COLLINGHAM *Parish Council*

Data Breach Policy

Adopted:	26th February 2026
Next Review:	February 2027

1. Purpose

This policy sets out how Collingham Parish Council (the Council) identifies, manages, records and reports personal data breaches in line with UK data protection law. It is designed to ensure breaches are contained quickly, risks to individuals are assessed consistently, and any required notifications are made on time.

2. Scope

This policy applies to all Councillors, staff, contractors, and volunteers who process personal data on behalf of the Council, including when working remotely and when using Council or personal devices for Council business.

3. Definition

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

Examples include:

- Access by an unauthorised person (inside or outside the Council).
- Sending personal data to the wrong recipient (email, post or messaging).
- Loss or theft of a device, paper file or USB drive containing personal data.
- Accidental deletion or loss of availability of personal data (e.g., no backup).
- Unauthorised alteration of personal data.
- Malware, phishing, account compromise or other cyber incident affecting personal data.

4. Roles and responsibilities

Everyone has a role in preventing and responding to breaches:

- All Councillors/staff/volunteers: take reasonable steps to protect personal data and report suspected breaches immediately.
- Clerk (Incident Lead): coordinates the response, ensures containment actions are taken, gathers facts, maintains the breach log, and supports communications.
- Data Protection Officer (DPO, at present the Clerk): advises on the risk assessment and whether notification is required; submits notifications to the ICO where required; advises on notifying individuals.
- Chair: supports governance and communications decisions (where needed) without delaying containment or statutory reporting.

5. Information security controls

The Council takes the security of personal data seriously. Appropriate measures include password protection, access controls, secure storage for paper records (locked cabinets), and use of approved systems for Council business. These controls do not eliminate risk; prompt reporting and response are essential.

6. What to do if you suspect a breach (immediate actions)

If you suspect a personal data breach, act immediately:

1. Contain: stop the breach and prevent further loss (e.g., recall an email, change passwords, disable access, secure or recover devices, retrieve mis-sent paperwork).
2. Preserve evidence: do not delete emails, logs or files. Take screenshots where helpful and note key times and actions.
3. Report internally: notify the Clerk immediately and copy/notify the DPO as soon as possible (phone first if urgent).
4. Do not contact the ICO or affected individuals directly unless instructed by the Clerk/DPO (to ensure consistent messaging and correct legal threshold decisions).

7. Risk assessment (how the Council decides what to report)

The Clerk and DPO will assess the breach to determine the likelihood and severity of any risk to individuals' rights and freedoms, including whether there is a high risk requiring communication to individuals.

Factors considered include:

- Type and sensitivity of data (e.g., special category data, financial details, safeguarding information).
- Number of individuals affected and ease of identification.
- Whether the data was protected (e.g., encryption, strong passwords, access controls).
- Potential consequences (e.g., identity theft, fraud, distress, discrimination, physical or safeguarding risk).
- Who has obtained (or could obtain) the data and the likelihood of misuse.
- Whether the breach is ongoing or likely to recur.

8. Notification duties and timescales

The Council must notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of a notifiable personal data breach. If notification is made after 72 hours, reasons for the delay must be provided.

The Council will also notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

9. What information is included in an ICO notification

When notifying the ICO, the Council will provide (as far as known at the time):

- A description of the nature of the breach, including the categories and approximate number of individuals concerned and records affected.
- The name and contact details of the DPO (or other relevant contact point).
- The likely consequences of the breach.

- The measures taken or proposed to address the breach, including steps to mitigate possible adverse effects.

10. Communicating with affected individuals

Where required, the Council will provide affected individuals with clear, plain-language information about the breach, its likely impact, and what steps they can take to protect themselves, including any support offered by the Council.

The Council may not need to communicate with individuals if:

- Appropriate technical and organisational measures (such as encryption) rendered the data unintelligible to unauthorised persons; or
- Subsequent measures ensure the high risk is no longer likely to materialise; or
- Direct communication would involve disproportionate effort (in which case a public communication may be used instead).

Even where individuals are not notified, the Council will still consider whether ICO notification is required and will always record the breach and the rationale for decisions taken.

11. Data processors and third parties

Where the Council uses a data processor (e.g., payroll provider, IT support, cloud service), the processor must notify the Council without undue delay if it becomes aware of a personal data breach. The Council remains responsible for deciding whether to notify the ICO and/or individuals. Contracts and data processing agreements should require processors to cooperate and provide the information needed to investigate and report breaches.

12. Record keeping and breach log

All personal data breaches (including near-misses) must be recorded, whether or not they are reported to the ICO or to individuals. This supports accountability, helps identify system failures, and informs improvements to security controls.

Minimum fields to record in the breach log include:

- Unique incident reference number.

- Date/time discovered and date/time the Council became aware.
- Reporter name/role and how the breach was discovered.
- Description of the incident and what data was involved.
- Categories of individuals affected and approximate numbers (where known).
- Immediate containment actions taken (what/when/by whom).
- Risk assessment summary (including factors considered).
- Decision: notified ICO? notified individuals? (yes/no) and rationale.
- Details of any notifications (dates, method, content summary).
- Recovery actions and steps to prevent recurrence.
- Lessons learned and follow-up date.

13. Review

This policy will be reviewed at least annually and after any significant breach or change in relevant law, guidance, or Council processes.