



RUDGWICK PARISH COUNCIL

INFORMATION AND DATA PROTECTION POLICY

Date Adopted	Minute Number	Review Date
9 th Feb 2026	FC222-25/26	Sept 2026
11 th May 2026	FC027-26/27	May 2027

1. Purpose

This policy sets out how **Rudgwick Parish Council** ("the Council") will comply with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It explains how personal data will be collected, stored, processed, shared, and disposed of, and how individuals can exercise their rights.

2. Scope

This policy applies to all personal data processed by the Council, whether held electronically or in paper format, including (but not limited to):

- Personal data concerning its current, past councillors, employees, contractors, volunteers, and job applicants
- Personal data of members of the public, clients, service users, and third parties

*Clerk, Rudgwick Parish Council, Rudgwick Parish Office,
Rudgwick Hall, Bucks Green, Rudgwick, West Sussex RH12 3JJ*

- Sensitive (special category) data where relevant
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked on.
- Confidential information about other organisations because of sensitivity issues.
- Both manual records and digital records

All staff, councillors, volunteers, contractors, and anyone acting on behalf of the Council must comply with this policy.

3. Definitions

Term	Definition
Personal data	Any information relating to a living individual who can be identified, directly or indirectly, from that data or in combination with other information.
Processing	Any operation or set of operations performed on personal data, e.g. collection, recording, use, storage, disclosure, erasure.
Controller	The entity which determines the purposes and means of processing personal data (here, the Council).
Processor	A person or organisation that processes data on behalf of the controller.
Special categories of personal data	Data such as racial or ethnic origin, political opinions, religious beliefs, health data, biometric data, etc.
Consent	A freely given, specific, informed and unambiguous indication of the individual's wishes by which they signify agreement to the processing of their data.
Data subject	The individual whose personal data is being processed.

4. Data Protection Principles

In accordance with Article 5 of GDPR, Rudgwick Parish Council will ensure that personal data is:

1. **Processed lawfully, fairly and transparently**
2. **Collected for specified, explicit and legitimate purposes** and not further processed in a manner incompatible with those purposes
3. **Adequate, relevant and limited** to what is necessary

4. **Accurate and, where necessary, kept up to date**; steps will be taken to rectify or erase inaccurate data without delay
5. **Retained only as long as necessary** for the purposes of processing
6. **Processed in a manner ensuring appropriate security**, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage

5. Lawful Basis for Processing

The Council will only process personal data where at least one of the following lawful bases applies:

- Performance of a contract (e.g. employment contract)
- Compliance with a legal obligation
- Legitimate interests of the Council or third party, unless outweighed by the rights of the individual
- Vital interests (to protect life)
- Public interest / official authority
- Consent (where none of the above applies)

For special category data, a further condition must be met (e.g. explicit consent, vital interests, employment law compliance, etc.).

6. Privacy Notices

The Council will publish or provide privacy notices that inform data subjects about:

- What personal data is collected
- The purpose(s) for processing
- The lawful basis for processing
- Who the data may be shared with
- Retention periods
- Data subject rights
- How to withdraw consent, lodge complaints, or access data

7. Data Subject Rights

Data subjects have rights under UK GDPR, including:

- Right of access (subject access request)

- Right to rectification
- Right to erasure (“right to be forgotten”)
- Right to restrict processing
- Right to object to processing
- Right to data portability
- Rights relating to automated decision-making / profiling

Requests should be directed to the Clerk or designated data protection contact. The Council will normally respond within one month, unless extended in complex cases (up to three months) in which case the data subject will be informed.

8. Responsibilities

Council / Governing Body

- Ensure adequate resources are allocated to compliance
- Approve policies, oversee audits

Clerk / Data Protection Lead

- Acts as point of contact for data protection
- Maintains records of processing, oversees training, advises staff

Staff, Volunteers & Councillors

- Must follow this policy
- Report data breaches or incidents immediately
- Ensure personal data processed within their remit is handled appropriately

Processors / Contractors

- Must act only on the Council’s instructions
- Must implement appropriate technical and organisational measures
- Will enter into written contracts (e.g. data processing agreement)

9. Data Security and Confidentiality

The Council will maintain appropriate security measures (physical, technical, organisational) to protect personal data:

- Access controls (passwords, user access levels)
- Encryption where appropriate
- Secure storage (locked cabinets for paper files)

- Secure disposal / deletion when no longer needed
- Regular backups
- Training and awareness

10. Data Breach Management

If a personal data breach occurs (or is suspected), it must be reported immediately to the Clerk / Data Protection Lead.

The Council will investigate, contain and, where appropriate, notify:

- The Information Commissioner's Office (ICO) (if the breach is likely to result in a risk to individuals' rights and freedoms)
- Affected data subjects (where there is likely to be a high risk)

A breach log will be maintained with details, remediation steps, lessons learned.

11. Record-Keeping / Documentation

The Council will maintain internal records of all processing activities in accordance with Article 30 of GDPR. These records should include:

- Purposes of processing
- Categories of data subjects and personal data
- Categories of recipients
- Transfers to third countries (if any)
- Retention periods
- Description of technical and organisational security measures

12. Data Protection Impact Assessments (DPIAs)

Where processing is likely to result in high risk to individuals' rights and freedoms (e.g. CCTV, profiling, large-scale processing), the Council will carry out DPIAs prior to processing. The DPIA will assess necessity, proportionality and mitigation measures.

13. Training and Awareness

Training on data protection, information security, and this policy will be provided to all councillors, staff, volunteers, contractors, and regular refresher training. Awareness will be maintained (e.g. via updates, guidance, reminders).

14. Third Party Sharing / Data Transfers

When personal data is shared with third parties (e.g. service providers, contractors), the following will be ensured:

- Only the minimum data necessary is provided

- Written agreement / contract in place (data processing agreement)
- Obligation on the third party to protect data in accordance with this policy and law
- No transfer to a country outside the UK/EU unless appropriate safeguards are in place

15. Retention and Disposal

Personal data will not be kept longer than necessary. Data will be kept for different lengths of time, depending on legal and operational requirements. The Council will maintain a

Retention Schedule. After expiry:

- Secure deletion from electronic systems
- Secure shredding or destruction of hard copies
- Logs may be kept of what was disposed, when, and by whom

16. Monitoring and Review

The Council will periodically review this policy (at least annually) and monitor compliance. Any changes in law or practice will be incorporated.

17. Complaints and Enforcement

Individuals may make a complaint to the Council's Clerk / Data Protection Lead. If unsatisfied, they can lodge a complaint with the Information Commissioner's Office (ICO) at ico.org.uk.