Stonesfield Parish Council

Data Protection & Information Management Policy

---

1. Introduction

Stonesfield Parish Council is committed to protecting the rights and privacy of individuals and to ensuring that personal data is handled lawfully, transparently, and securely.

This policy sets out how the Council collects, uses, stores, shares, and disposes of personal data in accordance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Other relevant legislation and good practice

The Council acts as both **Data Controller** and **Data Processor**.

---

2. Scope

This policy applies to all councillors, employees, contractors, and volunteers who process personal data on behalf of the Council.

It covers personal data held in any format, including:

- Emails and electronic documents
- Paper files and printed records
- Spreadsheets, PDFs, scanned files
- Photographs, audio, and video
- Data stored on Council devices or authorised cloud systems

---

3. Definitions

Personal Data
Any information relating to an identifiable living individual.

Special Category Data
Sensitive data requiring stronger protection (e.g. health data).

Processing
Any action applied to data — collection, storage, use, sharing, deletion, etc.

Data Subject
The individual whose personal data is being processed.

Data Controller
The organisation determining how and why data is processed — Stonesfield Parish Council.

---

4. Data Protection Principles

The Council will ensure that all personal data is:

1. **Processed lawfully, fairly, and transparently**
2. **Collected for specific, explicit purposes**
3. **Adequate, relevant, and limited** to what is necessary
4. **Accurate and kept up to date**
5. **Kept only for as long as necessary**
6. **Processed and stored securely**

---

5. Lawful Bases for Processing

The Council processes personal data under at least one of the lawful bases:

- Consent
- Contract
- Legal obligation
- Public task
- Vital interests
- Legitimate interests (rarely used in local councils)

The Council maintains a record of processing activities describing the lawful basis for each category of data.

---

6. Roles and Responsibilities

Full Council
Overall accountability for compliance with data protection legislation.

The Clerk (Data Protection Lead)

- Ensures compliance with this policy
- Maintains records of processing activities
- Responds to Subject Access Requests
- Reports data breaches where required
- Provides guidance and training

Councillors and staff
Must follow this policy and handle personal data securely at all times.

---

7. Collection and Use of Personal Data

The Council will:

- Collect only the minimum data necessary
- Inform individuals why their data is collected
- Use it only for the purpose it was collected
- Not share data with third parties unless lawful and necessary
- Review data regularly to ensure accuracy

Examples of Council-held data include:

- Contact details of residents
- Allotment tenancy information
- Burial ground records (if applicable)
- Supplier and contractor information
- Councillors' declarations and correspondence

---

8. Data Storage & Security

Personal data must be stored securely at all times.

Electronic Data

- Stored on secure, password-protected devices or cloud systems
- Encrypted where appropriate
- Backed up regularly
- Accessible only to authorised users

Paper Records

- Stored in locked cabinets
- Access limited to authorised individuals
- Secure destruction when no longer required

---

9. Data Sharing

The Council will not share personal data with third parties unless:

- A legal obligation applies
- The data subject has given consent
- Sharing is necessary to deliver a public task
- A written data processing agreement is in place (where required)

---

10. Data Retention & Disposal

The Council follows the **Local Government Association's standard retention guidelines** (adapted where appropriate) and retains data only for as long as necessary.

When no longer required, data will be:

- Deleted securely (electronic)
- Shredded or securely destroyed (paper)

---

11. Subject Access Requests (SARs)

Individuals have the right to:

- Know what personal data the Council holds about them
- Request a copy of their data
- Request correction of inaccurate data
- Request erasure (where lawful)
- Restrict or object to processing

SARs must:

- Be made in writing
- Include proof of identity
- Be responded to within **one month**

The Clerk is responsible for coordinating responses.

---

12. Data Breaches

A data breach is any loss, unauthorised access, or improper disclosure of personal data.

All councillors and staff must:

- Report suspected breaches immediately to the Clerk
- Assist in investigation and documentation

Serious breaches may require reporting to the ICO **within 72 hours**.

A breach log will be maintained.

---

13. Training & Awareness

The Council will ensure councillors, employees, and volunteers receive training on:

- Data protection principles
- Secure handling of personal data
- Recognising and reporting breaches
- Use of Council IT systems

Training will be refreshed annually or sooner if needed.

---

14. Compliance & Enforcement

Failure to comply with this policy may result in:

- Loss of access to Council systems
- Referral to the Monitoring Officer
- Disciplinary or governance action

---

15. Policy Review

This policy will be reviewed annually or earlier if legislation or Council practices change.

Adopted: 6 May 2026
Reviewed: