1. Introduction

Chevington Parish Council ("the Council") is committed to protecting the privacy and security of personal data. This policy explains how the Council complies with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

The Council is a *Data Controller* and processes personal data to carry out its statutory functions, deliver services, and respond to residents.

2. Definitions

- **Personal Data:** Information relating to an identifiable living individual.
- **Special Category Data:** Sensitive data requiring additional protection (e.g., health, ethnicity, political opinions).
- **Processing:** Any operation performed on personal data, including collection, storage, use, sharing, or deletion.
- **Data Subject:** The individual to whom the data relates.
- **Data Controller:** The organisation determining how and why data is processed.
- **Data Processor:** A third party processing data on behalf of the Council.

3. Lawful Bases for Processing and why it may be collected

The Council processes personal data under the following lawful bases:

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks. If the council

is doing something it is legally required or empowered to do, it cannot rely on legitimate interests.)

Individuals have the right to know how their personal data is used, to access it, correct it, delete it where possible, restrict or object to its use, receive a copy in a usable format, and not be subject to unfair automated decisions.

The Council does **not** rely on consent where another lawful basis applies.

4. Data the Council Collects

The Council typically processes:

Personal Data

- Names, addresses, telephone numbers, email addresses
- Correspondence from residents
- Contact details for contractors, suppliers, and community groups
- Employment and payroll information
- Lease and land-related information
- Website contact form submissions
- Electoral roll data (restricted access)

Special Category Data

The Council does **not routinely collect** special category data.
If collected (e.g., through surveys), responses are anonymised.

5. How Data Is Obtained

- Directly from individuals (emails, letters, forms, telephone calls)
- From third parties (District Council, contractors)
- From publicly available sources
- Automatically via the Council website (analytics, cookies)

6. How Data Is Used

Personal data is used only for the purpose it was collected, including:

- Responding to enquiries
- Managing council assets (e.g., recreation ground)

- Maintaining financial and audit records
- Managing contracts, leases, and suppliers
- Employment administration
- Publishing agendas, minutes, and statutory notices
- Maintaining the Council website

The Council does **not** sell personal data.

7. Data Sharing

Data may be shared with:

- West Suffolk District Council (statutory functions)
- Internal and external auditors
- Payroll provider
- Insurers
- Website administrator
- Contractors working on behalf of the Council

Data is shared only when necessary and with appropriate safeguards.

8. Data Storage and Security

The Council uses a combination of physical and digital security measures:

Physical Security

- Locked filing cabinets in the Clerk's home
- Controlled access to paper records

Digital Security

- Password-protected devices
- Up-to-date antivirus and security software
- Encrypted cloud storage (e.g., Microsoft OneDrive)
- Regular backups
- Access restricted to authorised personnel only

9. Data Retention

The Council retains data only as long as necessary.
Retention periods follow:

- **NALC / SLCC guidance**
- **Local Government Act requirements**
- **Audit and financial regulations**

A full **Retention Schedule** is maintained separately.

10. Data Subject Rights

Individuals have the right to:

- Access their data
- Rectify inaccurate data
- Request erasure (where applicable)
- Restrict processing
- Object to processing
- Data portability (rarely applicable to councils)

Requests must be submitted in writing.
The Council will respond within **one month**.

Identity verification may be required.

11. Subject Access Requests (SARs)

The Council will:

1. Acknowledge the request
2. Verify identity
3. Assess whether the request is valid
4. Provide the information within one month
5. Extend by up to two months for complex cases
6. Keep a log of all SARs

No fee is charged unless the request is manifestly excessive.

12. Data Breaches

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

The Council will:

1. Identify and contain the breach
2. Assess the risk to individuals
3. Notify the ICO within **72 hours** if required
4. Inform affected individuals where there is a high risk
5. Record all breaches
6. Review procedures to prevent recurrence

13. Data Processors

Where the Council uses third-party processors (e.g., payroll, website hosting), it ensures:

- Written contracts are in place
- Processors comply with UK GDPR
- Data is processed only on documented instructions

14. Roles and Responsibilities

- **The Council** is the Data Controller.
- **The Clerk** acts as the Council's **Data Protection Lead** (not a statutory DPO).
- All councillors and staff must follow this policy and complete training where required.
- Chevington Parish Council is registered with the Information Commissioner's Office as a Data Controller and pays the annual Data Protection Fee.
- The Council provides a Privacy Notice explaining how personal data is used. This is available on the Council website and on request.

15. Review and Updates

This policy is reviewed annually or sooner if:

- Legislation changes
- The Council's data processing activities change
- The ICO issues new guidance