Data Protection Policy

Document Control

Document last saved: 26 August 2026

Version	Changes	Author	Date
1.0	First release.	F Finlayson	31/05/2016
2.0	DP 2018 Act update – rewritten.	F Finlayson	12/06/2018
3.0	Updated to UK GDPR. Minor amendments. Added roles/responsibilities and training.	M Thomson	20/02/2023
4.0	Comprehensive update for regulatory compliance, integration of explicit DPO statutory duties, and text completion.	I Fox	18/08/2026
5.0	Update to formatting.	M Thomson	26/08/2026

Introduction

The Highland & Western Isles Valuation Joint Board handles personal information about individuals. This activity triggers strict legal obligations to protect that information under the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

The Assessor and Electoral Registration Officer (ERO) is registered as a Data Controller with the Information Commissioner's Office (ICO):

- ICO Registration Number**:** Z7182146

Data Processing Scope

The Assessor and Electoral Registration Officer is a Data Controller under the DPA and the UK GDPR. His office holds information for the purposes specified in the registered entry on the Data Protection Register; including valuing properties in Highland and Western Isles to compile the non-domestic rating Valuation Roll and the Council Tax Valuation List and he may use this information for any of the three services he is responsible for. He may get information about properties from others or may give property information to them. If he does, it will only be as the law permits. He may check information he receives about a property, with what is already in his records. This can include information provided by an individual, as well as by organisations, such as constituent councils, government departments or agencies and other Assessors Offices in Scotland. He may not give information to anyone outside The Highland & Western Isles Valuation Joint Board unless the law permits him to do so. This authority does not allow a third party to request personal information held about an individual under the subject access provisions of the DPA and the UK GDPR. As Electoral Registration Officer (ERO) he also holds information relating to the Register of Electors which he compiles under a delegated authority from each of our two constituent authorities. The data is protected and its publication and availability to others is regulated under Regulations 92 – 114 of the Representation of the People (Scotland) Regulations 2001 which impose tighter restrictions

on the Full Register than on the Open Register, which electors can opt to have their names excluded from.

Statement of Compliance

The Assessor and ERO processes large volumes of personal and special category data belonging to citizens, employees, suppliers, and service users. This policy applies strictly to all computerised, structured paper files, and unstructured records.

The Board ensures full adherence to the ICO Employment Practices Code for staff records, balancing statutory delivery with individual privacy rights.

Key Legal Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person ("data subject"). This includes direct or indirect identifiers such as names, ID numbers, location data, or online identifiers.
- **Special Categories of Personal Data**: High-risk personal data revealing racial/ethnic origin, political opinions, religious/philosophical beliefs, trade-union membership, genetic/biometric identification data, health data, or data concerning a person's sex life or sexual orientation.
- **Processing**: Any operation performed on data, including collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.
- **Data Controller**: The entity that determines the purposes and means of processing personal data. The Assessor and ERO acts as the primary Data Controller.

The Data Protection Principles

The Board enforces compliance with the seven core principles of the UK GDPR. Personal data must be:

1. Lawful, Fair, and Transparent: Processed legally and transparently.
2. Purpose Limitation: Collected for specified, explicit, and legitimate purposes.
3. Data Minimisation: Adequate, relevant, and limited to what is necessary.
4. Accuracy: Accurate and kept up to date; inaccurate data must be erased or rectified immediately.
5. Storage Limitation: Kept in an identifiable form no longer than necessary, except for statutory archiving or statistical purposes under Article 89(1).
6. Integrity and Confidentiality: Secured against unauthorised processing, accidental loss, destruction, or damage using robust technical and organisational barriers.
7. Accountability**:** The Data Controller is directly responsible for demonstrating compliance with all the principles listed above.

In addition, the controller shall be responsible for, and be able to demonstrate compliance with, the above principles.

Roles and Responsibilities

Upholding data protection principles is an operational requirement across all levels of the Valuation Joint Board:

- **The Assessor & Management Team**: Responsible for enforcing this policy uniformly across the Board's three regional offices.

- **Line Managers**: Tasked with ensuring operational staff are trained in, aware of, and compliant with their data security responsibilities.
- **Individual Staff Members**: Required to handle all personal data safely, report breaches immediately, and follow organisational data security protocols.
- **The Data Protection Officer (DPO)**: Appointed under Articles 37–39 of the UK GDPR and Sections 69–71 of the DPA 2018, the DPO is independently responsible for:

    - Informing and advising the Board and its employees of their data protection obligations.
    - Monitoring internal compliance, managing staff training, and conducting data protection audits.
    - Advising on and monitoring Data Protection Impact Assessments (DPIAs).
    - Acting as the primary point of contact for the Information Commissioner's Office (ICO) on all processing matters.

All staff handling information must have completed the Information Management course through the Highland Council's online learning module and any other relevant training that is required to use records management systems and supporting ICT systems required in their roles.

Managers and supervisors are responsible for information held within their areas. Managers and supervisors must ensure that all their staff have understood their obligations under this Policy (both general obligations and those that are specific to their role) and other relevant policies including the Highland Council's Information Management Policy. Managers should support their staff in this regard by highlighting relevant parts of policies that apply to the roles being performed by a member of staff. Managers and supervisors must ensure that all their staff have completed the Information Management online learning module and other relevant training and ensure that it is part of Employee Review & Development Plans. All training results should be provided to the Central Admin Team who will record when training was completed, and the pass rate achieved by each member of staff.

Managers and supervisors should also ensure that staff are aware of any relevant data sharing agreements.

Staff Communication

This policy and associated guidance will be made available to staff through the Valuation Joint Board's Intranet.

Lawful Bases for Processing

To process personal data legally, the Board relies on specific conditions set out under UK legislation.

1. Standard Personal Data

Processing is conducted primarily under the following UK GDPR Article 6 conditions:

- Public Task: Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Assessor and ERO.
- Legal Obligation: Necessary for compliance with statutory laws (e.g., Council Tax and Electoral Registration legislation).
- Contractual/Employment: Necessary for employee contracts and vendor management.

2. Special Category Data

Processing high-risk data (such as political opinions or health details) requires an Article 6 condition **plus** an Article 9 condition, alongside meeting the requirements of Schedule 1 of the DPA 2018:

- Statutory and Government Purposes: Processing is necessary for reasons of substantial public interest.
- Employment and Social Protection**:** Necessary for fulfilling employment law obligations.

Data Breach Notification & Audits

- **Breach Reporting:** Any identified or suspected data breach must be reported to the DPO immediately. If a breach poses a risk to individuals' rights and freedoms, the DPO must notify the ICO within 72 hours of detection.
- **Policy Review**: This document will be audited annually by the DPO to match updating guidance from the ICO Register of Data Controllers.

Further information is available from The Highland & Western Isles Valuation Joint Board's appointed Data Protection Officer at Lanarkshire Valuation Joint Board.

2 November 2026