Bishop Middleham Parish Council

Data Protection Policy

DOCUMENT CONTROL	
Version Number	V1-2026
Adopted on	8th April 2026
Reviewed	
Next Review	April 2028

Applies to: All Councillors, the Clerk/RFO, volunteers, contractors, and anyone processing personal data on behalf of the Council

1. Purpose of this Policy

Bishop Middleham Parish Council is committed to protecting the privacy and security of personal data. This policy explains how the Council complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all relevant data protection legislation. It applies to all personal data processed by the Council in the course of its duties, including data relating to residents, volunteers, garage tenants, event attendees, consultation participants, website users, contractors, councillors, and staff (except where covered by the separate HR Data Protection Policy).

2. Scope

This policy covers all personal data processed by the Council in any format: electronic files, emails, cloud-stored data, paper records, website submissions, photographs or media, and consultation responses. It applies to all councillors, the Clerk, volunteers, and contractors acting on behalf of the Council.

3. Data Protection Principles

The Council complies with the seven principles of the UK GDPR. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- kept for no longer than necessary;
- processed securely;
- and the Council is responsible for demonstrating compliance.

4. Lawful Bases for Processing

The Council relies on Public Task, Legal Obligation, Contract, Consent, and Legitimate Interests where appropriate. Special category data is processed only where strictly necessary and subject to additional safeguards.

5. Personal Data the Council Processes

The Council processes data relating to residents, website users, contractors, councillors, and staff. This includes contact details, correspondence, consultation responses, event registrations, volunteer details, garage tenancy information, invoices, and website analytics. The Council does not operate allotments, cemeteries, or CCTV.

6. How Personal Data is Stored

Data is stored on the Clerk's password-protected laptop, OneDrive cloud storage, email accounts hosted by Franklin Web/A2 Hosting, and paper files kept in locked storage. Only the Clerk has full access. Councillors access correspondence only. Contractors access only the data required to perform their function.

7. Data Security

The Council uses appropriate technical and organisational measures including password protection, encryption, secure cloud storage, locked filing cabinets, restricted access, secure email practices, and antivirus protection. Volunteers and contractors receive guidance where relevant.

8. Data Sharing

The Council shares personal data only where necessary and lawful, including with Durham County Council (payroll), website host (Franklin Web/A2 Hosting), auditors, HMRC, and event partners (where consent is obtained). All processors must comply with UK GDPR.

9. Data Retention and Disposal

The Council follows its adopted Document Disposal and Retention Policy. Personal data is kept only for as long as necessary and then securely destroyed by shredding or secure deletion.

10. Data Subject Rights

Individuals have the right to access their personal data, request rectification or erasure, restrict processing, object to processing, withdraw consent, and complain to the ICO. Requests must be submitted to the Clerk. The Council responds within one month.

11. Data Breaches

A breach must be reported immediately to the Clerk. The Clerk will assess the breach, record it, notify the ICO within 72 hours if required, and notify affected individuals where there is a high risk.

12. Data Protection Impact Assessments (DPIAs)

The Council will carry out DPIAs for any processing that may pose a high risk, such as new technologies or large-scale data collection.

13. Privacy Notices

The Council maintains a clear Privacy Notice covering what data is collected, why it is collected, lawful bases, retention periods, and rights of individuals. Additional notices may be issued for events, consultations, or volunteer activities.

14. Councillor and Volunteer Responsibilities

Councillors and volunteers must use council-approved email accounts, keep information secure, not disclose personal data without authority, report concerns immediately, and follow this policy.

15. Use of Messaging Applications (WhatsApp)

The Council has adopted WhatsApp as an official communication tool for internal discussions. WhatsApp may be used for informal conversations relating to agenda

items; however, it must not be used for decision-making or for the sharing of confidential, sensitive, or personal data. Councillors must ensure that any device used to access WhatsApp is secured with a password or biometric lock.

For security purposes, general discussion messages are automatically cleared every 90 days.

Notwithstanding this automatic deletion, WhatsApp messages relating to council business **may fall within the scope of the Freedom of Information Act (FOIA)**. Councillors must therefore forward any WhatsApp messages relevant to a valid FOI request to the Clerk upon request.

The Council's official communication channel for all formal correspondence and decision-related matters remains the council email system.

16. Review

This policy will be reviewed every two years or sooner if legislation or Council activities change.