



# DATA BREACH POLICY

## Document history

Notes of changes	Version No.	Date of approval and adoption
Data breach policy in original format	1.0	24 April 2021
Reviewed 2023 no changes		27 March 2023
Reviewed 2025 no changes		5 April 2025
Reviewed 2025 change to contact details		11 April 2026

**THIS DATA BREACH POLICY IS PUBLISHED AS APPROVED BY  
CUMBRIA ASSOCIATION OF LOCAL COUNCILS ON 11 April 2026**



## **Cumbria Association of Local Councils (CALC)**

### **Data Breach Policy**

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

#### **1. Notifying the Information Commissioners Office (ICO)**

Currently, data breaches do not have to be routinely notified to the ICO or others although the ICO recommends that it is good practice so to do. However, guidance states that organisations should notify the Information Commissioners Office of a breach where it is likely to result in a risk to the rights and freedoms of individuals or if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

All data breaches will be recorded using the ICO's online system and the following information will be provided:

- The potential scope and cause of the breach
- Mitigation actions the council plans to take
- Details of how the council plans to address the problem.

#### **2. Notifying the individual concerned**

If a breach is likely to result in a high risk to the rights and freedoms of individuals (such as through identity theft) CALC will notify those concerned.

#### **3. Timescales**

Under the UK GDPR, we are required to report a personal data breach, which meets the reporting criteria, within 72 hours to the Information Commissioner. In line with the accountability requirements, all data breaches must be recorded by CALC along with details of actions taken. This record will help to identify system failures and should be used to improve the security of personal data.

#### **4. Notifying CALC**

If anyone (including a third party such as a payroll provider) suspects that a data breach has occurred details of the alleged breach should be submitted immediately in writing to:

Parish Development Officer (PDO)  
Cumbria Association of Local Councils  
Voreda House  
Portland Place  
Penrith  
CA11 7BF



## **5. ICO Self-assessment tool**

Following notification of a breach the PDO will carry out the ICO self-assessment tool to determine whether or not the breach needs to be reported to the ICO.

CALC's PDO will also advise the Chief Officer and the Chair of the situation as soon as possible.

## **6. Recording and investigating the breach**

Whether or not the breach is required to be reported to the ICO the breach must be recorded by the PDO and investigated.

## **7. Following the investigation**

The PDO will inform the Chief Officer and the Chair of CALC of the result of the investigation. Any lessons learned from the outcome of the investigation will be disseminated to all employees by the Chief Officer through a team debrief.

It should be noted that if the PDO is responsible for the breach, all actions outlined above will instead be carried out by the Chief Officer of CALC.