a DPIA in circumstances where data protection law requires it.

Training and awareness

The Commission will ensure that all its staff and contractors understand their responsibilities in relation to data protection and privacy by providing annual training,

including specialised training for those working in areas, or undertaking roles, with higher privacy risk.

Roles and responsibilities

All Commission staff and contractors have responsibilities for data protection and privacy, are bound by the commitments of this policy, and are required to effectively operate the various operational procedures which facilitate its fulfilment in practice.

The DPO has operational responsibility for data protection and privacy within the Commission. The role is mandated and governed by data protection legislation and is an impartial advisory role to the organisation's highest level of management. They must act as the point of contact with the ICO and are responsible for ensuring that the procedures and training which support the fulfilment of this policy are operated effectively and kept up to date.

The Commission's Accountable Officer has strategic oversight and overall responsibility for data protection and privacy.

Management team are responsible for ensuring that the commitments given in this policy are met, and that the privacy function is appropriately resourced and accounted for within wider governance of the Commission.

The Commission's board is responsible for ensuring that the DPO is able to fulfil their role impartially and without conflict of interest and can operate according to the requirements set out in data protection legislation.

It is expected that the Commission's Data Processors and Data Sharing Partners assist in meeting the commitments given in this policy, to uphold the agreements made in data processing contract and data sharing agreements, and to fulfil their own statutory obligations in respect of data protection.

Review

This policy will be reviewed by the DPO and approved by Management Team at two-year intervals, unless earlier review is appropriate.

Version	Description	Author	Effective date	Date for review
V1.0	**Initial policy adopted**	**C. Bremner**	**2018**	**2020**
V2.0	**Policy updated inline with legisltation**	**S. Smith**	**April 2026**	**April 2028**

Data protection policy – Annex A

Definition of key terms

Anonymisation

The process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

Criminal conviction data

Personal data relating to an individual's criminal convictions, or the alleged prosecution of offences, is covered by additional safeguards and cannot be processed unless under official authority or where authorised by law.

Data controller

An organisation processing personal data on behalf of a data controller, acting on their instruction.

Data processor

An organisation processing personal data on behalf of a data controller, acting on their instruction.

Data Protection Impact Assessment (DPIA)

A form of risk assessment that can help identify privacy risk at an early stage in the change cycle to allow that risk to be controlled appropriately.

Data Protection Officer

The Data Protection Officer (DPO) is a role required for certain organisations under the GDPR. DPOs are responsible for overseeing data protection strategy and implementation to ensure compliance with data protection legislation.

Data subject

The 'natural person' to whom the personal data relates and who is identifiable from that data.

Data subjects' rights and lawful purpose

Data protection legislation sets out the following rights for data subjects:

- to be informed
- to access personal data
- to rectification of inaccurate personal data
- to erasure of personal data
- to restrict processing of personal data
- to data portability

- to object to processing of personal data
- to protection from automated decision making, including profiling.

Encryption

The process of encoding information or data so that only authorised parties can access it.

Personal data

Information relating to identifiable person who can be directly or indirectly identified.

Processing

The use of personal data in any way – this includes collecting, creating, analysing, copying, storing, transferring, sharing, disclosing, publishing and disposing of personal data.

Pseudonymisation

De-identifying data so that a coded reference or pseudonym in attached to a record to allow the data to be associated with a particular individual without that individual being identified directly. Legally, this data remains personal data.

Record of Processing

A record of the activities an organisation undertakes that involve the processing of personal data. This is a legal requirement and must contain certain information in relation to each processing activity.

Special category personal data

Types of personal data which require additional safeguards and conditions to be met for processing to be fair and lawful. Categories are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic or biometric data
- sex life or sexual orientation.