



Ballingham Bolstone and Hentland Group Parish Council

Data Protection Policy

Adopted by Council: 16th April 2026

1. Purpose of this Policy

Ballingham Bolstone and Hentland Group Parish Council (“the Council”) is committed to protecting the privacy and personal data of councillors, employees, volunteers, contractors, residents, and all individuals whose information it processes.

This policy sets out how the Council complies with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and associated data protection legislation.

The Council recognises that personal information must be collected, used, stored, shared and disposed of responsibly and securely.

2. Scope

This policy applies to all personal data processed by the Council, whether held electronically or in paper format.

It applies to:

- Councillors;
- Employees and contractors;
- Volunteers;
- Residents and members of the public;
- Suppliers and service providers;
- Users of Council facilities or services;
- Any other individuals whose personal information is processed by the Council.

All councillors, employees and others acting on behalf of the Council are responsible for complying with this policy.

3. Data Protection Principles

The Council will comply with the following principles when processing personal data:

Lawfulness, fairness and transparency



Personal data will only be processed where there is a lawful basis to do so, and individuals will be informed how their information is used.

Purpose limitation

Personal data will only be collected and used for specified, explicit and legitimate purposes.

Data minimisation

The Council will only collect information that is necessary and relevant.

Accuracy

The Council will take reasonable steps to ensure personal information is accurate and kept up to date.

Storage limitation

Personal data will not be kept longer than necessary and will be disposed of securely.

Integrity and confidentiality

Personal data will be protected against unauthorised access, loss, damage or disclosure.

Accountability

The Council will maintain appropriate records and procedures to demonstrate compliance.

4. Responsibilities

The Parish Council

The Council is the Data Controller and is responsible for ensuring that personal data is processed lawfully and securely.

Parish Clerk / Data Protection Lead

The Clerk will:

- oversee day-to-day compliance with this policy;
- maintain relevant records and procedures;
- ensure appropriate security measures are in place;
- advise councillors and staff on data protection matters;
- manage data protection requests and incidents.
-



Data Protection Officer

The Council appointed a Data Protection Officer (DPO) and published their contact details on Website - 16th April 2026.

Councillors, Employees and Volunteers

Anyone handling personal data on behalf of the Council must:

- keep information confidential;
- only access information needed for their role;
- follow Council procedures;
- report suspected breaches promptly.

5. Personal Data Processed by the Council

The Council may process personal data including:

- names and contact details;
- correspondence and enquiries;
- council employee records;
- payroll and HR information;
- allotment records;
- cemetery records;
- grant applications;
- bookings and service requests;
- supplier and contractor information;
- website and communications information.

The Council will only process special category data (such as health information) where there is a lawful reason to do so, and appropriate safeguards are in place.

6. Lawful Basis for Processing

The Council will process personal data only where a lawful basis applies, including:

- legal obligation;
- public task;
- legitimate interests;
- contractual necessity;
- consent where appropriate.

The Council will record the lawful basis for significant processing activities.



7. Privacy Information

The Council will provide clear privacy notices explaining:

- what personal data is collected;
- why it is collected;
- the lawful basis for processing;
- who information may be shared with;
- how long information is retained;
- individuals' rights.

Privacy notices will be made available through appropriate channels, including the Council website where applicable.

8. Information Security

The Council will take appropriate technical and organisational measures to protect personal data.

These measures may include:

- secure passwords;
- restricted access to confidential information;
- secure storage of paper records;
- appropriate use of email;
- protection of Council devices;
- secure disposal of confidential documents;
- ensuring suppliers use appropriate safeguards.

Councillors and staff must not share confidential Council information through insecure methods.

9. Data Retention and Disposal

The Council will retain information only for as long as necessary or as required by law.

A retention schedule will be maintained setting out appropriate retention periods for different categories of records.

When records are no longer required, they will be securely destroyed or deleted.

10. Data Sharing

The Council may share personal data where:

- there is a legal requirement;



- it is necessary to provide a service;
- there is a legitimate reason to do so;
- appropriate safeguards are in place.

The Council will ensure that any third-party processing personal data on its behalf has appropriate contractual arrangements and security measures.

11. Individual Rights

Individuals have rights under data protection legislation, including:

- the right to be informed;
- the right of access to their personal data;
- the right to request correction of inaccurate information;
- the right to request deletion where applicable;
- the right to restrict processing;
- the right to object to certain processing;
- rights relating to automated decision-making where applicable.

Requests will be handled in accordance with legal requirements.

12. Subject Access Requests

Individuals may request access to personal information held about them.

The Council will:

- verify the identity of the requester;
- respond within the statutory timescale;
- provide information unless an exemption applies.

Requests should be submitted to the Parish Clerk.

13. Data Breaches

A personal data breach includes the accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data.

All suspected breaches must be reported immediately to the Parish Clerk.

The Council will:

- record and assess the breach;
- take steps to reduce any risk;
- notify the Information Commissioner's Office (ICO) where required;
- notify affected individuals where appropriate;
- review procedures to prevent recurrence.



14. Data Protection Impact Assessments

The Council will carry out a Data Protection Impact Assessment (DPIA) where proposed processing is likely to result in a high risk to individuals' rights and freedoms.

15. Records Management

The Council will maintain appropriate records of its data processing activities and ensure that records are:

- accurate;
- accessible to authorised persons;
- securely stored;
- retained appropriately;
- disposed of safely.

16. Training and Awareness

The Council will ensure that councillors, employees and volunteers who handle personal data understand their responsibilities.

Training and guidance will be provided where appropriate.

17. Complaints

Anyone who believes the Council has not handled their personal data appropriately should contact the Parish Clerk.

Individuals also have the right to complain to the Information Commissioner's Office (ICO).

18. Policy Review

This policy will be reviewed at least annually, or sooner if there are changes to legislation, Council procedures, or working practices.