Personal Data Breach Policy

Document Control

Document last saved: 25 August 2026

Version	Changes	Author	Date
1.0	First release	M Thomson	11/06/18
1.1	Review	W Gillies	13/06/18
1.2	Review	M Thomson	25/02/23
1.3	Review	I Fox	30/07/26
1.4	Review – DUAA amendments	M Thomson	25/08/26

Overview

Under the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (DUAA), all organisations have a statutory duty to report certain types of personal data breaches to the Information Commissioner's Office (ICO) where the incident poses a risk to individuals.

Organisations must inform the ICO within 72 hours of becoming aware of a breach, where feasible. This 72 hour window applies universally to all forms of personal data, including processing covered under the Privacy and Electronic Communications Regulations (PECR).

This policy and procedure apply to all personal data breaches involving:

- The Highland & Western Isles Valuation Joint Board data.
- The Assessor for Highland & Western Isles data.
- The Electoral Registration Officer for Highland & Western Isles data.

What is a Personal Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

A breach is more than just losing data; it is a security incident affecting the confidentiality, integrity, or availability of personal data. Examples include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data (e.g., encryption by ransomware, accidental deletion).

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable e.g., when it has been encrypted by ransomware, or accidentally lost or destroyed.

Reporting & Internal Complaints Handling

All data security breaches or suspected data security breaches must be reported immediately to the Data Protection Officer (DPO), the internal DPO (investigating officer), and the Assessor. The DPO is currently based at Lanarkshire Valuation Joint Board.

Data Subject Complaints under DUAA 2025

If an individual submits an internal complaint regarding a personal data breach or an alleged failure to protect their information, the Board will adhere to the following statutory requirements:

- Accessible Channels: The Board provides an accessible electronic data breach complaint form on its website.
- 30-Day Acknowledgment: The internal investigating officer must formally acknowledge receipt of the complaint within 30 days.
- Investigation and Updates: The Board will investigate the subject matter and keep the complainant informed of its progress and final outcome without undue delay.

Details of all breaches and subsequent data protection complaints must be recorded in the Personal Data Breach Log held within Central Admin. The log must record the date, nature of the breach/complaint, notification timelines, and all appropriate investigative or mitigating steps taken.

Containment and Recovery

The DPO or delegated investigating officer will take immediate action to:

- Confirm Data Nature: Determine if the incident involves sensitive personal data (e.g. medical information, biometric data, or criminal convictions) or data that could facilitate identity theft (e.g. bank details, National Insurance numbers).
- Isolate the Incident: prevent further data loss or dissemination.
- Enforce Cooperation: ensure all staff cooperate fully and transparently to allow accurate risk assessments.
- Determine Actions: decide who must be notified internally, whether to report the loss to the ICO, and if affected, individuals must be notified without undue delay.

Assessing the Risks

The DPO or investigating officer will evaluate the likelihood and severity of the impact on individuals' rights and freedoms based on:

- The type and sensitivity of the data.
- Technological protections in place (e.g. end-to-end encryption).
- The current status and location of the compromised data, if known.
- The categories and approximate number of individuals and records affected.
- The potential material, non-material, physical, or financial harm to individuals.
- Any wider organisational or societal consequences.

The results of this risk assessment will be communicated immediately to the Assessor.

Notification of Breach

Recital 85 of the UK GDPR clarifies that unaddressed personal data breaches can result in physical, material, or non-material damage to natural persons (e.g., identity theft, financial loss, or damage to reputation).

- ICO Notification: If the assessment reveals that a risk to individuals' rights and freedoms is likely, the DPO or Assessor must notify the ICO within 72 hours of becoming aware of the breach. If the risk is unlikely, an ICO notification is not required, but the justification must be recorded in the internal log.
- Individual Notification: If a breach is likely to result in a high risk to individuals, they must be notified without undue delay. The notification will explain how and when the breach occurred, the data involved, and the remedial steps taken by the Board. Large-scale notifications require final sign off from the Assessor.
- Third Parties: Where appropriate, law enforcement (Police Scotland), banks, or professional bodies will be contacted to reduce potential financial fraud or crime.

All official regulatory reports must be completed through the ICO online portal on the ICO Report a Breach webpage.

Data Processors

Where the Board utilises third-party data processors (such as external print contractors or cloud software providers), those processors are required under Article 33(2) of the UK GDPR to inform the Board without undue delay as soon as they become aware of any actual or suspected personal data breach.

Evaluation and Response

Containing a data breach is only the first step. If an incident is caused by a systemic weakness, ongoing procedural error, or data inaccuracy, immediate steps must be taken to update organisational and technical measures.

1. DPO Review: The DPO or investigating officer will review the incident and effectiveness of the containment.
2. Management Reporting: A formal report detailing root causes and preventative recommendations must be provided to the Assessor and the Management Team within three weeks of the incident.
3. Oversight: Any data breach escalated to the ICO will be added to the agenda of the next scheduled Management Team meeting to monitor preventative updates.

2 November 2026