

Marbury and District Parish Council

IT, Data Protection & Freedom of Information Policy

Adopted by Full Council: 19 May 2026

Review Date: May 2029 (or sooner if required by changes in legislation or Council procedures)

1. Purpose

This policy sets out how **Marbury and District Parish Council** manages:

- Information Technology (IT) systems;
- personal data protection;
- Freedom of Information (FOI) requests;
- records management and information security.

The Council is committed to openness, transparency and accountability whilst ensuring that personal information is processed lawfully, securely and in accordance with data protection legislation.

2. Legal Framework

The Council complies with the requirements of:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004 (where applicable);
- Computer Misuse Act 1990; and
- Local Government Act 1972 (where applicable).

3. Data Protection Principles

The Council will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- stored securely and protected against unauthorised access or loss;

- retained only for as long as necessary; and
- disposed of securely when no longer required.

4. Roles and Responsibilities

Parish Council (Data Controller)

Marbury and District Parish Council is the **Data Controller** for the personal information it processes in carrying out its statutory functions.

Parish Clerk (Responsible Officer)

The Clerk is responsible for:

- administering the Council's data protection arrangements;
- maintaining secure Council records;
- responding to Subject Access Requests (SARs);
- coordinating responses to Freedom of Information requests;
- ensuring compliance with UK GDPR and data protection legislation;
- maintaining secure storage and appropriate backups of Council records; and
- reporting any data breaches in accordance with this policy.

Councillors

Councillors:

- may access Council information only where necessary for Council business;
- must maintain the confidentiality of personal information;
- must not store Council data on personal devices unless appropriate security measures are in place;
- must comply with data protection legislation and this policy; and
- must report any actual or suspected data breaches to the Clerk immediately.

5. Data Security and IT Systems

The Council seeks to protect its information through appropriate technical and organisational measures, including:

- password-protected devices used for Council business;
- secure cloud storage approved for Council use (such as Google Drive or an equivalent secure service);
- restricted access to Council records;

- regular backup of Council data;
- use of secure email accounts for Council business;
- appropriate anti-virus and software updates where applicable; and
- ensuring sensitive information is not stored on unsecured devices.

6. Personal Data Handling

The Council may process personal data relating to:

- Councillors;
- employees (including the Clerk);
- contractors and suppliers;
- residents;
- members of the public who contact the Council; and
- individuals involved in Council consultations, services or statutory functions.

Personal data will only be used for legitimate Council purposes and will not be shared unless required or permitted by law.

7. Data Breach Procedure

In the event of a personal data breach:

- the Clerk will assess the breach as soon as practicable;
- immediate action will be taken to minimise any risks;
- the Information Commissioner's Office (ICO) will be notified where the breach meets the reporting threshold under UK GDPR;
- affected individuals will be informed where legally required; and
- the breach and any corrective actions will be recorded.

8. Data Retention

The Council retains records only for as long as necessary and in accordance with statutory requirements and its Document Retention Policy.

Examples include:

- financial records in accordance with statutory retention periods;
- minutes and agendas as permanent records;

- correspondence where required for Council business; and
- personal data only for as long as necessary for the purpose for which it was collected.

Records will be securely destroyed when no longer required.

9. Freedom of Information (FOI)

9.1 Right of Access

Under the Freedom of Information Act 2000, any person has the right to request recorded information held by the Council, subject to any applicable exemptions.

9.2 Publication Scheme

The Council will proactively publish information including:

- agendas and approved minutes;
- financial information;
- policies and procedures;
- governance documents; and
- other information required by the Information Commissioner's Office Publication Scheme.

9.3 Handling FOI Requests

- Requests will normally be responded to within 20 working days.
- Information will be provided unless an exemption applies under the Freedom of Information Act 2000.
- Personal data will be withheld where disclosure would breach the UK GDPR or where another exemption applies.
- The Clerk is responsible for coordinating responses.

9.4 Refusals and Exemptions

Information may be withheld where:

- it contains personal information protected by Section 40 of the Freedom of Information Act 2000;
- it is commercially sensitive;
- disclosure would breach legal obligations; or
- another statutory exemption applies.

10. Subject Access Requests (SARs)

Individuals have the right to request:

- confirmation that the Council holds their personal data;
- access to copies of their personal data;
- correction of inaccurate or incomplete personal data, where appropriate.

Subject Access Requests will:

- normally be responded to within one month, unless an extension is permitted by law;
- be processed securely;
- require proof of identity where appropriate; and
- ensure that third-party personal information is redacted where necessary.

11. Website Privacy

The Council publishes a Privacy Notice explaining how personal information is collected, used, stored and protected. The Privacy Notice is available on the Council's website and will be reviewed periodically to ensure it remains accurate and compliant with current legislation.

12. Training

The Council recognises the importance of maintaining awareness of information governance responsibilities. Councillors and the Clerk will receive appropriate guidance or training on data protection, information security and Freedom of Information requirements where necessary.

13. Policy Review

This policy will be reviewed at least every three years, or sooner if there are significant changes to legislation, guidance issued by the Information Commissioner's Office (ICO), or the Council's working practices.