COULSTON PARISH COUNCIL

Data Breach Policy

ADOPTED: FOR REVIEW:

Coulston Parish Council – Data Breach Policy

Approved by Coulston Parish Council on: [Insert Date] **Next Review Date:** [Insert Date]

1. Purpose and Objective

Coulston Parish Council (the Council) is a **data controller** under the **Data Protection Act 2018 (DPA 2018)** and the **UK General Data Protection Regulation (UK GDPR)**. The Council routinely holds and uses personal data about staff, councillors, electors, and contractors in the performance of its statutory functions. This policy sets out the procedures for identifying, reporting, and managing personal data breaches to ensure compliance with the law and to protect the rights of individuals.

2. Definition of a Data Breach

A personal data breach is a security incident leading to the **accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data**. Common examples include:

- Loss of a laptop, smartphone, or unencrypted USB drive containing personal data.
- Sending an email containing personal data to the wrong recipient.
- Unauthorised access to Council IT systems or records.
- Leaving paper records containing sensitive information in an unsecured, public-facing area.

3. Roles and Responsibilities

- **The Council:** Holds ultimate legal responsibility for compliance with data protection laws.
- **The Clerk (Proper Officer):** Typically acts as the Council's **Data Protection Officer (DPO)** or manages the arrangements to comply with the DPA 2018. The Clerk is responsible for investigating suspected breaches and maintaining the Council's breach log.
- **Councillors and Staff:** Must follow safe working practices and report any suspected data breach to the Clerk immediately upon discovery.

4. Incident Response Procedure

In the event of a suspected or actual data breach, the following steps must be taken:
Step 1: Internal Reporting The person who discovers the breach must notify the **Clerk** immediately. If the Clerk is unavailable, the Chair of the Council should be notified.
Step 2: Containment and Recovery The Clerk will take immediate action to limit the breach. This may include:

- Disconnecting a compromised computer from the network.
- Remotely wiping a lost mobile device if such facilities are set up.
- Attempting to recover lost data (e.g., through backups).

Step 3: Risk Assessment The Clerk will assess the severity of the breach based on the **likelihood and impact** on the rights and freedoms of the affected individuals. This assessment will determine if the breach must be reported externally.
Step 4: Notification to the ICO If the breach is likely to result in a risk to individuals, the Council must report it to the **Information Commissioner's Office (ICO)** without undue delay and, where feasible, within **72 hours** of becoming aware of it.
Step 5: Notification to Affected Individuals If the breach is likely to result in a **high risk** to the rights and freedoms of individuals (e.g., identity theft or financial loss), the Council must inform the affected data subjects directly and without undue delay.

5. Documentation

The Council must maintain a record of **all personal data breaches**, including the facts relating to the breach, its effects, and the remedial action taken. This log must be available for inspection by the ICO if requested.

6. Prevention and Review

Following any breach, the Council will conduct a review of its **internal controls** and **risk management** procedures to identify necessary improvements. The Council will ensure that:

- Staff and councillors receive regular data protection and cyber security training.
- **Strong passwords** are used and never shared.
- All portable devices and removable media are **encrypted**.
- Backups are performed regularly and tested for reliability.

7. Policy Review

This policy shall be reviewed **annually** by the Council to ensure it remains fit for purpose and compliant with current legislation.