

Shepherdswell *with* Coldred Parish Council

Data Protection Policy

1. Introduction

Shepherdswell with Coldred Parish Council ("the Council") is committed to protecting the privacy and security of personal data. The Council collects and processes personal information to carry out its functions as a public authority. This policy sets out how the Council complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Purpose of the Policy

This policy explains:

- what personal data the Council collects and why
 - how personal data is used, stored and protected
 - the rights of individuals whose data is held
 - the responsibilities of councillors, staff and volunteers
 - how the Council ensures compliance with data protection legislation
-

3. Scope

This policy applies to:

- all personal data processed by the Council
 - all councillors, employees, contractors and volunteers who handle personal data on behalf of the Council
 - all formats, including electronic files, emails, paper records, photographs and CCTV (if applicable)
-

4. Data Protection Principles

The Council complies with the six principles of UK GDPR. Personal data must be:

1. **Processed lawfully, fairly and transparently**
2. **Collected for specified, explicit and legitimate purposes**
3. **Adequate, relevant and limited to what is necessary**
4. **Accurate and kept up to date**
5. **Kept no longer than necessary**
6. **Processed securely**

The Council is responsible for demonstrating compliance with these principles (the "accountability" requirement).

5. Lawful Bases for Processing

The Council processes personal data under the following lawful bases:

- **Public task** – carrying out functions and powers as a parish council
- **Legal obligation** – complying with statutory duties (e.g., financial, audit, employment, cemetery regulations)
- **Contract** – where processing is necessary for a contract with an individual
- **Consent** – for optional activities where consent is freely given
- **Legitimate interests** – where appropriate and balanced

Special category data is processed only where a lawful condition applies.

6. Types of Personal Data the Council Processes

The Council may process:

- Contact details (names, addresses, phone numbers, email addresses)
- Correspondence and enquiries
- Allotment tenancy information
- Cemetery records and burial registers
- Employment and HR records
- Contractor and supplier information
- Planning comments submitted by residents
- Complaints and FOI/EIR requests
- Photographs or CCTV images (if applicable)

The Council does **not** collect more information than is necessary for its functions.

7. Data Subject Rights

Individuals have the right to:

- be informed about how their data is used
- access their personal data
- request correction of inaccurate data
- request erasure (where applicable)
- restrict or object to processing (in certain circumstances)
- data portability (where applicable)
- not be subject to automated decision-making

Requests must be submitted to the Clerk as the Council's Data Protection Officer (or designated lead). The Council will respond within one month.

8. Data Security

The Council ensures that personal data is kept secure by:

- using password-protected devices and secure storage
- limiting access to authorised personnel only
- keeping paper records in locked storage

- using secure email practices
- ensuring regular backups of electronic data
- disposing of data safely and confidentially

Councillors must follow the Council's security procedures when handling personal data.

9. Data Sharing

The Council only shares personal data when:

- required by law
- necessary to carry out a public task
- required for audit or regulatory purposes
- the individual has given consent

The Council does not sell personal data to third parties.

10. Data Retention

Personal data is retained only for as long as necessary. The Council follows its **Records Management & Retention Policy** (to be adopted separately) which sets out specific retention periods for different categories of information.

11. Data Breaches

A data breach is any incident that results in:

- loss of personal data
- unauthorised access
- accidental disclosure
- destruction or alteration

All breaches must be reported immediately to the Clerk.

Where a breach poses a risk to individuals, the Council will notify the Information Commissioner's Office (ICO) within 72 hours and inform affected individuals where required.

12. Roles and Responsibilities

- The **Council** is the Data Controller.
- The **Clerk** is responsible for day-to-day data protection compliance.
- **Councillors and staff** must follow this policy and handle personal data responsibly.

Training will be provided where appropriate.

13. Review of Policy

This policy will be reviewed every two years or sooner if legislation or guidance changes.

Adopted by Shepherdswell with Coldred Parish Council

Date: _____
Chair: _____
Clerk: _____

DRAFT