COLLINGHAM *Parish Council*

Data Protection Policy

Adopted:	26th February 2026
Next Review:	February 2027

1. Purpose

This policy explains how Collingham Parish Council (the Council) will comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 when processing personal data. It is intended to support consistent, lawful, and secure handling of personal data and to provide clear steps for responding to requests and incidents.

2. Scope

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

3. Key definitions

- Personal data: information relating to an identified or identifiable living individual (e.g., name, address, email, phone number).
- Special category personal data: data revealing racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic/biometric data, health data, sex life or sexual orientation.
- Processing: anything done with personal data (e.g., collecting, recording, storing, using, sharing, deleting).
- Controller: the organisation that decides why and how personal data is processed (the Council is the controller for its business).
- Processor: an organisation processing personal data on the Council's behalf (e.g., payroll provider, IT support, hosting).
- Data subject: the individual the personal data relates to.

4. Roles and responsibilities

Everyone has a role in protecting personal data:

- All Councillors/staff/volunteers: follow this policy, keep personal data secure, and report suspected breaches promptly.
- Clerk/Proper Officer: day-to-day lead for data protection, maintains records, supports responses to requests and incidents.
- Data Protection Officer (DPO): provides advice and oversight, supports risk assessment, and advises on ICO notifications where required.
- Chair: supports governance and decision-making where needed, without delaying legal timescales.

5. Data protection principles

The Council will process personal data in line with the UK GDPR principles:

- Lawfulness, fairness and transparency.
- Purpose limitation (use data only for specified, explicit and legitimate purposes).
- Data minimisation (only what is necessary).
- Accuracy (keep data up to date where required).
- Storage limitation (keep data only as long as necessary).
- Integrity and confidentiality (appropriate security).
- Accountability (be able to demonstrate compliance).

6. Lawful basis and special category data

The Council will identify and document a lawful basis before processing personal data. For most Council activity, the lawful basis will be “public task” (processing necessary to perform a task in the public interest or in the exercise of official authority) and/or “legal obligation” (necessary for compliance with a legal obligation). Consent will be used only where appropriate and where individuals can genuinely refuse or withdraw without detriment.

Where the Council processes special category personal data, it will identify both a UK GDPR lawful basis and an additional special category condition under the Data Protection Act 2018, and will apply enhanced safeguards.

7. Transparency and records

The Council will provide clear privacy information describing what data is collected, why it is needed, how it is used, who it is shared with, how long it is kept, and how individuals can exercise their rights. The Council will maintain appropriate documentation such as a record of processing activities and a retention schedule.

The Council will pay the ICO data protection fee where required (unless exempt) and will keep its data protection documentation up to date.

8. Individuals' rights

Individuals have rights under UK GDPR, including:

- Right to be informed (privacy information).
- Right of access (Subject Access Request).
- Right to rectification (correction of inaccurate data).
- Right to erasure (in limited circumstances).
- Right to restrict processing (in limited circumstances).
- Right to object (in limited circumstances, including direct marketing).
- Rights related to automated decision-making and profiling (where applicable).

Some rights are qualified and may not apply where the Council must process data to meet legal duties or where exemptions apply (e.g., third-party data, confidentiality, legal privilege, crime and taxation).

9. Data sharing and disclosure

The Council will share personal data only where it is lawful, necessary and proportionate, and where appropriate it will document the sharing decision. Data may be shared with other public bodies, auditors, insurers, professional advisers, and contractors where required for Council business or legal duties.

When sharing personal data, the Council will:

- Share the minimum necessary.
- Ensure appropriate safeguards and secure transfer methods are used.
- Record significant disclosures where appropriate.
- Consider confidentiality and exemptions (including where disclosure could cause harm or prejudice lawful functions).

10. Processors (suppliers handling personal data)

Where the Council uses a processor (e.g., payroll, IT support, cloud hosting), the Council will ensure there is an appropriate contract or data processing agreement setting out security requirements, confidentiality, sub-processing controls, and breach reporting obligations.

11. Retention and disposal

The Council will keep personal data only for as long as necessary for the purpose it was collected, in line with the Council's retention schedule and legal requirements (including audit and statutory retention).

Disposal will be secure and appropriate to the medium:

- Paper records: cross-cut shredding or secure confidential waste disposal.
- Electronic records: secure deletion and removal from devices and backups where feasible and appropriate.
- Devices/media: secure wiping or certified destruction.

12. Information security

The Council will take appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Measures may include access controls, strong passwords and multi-factor authentication (where available), encryption, secure storage, regular updates, and staff awareness.

Councillors and staff must take reasonable steps to keep Council data separate from personal data where possible and must not store Council personal data in insecure or unapproved locations.

13. Personal data breaches

Any suspected or actual personal data breach must be reported immediately to the Clerk/Proper Officer and the DPO and handled in line with the Council's Data Breach Policy. All breaches (including near-misses) will be recorded, and notifications to the ICO and/or individuals will be made where legally required.

14. Training and awareness

The Council will provide appropriate guidance and support to Councillors, staff, and volunteers to help them understand their responsibilities under this policy.

15. Complaints

Individuals should raise data protection queries or complaints with the Clerk/Proper Officer in the first instance. Individuals also have the right to complain to the Information Commissioner's Office (ICO).

16. Review

This policy will be reviewed at least annually and after any significant change in law, guidance, Council systems, or following any significant personal data breach.