Marbury and District Parish Council

IT, Data Protection & Freedom of Information Policy

Adopted by Full Council on *** May 2026

This Policy was adopted by Marbury and District Parish Council at its meeting held on *** May 2026

Marbury and District Parish Council

IT, Data Protection & Freedom of Information Policy

1. Purpose

This policy sets out how Cholmondeley & Chorley Parish Council manages:

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

The Council is committed to transparency, lawful data processing, and protecting the privacy of individuals.

2. Legal Framework

The Council complies with the following legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004 (where applicable)

3. Data Protection Principles

The Council ensures that all personal data is:

- processed lawfully, fairly and transparently
- collected for specified and legitimate purposes
- adequate, relevant and limited to what is necessary

- accurate and kept up to date
- stored securely
- retained only as long as necessary

4. Roles and Responsibilities

Parish Clerk (Data Controller Function)

The Clerk is responsible for:

- day-to-day handling of personal data
- maintaining secure records
- responding to Subject Access Requests (SARs)
- ensuring compliance with UK GDPR
- managing FOI requests
- secure storage and backups of Council records

Councillors

Councillors:

- may access Council data only for Council business
- must respect confidentiality of personal information
- must not store Council data on personal devices without security controls
- must comply with GDPR principles

5. Data Security & IT Systems

The Council ensures data security through:

- password-protected devices used by the Clerk
- secure cloud storage (e.g. Google Drive or equivalent)
- restricted access to Council files
- regular backup of Council data
- use of secure email for Council business
- no storage of sensitive data on unsecured personal devices

6. Personal Data Handling

The Council may hold personal data relating to:

- Councillors
- employees (including Clerk)
- contractors and suppliers
- members of the public contacting the Council

Data is only used for legitimate Council business and is not shared unless required by law.

7. Data Breach Procedure

In the event of a data breach:

- the Clerk will assess the risk immediately
- steps will be taken to secure systems
- the ICO will be notified if legally required
- affected individuals will be informed where necessary
- the incident will be recorded

8. Data Retention

The Council retains records only for as long as necessary, including:

- financial records (minimum statutory retention periods)
- minutes and agendas (permanent record)
- correspondence (as required for Council business)
- personal data (only while relevant to Council function)

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.

9.2 Publication Scheme

The Council will proactively publish:

- minutes and agendas
- financial information
- policies and procedures
- governance documents

9.3 Handling FOI Requests

- Requests will be responded to within 20 working days
- Information will be provided unless exempt under FOI legislation
- Personal data will be withheld where required under UK GDPR exemptions
- The Clerk is responsible for coordinating responses

9.4 Refusals & Exemptions

Information may be withheld where:

- it contains personal data (Section 40 exemption)
- it is commercially sensitive
- disclosure would breach legal obligations

10. Subject Access Requests (SARs)

Individuals have the right to request:

- copies of personal data held about them
- correction of inaccurate data

Requests will be:

- responded to within 1 month (unless extended under law)
- processed securely
- redacted where third-party data is involved

11. Email, Devices & Communication

- Council business should be conducted using secure email accounts
- Emails containing personal data must not be forwarded unnecessarily
- Councillors should avoid storing Council data on unsecured personal devices
- Confidential information must not be shared outside Council business

12. Transparency & FOI Compliance

The Council is committed to openness and transparency.
However, this is balanced with:

- protection of personal data
- safeguarding confidential information
- compliance with UK GDPR exemptions

13. Review of Policy

This policy is reviewed annually or when:

- legislation changes
- ICO guidance is updated
- Council processes change

Audit Statement

The Council complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Freedom of Information Act 2000. The Clerk is responsible for data protection compliance, FOI responses, and secure handling of Council information. Data is stored securely using password-protected systems and cloud storage. FOI requests are processed within statutory time limits and subject to lawful exemptions. The Council maintains proportional IT and data protection controls appropriate to its size and resources.