

Dalton with Newton Town Council – Data Breach Policy

Adopted by Full Council on:

Review Date:

1. Purpose

This policy sets out Dalton with Newton Town Council's procedures for responding to and managing personal data breaches, in accordance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

The Council is committed to protecting the personal data it holds and processes, and to responding promptly and effectively in the event of any data breach to minimise potential harm to individuals and to the Council.

2. Definition of a Personal Data Breach

A **personal data breach** is any incident that results in the **accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to**, personal data transmitted, stored or otherwise processed by the Council.

This may occur through, for example:

- Loss or theft of equipment or data (e.g. laptop, USB drive, paper file);
 - Unauthorised access to or disclosure of personal data;
 - Human error (e.g. sending information to the wrong recipient);
 - Failure of IT systems or cyber-attack;
 - Accidental deletion or alteration of records.
-

3. Identifying and Reporting a Data Breach

Any councillor, employee, contractor, or third-party service provider (such as a payroll or IT provider) who becomes aware of a data breach or suspects one has occurred **must report it immediately** to the **Clerk**, who acts as the Council's **Data Protection Officer**.

Reports should include:

- A description of what has happened;
- The type and amount of personal data affected;
- The number or categories of individuals involved (if known);

- When and how the breach was discovered.

Reports should be made in writing to:

The Clerk, Dalton with Newton Town Council

Station Road, Dalton-in-Furness, Cumbria, LA15 8DT

Email: townclerk@daltontowncouncil.gov.uk

4. Assessing and Recording the Breach

Upon notification, the Clerk will:

- Log the incident in the **Council's Data Breach Register**;
- Conduct an initial assessment to determine:
 - The nature and scope of the breach;
 - The type of data involved;
 - The potential impact on affected individuals; and
 - Whether the breach is reportable to the **Information Commissioner's Office (ICO)**.

The assessment and any follow-up actions will be documented, including corrective measures taken to prevent recurrence.

5. Notifying the Information Commissioner's Office (ICO)

Under the **UK GDPR**, the Council **must report** any personal data breach to the **Information Commissioner's Office (ICO) within 72 hours** of becoming aware of it, **unless it is unlikely to result in a risk to the rights and freedoms of individuals**.

Reports will be made using the ICO's online system:

 <https://ico.org.uk/for-organisations/report-a-breach/>

When notifying the ICO, the Council will provide:

- The nature of the personal data breach (including categories and approximate number of individuals and data records concerned);
- The likely consequences of the breach; and
- The measures taken or proposed to address the breach and mitigate any adverse effects.

If all details are not yet known at the time of notification, the Council will submit the initial report within the 72-hour period and provide further information as it becomes available.

6. Notifying Affected Individuals

Where a personal data breach is **likely to result in a high risk** to the rights and freedoms of individuals (for example, risk of identity theft, financial loss, or damage to reputation), the Council will notify affected individuals **without undue delay**.

Such notifications will include:

- A clear description of the breach and its likely consequences;
 - The measures taken or proposed by the Council to address it;
 - Contact details for further information and assistance (the Clerk).
-

7. Review and Learning

Following any data breach, the Clerk will:

- Investigate the cause and evaluate the effectiveness of the Council's response;
 - Implement any necessary changes to prevent recurrence (e.g. staff training, policy review, system improvements); and
 - Report findings to the **Full Council** where appropriate.
-

8. Record Keeping and Accountability

The Clerk will maintain a **Data Breach Register**, documenting:

- Details of all personal data breaches (whether reportable or not);
- The results of investigations;
- Any notifications made to the ICO and/or individuals;
- Steps taken to prevent recurrence.

This record will support compliance with the Council's accountability obligations under the UK GDPR.

9. Policy Review

This policy will be reviewed annually by the Clerk and approved by Full Council, or sooner if there are changes to relevant legislation or guidance issued by the **Information Commissioner's Office (ICO)**.

Signed: _____

Clerk to Dalton with Newton Town Council

Date: _____