Bishop Middleham Parish Council

HR Data Protection Policy

DOCUMENT CONTROL	
Version Number	V1 – 2026
Adopted on	11th March 2026
Reviewed	
Next Review	March 2028

Purpose

Bishop Middleham Parish Council is committed to being transparent about how it collects and uses the personal data of staff and to meeting its data protection obligations. This policy sets out the Council's commitment to data protection, and the rights and obligations of individuals in relation to personal data, in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to the personal data of current and former job applicants, employees, workers, contractors, and former employees (HR-related personal data). It does not apply to personal data relating to members of the public or data processed for wider council business.

The Council has appointed a Data Protection Lead responsible for overseeing compliance. Questions about this policy should be directed to the Clerk.

Definitions

Personal data: Information relating to an identifiable living individual.

Processing: Any operation performed on personal data, including collecting, storing, amending, disclosing, or deleting it.

Special category data: Sensitive data requiring additional protection, including health, ethnicity, political opinions, religious beliefs, trade union membership, sexual orientation, and biometric/genetic data.

Criminal offence data: Information relating to criminal convictions, allegations, or proceedings.

Data Protection Principles

The Council processes HR-related personal data in accordance with the UK GDPR principles. 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 only for as long as necessary.
- Processed securely.

The Council is responsible for demonstrating compliance (accountability).

Processing Personal Data

The Council processes personal data on the following lawful bases:

- **Contract**: necessary for employment or engagement.
- **Legal obligation**: compliance with employment, tax, or audit law.
- **Legitimate interests**: where processing is necessary and does not override individual rights.
- **Vital interests**: to protect life.
- **Public task**: where processing is necessary for official functions.

Where none of the above apply, consent will be sought. Consent can be withdrawn at any time.

Personal data is stored securely in personnel files, HR systems, and Council IT systems. Retention periods are set out in the Council's retention schedule.

The Council may share personal data with third-party processors (e.g., payroll providers). Such processors must comply with UK GDPR and act only on the Council's instructions.

Special Category Data

The Council processes special category data only where permitted by law, including:

- Employment law obligations.
- Vital interests.
- Data made public by the individual
- Legal claims.
- Occupational health purposes.
- Substantial public interest conditions under the DPA 2018.

Where required, explicit consent will be obtained.

Individual Rights

Individuals have the right to:

- Access their personal data (Subject Access Request).
- Rectify inaccurate data.
- Erase data in certain circumstances.
- Restrict or object to processing.
- Data portability (where applicable).
- Complain to the Information Commissioner's Office (ICO).

Subject Access Requests must be submitted to the Clerk. The Council will respond within one month unless an extension is justified.

Data Security

The Council takes data security seriously and uses technical and organisational measures including:

- Password protection and encryption.
- Secure storage for paper records.
- Access controls.
- Secure disposal of data.

Third-party processors must implement appropriate security measures.

Data Breaches

All data breaches must be reported immediately to the Clerk.

The Council will assess the breach and, where required, report it to the ICO within 72 hours. Individuals will be notified where there is a high risk to their rights and freedoms.

International Transfers

The Council will not transfer HR-related personal data outside the UK unless appropriate safeguards are in place in accordance with UK GDPR.

Individual Responsibilities

All staff, councillors, and contractors handling HR-related personal data must:

- Access only authorised data.
- Keep data secure.
- Not disclose data without authorisation.
- Use secure systems and devices.
- Report concerns or breaches immediately.

Training

The Council will provide training to ensure individuals understand their responsibilities under this policy.

Review

This policy will be reviewed regularly and updated as required to reflect changes in legislation or Council operations.