FRATING PARISH COUNCIL

Memorial Hall, Main Road, Frating, CO7 7DJ.
Clerk to the Council: Kay English
Email: clerk@fratingparishcouncil.gov.uk
Website: www.fratingparishcouncil.gov.uk

DATA PROTECTION POLICY

Reviewed: Full Council 1st June 2026
Next Review Date: June 2027

1. Introduction
This Data Protection Policy sets out how Frating Parish Council (FPC) collects, uses, stores, shares, and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Council is committed to ensuring that personal data is processed lawfully, fairly, transparently, and securely.

2. Scope
This policy applies to:
- All councillors
- The Clerk and any other employees
- Volunteers, contractors, and third-party processors acting on behalf of the Council

All personal data processed by the Council in any format (paper, electronic, audio, photographic)

3. Definitions
Personal Data
Any information relating to an identified or identifiable individual (e.g., name, address, email, IP address, opinions about a person).
Special Category Data
Sensitive data requiring additional protection (e.g., health information, political opinions, religious beliefs).

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

Data Subject
The individual whose personal data is being processed.

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

Data Processor
Any third party that processes personal data on behalf of the Council (e.g., payroll provider, website host).

Data Breach
A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. Data Protection Principles
The Council adheres to the seven principles of the UK GDPR:

1. Lawfulness, Fairness and Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality (Security)
7. Accountability

(See Appendix A for full explanation.)

5. Lawful Bases for Processing
The Council processes personal data under one or more of the following lawful bases:

- Public Task – performing a function in the public interest or exercising official authority
- Legal Obligation – compliance with statutory duties
- Contract – fulfilling a contract with an individual
- Consent – freely given, specific, informed, and unambiguous
- Legitimate Interests – where appropriate and balanced

Special category data is processed only under permitted conditions.

6. Roles and Responsibilities
The Parish Council (as Data Controller)

- Ensures compliance with data protection law
- Approves policies and oversees governance
- Ensures appropriate contracts with data processors

The Clerk

- Acts as the Council's primary data protection contact (unless a Data Protection Officer is formally appointed)
- Maintains records, retention schedules, and privacy notices
- Manages subject access requests and data breaches
- Ensures councillors receive appropriate guidance

Councillors

- Handle personal data only for legitimate council business
- Follow this policy and related procedures
- Keep devices secure and avoid using personal accounts for council work

Third-Party Processors

- Must comply with written data processing agreements
- Must implement appropriate security measures

7. Privacy Notices
The Council provides clear privacy notices explaining:

- What data is collected

- Why it is collected
- How long it is kept
- Who it may be shared with
- How individuals can exercise their rights

Privacy notices are published on the Council's website.

8. Data Subject Rights

The Council upholds the following rights:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability (where applicable)
- Right to object
- Rights related to automated decision-making (not used by the Council)

Requests are acknowledged within 10 working days and completed within one month unless an extension is justified.

9. Data Sharing and Third-Party Processing

The Council shares personal data only when:

- Required by law
- Necessary for statutory functions
- Covered by a written data processing agreement

Examples include:

- Payroll services
- Website hosting
- Internal and external auditors
- HMRC and pension providers

10. Records Management, Retention and Secure Disposal

The Council:

- Maintains a Records Retention Schedule (Appendix B)
- Stores data securely in locked cabinets or password-protected systems
- Restricts access to authorised personnel
- Reviews records regularly
- Disposes of data securely using:
- Cross-cut shredding
- Secure digital deletion
- Certified disposal for IT equipment

Historic records are transferred to the County Record Office where appropriate.

11. Data Security

Security measures include:

- Strong passwords and two-factor authentication where available
- Encrypted storage for sensitive data
- Regular backups
- Secure email practices
- Avoiding use of personal devices for council business unless protected
- Locking paper files away when not in use

12. Data Breach Procedure

A data breach must be reported immediately to the Clerk.

The Clerk will:

1. Assess the breach
2. Contain and mitigate risks
3. Record the incident in the Breach Log
4. Notify the ICO within 72 hours if the breach risks individuals' rights
5. Inform affected individuals where necessary

13. Training and Awareness

Councillors and staff receive periodic guidance on:

- Handling personal data
- Recognising breaches
- Secure communication
- Records retention

Appendix A – The Seven Data Protection Principles

1. Lawfulness, Fairness, Transparency – Data must be processed legally and openly.
2. Purpose Limitation – Data must be collected for specific purposes.
3. Data Minimisation – Only necessary data should be collected.
4. Accuracy – Data must be correct and updated.
5. Storage Limitation – Data must not be kept longer than needed.
6. Integrity and Confidentiality – Data must be kept secure.
7. Accountability – The Council must demonstrate compliance.

Appendix B – Records Retention Schedule (separate document)

Appendix C – Subject Access Request Procedure

1. Request received (email, letter, or verbal).
2. Identity verified.
3. Logged by the Clerk.
4. Data gathered from all systems.
5. Response issued within one month.
6. Extensions documented if needed.
7. Data provided securely (encrypted email or printed copy).

Appendix D – Data Breach Reporting Form

- Date and time of breach
- Description of incident
- Categories of data involved
- Number of individuals affected
- Immediate actions taken
- Assessment of risk
- Whether ICO notification is required
- Follow-up actions

.