GRINDALE PARISH COUNCIL

Data Protection Policy Adopted 6 July 2026

---

1. Purpose

This policy sets out how the Council protects personal information, ensures lawful and transparent processing, and upholds the rights of individuals in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Council is committed to handling all information responsibly, securely and with respect. This policy works alongside the Council's:

- Privacy Notice (explains what data we collect, why, and how long we keep it)
- Document Retention Policy (sets out how long information is stored and when it is securely destroyed)
- Freedom of Information (FOI) Publication Scheme (outlines what information the Council routinely makes publicly available)
- Councillor Code of Conduct
- Vexatious Complaints & Correspondence Policy

2. Scope

This policy applies to all information/data processed by or on behalf of the Council, which includes:

- Staff and job applicants
- Volunteers
- Councillors
- Contractors
- Residents and service users

It covers all information formats, including electronic systems, paper records, emails, photographs, audio, video and recorded communications.

This policy applies to all information processed on behalf of the Council, regardless of the device, system or location used. Personal devices, private email accounts and messaging applications must not be used for Council business.

3. Key Definitions

Personal Data: Information that identifies, or could identify, a living person.

Special Category Data: Sensitive information requiring additional protection, such as health, ethnicity, beliefs, sexual orientation or biometric data.

Criminal Offence Data: Information relating to criminal allegations, investigations or convictions.

Processing: Any action involving personal data, including collecting, storing, sharing, amending or deleting it.

Data Controller: The organisation that determines the purpose and means of processing personal data. For all Council business, the Data Controller is the Council as a corporate body.

Data Processor: Any individual or organisation processing data on behalf of the Council under its instruction.

4. Data Protection Principles

The Council processes personal data in line with the UK GDPR principles. Personal data must be:

1. Lawful, fair and transparent
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 as long as necessary (see Document Retention Policy)
6. Processed securely to prevent loss, misuse or unauthorised access

5. Lawful Bases for Processing

The Council processes personal data only where one or more lawful bases apply:

- **Public task** – performing statutory or official duties
- **Legal obligation** – complying with the law
- **Contract** – managing employment, volunteer or service arrangements
- **Legitimate interests** – where appropriate and balanced
- **Vital interests** – protecting life
- **Consent** – used only where no other lawful basis applies

Special category data is processed only where a specific legal condition applies, such as employment law, public health, substantial public interest or explicit consent.

6. How the Council Uses Personal Data

Personal data may be used for purposes including:

- Recruitment, employment and volunteer administration
- Councillor role administration
- Delivering services to residents
- Managing enquiries, complaints and statutory duties
- Contract and supplier management
- Community engagement and public consultations
- Safeguarding and public protection
- Emergency planning and public safety

The Council does not use personal data for direct marketing, political campaigning or any purpose incompatible with its statutory functions.

Full details are provided in the Council's Privacy Notice.

7. Sharing Personal Data

The Council may share personal data with:

- Government departments and regulators
- Payroll, HR, IT and professional service providers
- Contractors delivering services on the Council's behalf
- Law enforcement agencies
- Other public authorities where legally permitted

All third parties must comply with data protection law and process data only on the Council's instructions.

Personal data will only be shared where there is a lawful basis and, where appropriate, with the written authorisation of the Clerk or the Council. Unauthorised disclosure of personal data is prohibited.

8. Individual Rights

Individuals have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request deletion (in certain circumstances)
- Restrict or object to processing
- Request data portability (where applicable)
- Complain to the Information Commissioner's Office (ICO)

Subject Access Requests (SARs)

All Subject Access Requests must be submitted in writing to the Clerk. Verbal or informal requests cannot be accepted. The Council may require proof of identity before processing a request.

The Council will respond within one calendar month of receiving a valid written request and any required identification. This period may be extended where the request is complex or where multiple requests are made.

9. Data Security

Everyone working with or for the Council must:

- Keep personal data secure and confidential
- Use strong passwords and lock screens
- Store documents safely and dispose of them securely
- Access only the information they are authorised to use
- Not store Council data on personal devices
- Not remove data from Council premises without authorisation
- Report any concerns or breaches immediately

10. Data Breaches

A data breach is any incident that results in the loss, alteration, unauthorised disclosure or access to personal data.

If a breach occurs, the Council will:

- Record the incident
- Assess the risk
- Notify the ICO within 72 hours if required
- Inform affected individuals where there is a high risk

All staff, volunteers and councillors must report suspected breaches immediately to the Clerk. The Clerk will assess the breach and report it to the Council. The Council, as Data Controller, will determine whether the ICO or affected individuals must be notified

11. Information Governance and Transparency

The Council is committed to openness and accountability. Information routinely published under the ICO Model Publication Scheme includes:

- Governance and decision-making information
- Financial information
- Policies and procedures
- Public meeting agendas and minutes

Requests for information under the Freedom of Information Act 2000 or Environmental Information Regulations 2004 will be handled in line with statutory requirements.

Councillors must not release information in response to FOI or EIR requests. All statutory information requests must be handled by the Clerk.

The Council may refuse or charge for requests that are manifestly unfounded, excessive, repetitive or abusive, in line with the Council's Vexatious Complaints & Correspondence Policy.

12. International Transfers

The Council does not transfer personal data outside the UK/EEA unless appropriate legal safeguards are in place.

13. Responsibilities

The Council is the Data Controller and holds overall responsibility for compliance with data protection legislation. The Clerk acts as the Data Protection Lead, implementing this policy under the direction and authority of the Council.

All staff, volunteers and councillors must:

- Follow this policy and all related information governance procedures

- Complete mandatory training where required
- Report any concerns, risks or data breaches immediately
- Handle all information responsibly, securely and only for authorised purposes

In addition, councillors are required to:

- Use only Council-approved email accounts and Council-approved online storage systems for all Council business
- Avoid storing resident or Council data on personal devices, personal email accounts or messaging apps
- Comply with the Council's retention and deletion rules
- Not create or maintain personal mailing lists, databases or unofficial records of residents or service users.

Failure to comply with this policy may result in disciplinary action or referral under the Councillor Code of Conduct.

Staff, volunteers and councillors acting in good faith and in accordance with this policy will not be personally liable for honest mistakes. Disciplinary or corrective action applies only to deliberate, negligent or reckless breaches of data protection requirements.

14. Training

Training is provided to all staff, volunteers and councillors who handle personal data. Additional training is provided for those with specific responsibilities.

Councillors must complete data protection training within six months of taking office and refresh it at least once every four years.

Version Control		
	Date	Comments
Adopted	06/07/2026	By Full Council
Reviewed		