Marsham Parish Council

Data Protection Policy

1. Introduction
This Data Protection Policy sets out how Marsham Parish Council ("the Council") collects, uses, stores, shares, and protects personal data. The Council is committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all other relevant legislation.

The Council is a data controller and is responsible for ensuring that personal data is processed lawfully, fairly, and transparently.

2. Purpose of the Policy
The purpose of this policy is to:
- Protect the rights and privacy of individuals whose data is held by the Council.
- Ensure compliance with data protection law.
- Establish clear responsibilities for councillors, employees, volunteers, and contractors.
- Provide transparency on how personal data is handled.

3. Scope
This policy applies to:
- All councillors and employees of the Council.
- Any volunteers, contractors, or third parties working on behalf of the Council.
- All personal data that the Council processes in any format, including electronic, paper, audio, and visual records.

4. What Is Personal Data?
Personal data is any information relating to an identified or identifiable individual. Examples include:
- Names, addresses, email addresses, and phone numbers
- Photographs and CCTV images
- Bank details
- Correspondence from residents
- Employment-related information

Special category data (e.g., health information, political opinions, religious beliefs) requires additional protection.

5. Data Protection Principles
The Council will ensure that personal data is:
1. **Processed lawfully, fairly, and transparently**
2. **Collected for specific, explicit, and legitimate purposes**
3. **Adequate, relevant, and limited to what is necessary**
4. **Accurate and kept up to date**
5. **Kept only for as long as necessary**
6. **Processed securely**

6. Lawful Bases for Processing

The Council will process personal data only where at least one lawful basis applies, including:

- **Public task** (for carrying out statutory duties and functions)
- **Legal obligation**
- **Contract**
- **Consent** (for activities not covered by statutory functions)
- **Legitimate interests** (only where appropriate for non-statutory activities)

Special category data will be processed only under additional lawful conditions.

7. Rights of Individuals

Individuals have the following rights regarding their personal data:

- Right to be informed
- Right of access (Subject Access Request)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision-making

Requests will be responded to within **one month** unless an extension is permitted by law.

8. Data Collection and Use

The Council collects and uses personal data for purposes including:

- Managing Council meetings, public consultations, and statutory notices
- Responding to enquiries from residents
- Administering finances, grants, contracts, and assets
- Maintaining employment and personnel records
- Operating CCTV, websites, and mailing lists

Personal data will be used only for the purpose for which it was collected unless another lawful basis applies.

9. Data Sharing

The Council may share personal data with:

- Government bodies (e.g., HMRC, ICO)
- Service providers or contractors acting on behalf of the Council
- Law enforcement agencies (where legally required)

Data will never be sold to third parties.
Data sharing agreements will be in place where appropriate.

10. Data Retention

Personal data will be kept only for as long as necessary. A separate Retention List sets out specific retention periods.

11. Data Security

The Council will implement appropriate technical and organisational measures to protect data, including:

- Secure email and password protection
- Locked filing cabinets for paper records

- Restricted access to systems and data
- Regular backups
- Encryption where appropriate
- Secure disposal of data

Councillors and staff must ensure personal devices used for Council work are password-protected.

12. Data Breaches

A data breach includes loss, theft, unauthorised access, disclosure, or destruction of personal data. All breaches must be reported to the Clerk immediately. Where a breach poses a risk to individuals, the Council will notify the ICO within 72 hours and inform affected individuals as required.

13. Data Protection Officer (DPO)

The Council appoints the Clerk as DPO.
The DPO will:

- Monitor compliance with data protection law
- Advise on data protection matters
- Assist with data breaches, Subject Access Requests, and impact assessments

14. Training and Awareness

Councillors, employees, and volunteers will receive appropriate training on:

- Data protection responsibilities
- Secure data handling
- Recognising and reporting data breaches

15. Review of Policy

This policy will be reviewed annually every 2 years or sooner if legislation or operational processes change.

Adopted 12 January 2025
For review January 2027