Data Protection Policy V1

1. Introduction

This policy sets out how Great Bedwyn Parish Council complies with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The Council is committed to protecting the personal data of residents, councillors, employees, and other individuals.

This policy applies to all personal data processed by the Council, regardless of the format in which it is held.

2. Scope

This policy applies to:

- All elected and co-opted councillors
- All employees and volunteers
- All contractors and third parties processing data on behalf of the Council
- All personal data held by the Council in any format

3. Key Definitions

Personal Data: Information relating to an identifiable living individual.

Special Category Data: Sensitive personal data including racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

Data Controller: The Parish Council, which determines the purposes and means of processing personal data.

Data Processor: Any person or organisation that processes personal data on behalf of the Council.

Data Subject: The individual to whom the personal data relates.

Processing: Any operation performed on personal data, including collection, storage, use, disclosure, or deletion.

4. Data Protection Principles

The Council will ensure that all personal data is:

1. **Processed lawfully, fairly and transparently**
2. **Collected for specified, explicit and legitimate purposes**
3. **Adequate, relevant and limited to what is necessary**
4. **Accurate and kept up to date**
5. **Kept for no longer than necessary**
6. **Processed securely with appropriate technical and organisational measures**

The Council will be accountable for compliance with these principles.

5. Lawful Basis for Processing

The Council will identify a lawful basis for all processing activities. Common lawful bases include:

- **Legal obligation:** Processing necessary to comply with statutory duties
- **Public task:** Processing necessary to perform functions as a public authority
- **Consent:** Where freely given, specific, informed and unambiguous
- **Legitimate interests:** Where necessary for the Council's legitimate interests (balanced against individual rights)

6. Types of Data Processed

The Council processes personal data including:

- Names, addresses, telephone numbers and email addresses
- Financial information for payments and invoicing
- Employment records
- Correspondence and communications with residents
- CCTV footage
- Planning application comments
- Electoral register information
- Information about complaints and grievances

7. Individual Rights

Data subjects have the following rights:

- **Right to be informed** about data processing
- **Right of access** to their personal data (Subject Access Request)
- **Right to rectification** of inaccurate data
- **Right to erasure** in certain circumstances
- **Right to restrict processing** in certain circumstances
- **Right to data portability** where applicable
- **Right to object** to processing in certain circumstances
- **Rights related to automated decision making** (where applicable)

All requests will be responded to within one month, which may be extended by two further months where requests are complex.

8. Subject Access Requests (SARs)

Individuals may request access to their personal data. The Council will:

- Verify the identity of the requester
- Respond within one month (extendable to three months for complex requests)
- Provide information free of charge (unless requests are manifestly unfounded or excessive)
- Explain any exemptions applied

SARs should be directed to the Clerk, who will coordinate the response.

9. Data Security
The Council will implement appropriate technical and organisational measures including:
- Secure storage of paper records in locked cabinets
- Password protection for electronic files and devices
- Encryption of sensitive data
- Regular backups of electronic data
- Secure disposal of confidential waste (shredding)
- Clear desk and clear screen policies
- Access controls limiting data access to authorised personnel only
- Regular security reviews and updates
- The councils IT policy should be considered as part of data security.

10. Data Retention
Personal data will be retained only for as long as necessary. The Council will maintain a retention schedule specifying retention periods for different categories of data, based on legal requirements and operational needs.

The council's data retention document should be referenced for how long the council keeps its data.

11. Data Sharing
The Council may share personal data with:
- Other local authorities and public bodies
- Legal and professional advisors
- Contractors and service providers (under appropriate agreements)
- Law enforcement agencies where required

Data will only be shared where there is a lawful basis and, where applicable, data processing agreements will be in place.

12. Privacy Notices
A privacy notice is published on the Council website and will be provided directly where appropriate.

13. Data Breaches
A personal data breach is any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
In the event of a breach, the Council will:
1. Contain and assess the breach
2. Notify the Information Commissioner's Office (ICO) within 72 hours if the breach poses a risk to individuals' rights and freedoms
3. Notify affected individuals without undue delay if there is a high risk to their rights and freedoms
4. Document all breaches and actions taken
5. Review procedures to prevent future breaches

All suspected breaches must be reported immediately to the Clerk.

14. Accountability and Governance

Responsible Officer: The Clerk is responsible for day-to-day data protection compliance and acts as the primary contact for data protection matters.
Training and bulletins All councillors, staff and volunteers will receive appropriate data protection training and bulletins.
Records: The Council will maintain a Record of Processing Activities which is held on the councils website as part of the Privacy Statement.
Audits: Regular audits will be conducted to ensure compliance with this policy.

15. Third Party Processors

When engaging third parties to process personal data on the Council's behalf, the Council will:

- Conduct due diligence to ensure the processor can provide sufficient guarantees
- Establish a written data processing agreement
- Ensure the processor processes data only on documented instructions
- Monitor the processor's compliance

16. Publication of Information

The Council publishes certain information as part of its transparency obligations. Care will be taken to:

- Redact personal data from published documents where appropriate
- Balance transparency with data protection obligations
- Consider whether publication serves a legitimate purpose
- Apply exemptions appropriately (e.g., for information already in the public domain)

Minutes, agendas and financial information may be published with personal data redacted as necessary.

17. Complaints

Complaints about data protection should be directed to the Clerk in the first instance. If dissatisfied with the Council's response, individuals may complain to:

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Website: www.ico.org.uk

18. Policy Review

This policy will be reviewed every 2 years or following:

- Changes to data protection legislation
- Changes to the Council's data processing activities
- A significant data breach
- Guidance from the ICO

V1 approved February 2026 Full Council meeting.

Date: 8.1.26
Minute ref: 1091.25.19

Review date Jan 2028.