Hatfield Peverel Parish Council – Data Protection Policy (Updated 2026)

1. Introduction

Hatfield Peverel Parish Council ("the Council") is committed to protecting the rights and freedoms of individuals in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines how the Council collects, uses, stores and protects personal data.

2. Scope

This policy applies to all personal data processed by the Council, including data relating to residents, employees, contractors, volunteers, and other individuals who interact with the Council.

3. Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person.
- **Special Category Data**: Sensitive personal data including racial or ethnic origin, political opinions, religious beliefs, health data, etc.
- **Processing**: Any operation performed on personal data, including collection, storage, use, and deletion.
- **Data Subject**: An individual whose personal data is processed.
- **Data Controller**: The organisation that determines the purposes and means of processing personal data.
- **Data Processor**: A third party that processes personal data on behalf of the controller.

4. Roles and Responsibilities

The Council is the Data Controller and is responsible for ensuring compliance with data protection laws. All staff and councillors must adhere to this policy and undertake relevant training.

5. Lawful Bases for Processing

The Council processes personal data under one or more of the lawful bases defined in Article 6 of the UK GDPR, including:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task
- Legitimate interests (where applicable)

6. Data Protection Principles (UK GDPR Article 5)

The Council adheres to the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

7. Data Subject Rights

Data subjects have the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making and profiling

8. Consent

Consent must be freely given, specific, informed and unambiguous. The Council will ensure that consent is obtained where required and that individuals can withdraw consent at any time.

9. Data Collection and Use

The Council collects personal data only for specified, explicit and legitimate purposes. Individuals will be informed of the purpose at the time of collection. Data will be used only for the stated purposes and retained only as long as necessary.

10. Data Sharing and Disclosure

Personal data may be shared with third parties only where lawful and necessary. The Council will ensure appropriate data sharing agreements are in place and that data subjects are informed of such disclosures unless legally exempted.

11. Data Security

The Council implements appropriate technical and organisational measures to ensure data security, including:

- Secure storage systems
- Access controls
- Staff training
- Regular audits and reviews

12. Data Retention and Disposal

Personal data will be retained only as long as necessary for the purpose for which it was collected. The Council follows its Data Retention Policy and ensures secure disposal of data when no longer required.

13. Data Breaches

In the event of a personal data breach, the Council will assess the risk to individuals and report to the Information Commissioner's Office (ICO) within 72 hours if required. Affected individuals will be informed where there is a high risk to their rights and freedoms.

14. Subject Access Requests (SARs)

Individuals have the right to access their personal data. Requests must be responded to within one month. The Council will verify the identity of the requester before disclosing any information.

15. Data Protection Impact Assessments (DPIAs)

DPIAs will be conducted for high-risk processing activities to assess and mitigate potential risks to data subjects.

16. International Transfers

Personal data will not be transferred outside the UK unless appropriate safeguards are in place in accordance with UK GDPR requirements.

17. Policy Review

This policy will be reviewed annually or when there are significant changes to data protection legislation or Council practices. Last reviewed: May 2026.

18. Glossary

- **ICO**: Information Commissioner's Office – the UK’s independent authority for data protection.
- **UK GDPR**: United Kingdom General Data Protection Regulation.
- **SAR**: Subject Access Request.
- **DPIA**: Data Protection Impact Assessment.