Snodland Town Council

Data Protection Policy

Document Control	
Version Number:	1
Adopted on:	6th August 2026
Next Review in:	2031

1. Introduction

Snodland Town Council is committed to ensuring that personal data is handled lawfully, fairly, and transparently, and that the rights of individuals are respected.

This policy sets out how the Council meets its obligations under the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Related legislation and guidance issued by the Information Commissioner's Office (ICO)

This policy forms part of the Council's wider information governance framework and should be read alongside:

- Privacy Notices
- Retention and Disposal Policy;
- Freedom of Information and Publication Scheme Policy
- Subject Access Request (SAR) Procedure
- Digital IT and Security Policies

2. Scope

This policy applies to:

- All Councillors
- All employees
- Volunteers
- Contractors and service providers where relevant to Council data processing activities

It covers all personal data processed by the Council in any format, including paper records, electronic records, email, cloud-based systems, and portable devices.

3. Data Protection principles

The Council will comply with the data protection principles set out in Article 5 of the UK General Data Protection Regulation (UK GDPR), as supplemented by the Data Protection Act 2018. Personal data shall 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, where necessary, kept up to date.
5. Kept for no longer than is necessary.
6. Processed securely using appropriate technical and organisational measures.

The Council is accountable for, and must be able to demonstrate, compliance with these principles.

4. Lawful basis for processing

The Council processes personal data under one or more lawful bases, including:

- Public task (performance of statutory functions)
- Legal obligation
- Contract
- Consent (where appropriate)
- Legitimate interests (where applicable)

Where special category data is processed, the Council will ensure an additional lawful condition applies under UK GDPR and the Data Protection Act 2018.

5. Roles and responsibilities

5.1 The Council

The Council has overall responsibility for ensuring compliance with data protection legislation.

5.2 Chief Executive Officer

The Chief Executive Officer is responsible for day-to-day oversight of data protection compliance, including:

- Ensuring policies and procedures are implemented.
- Acting as the first point of contact for data protection matters.
- Coordinating responses to Subject Access Requests.
- Managing data breaches and notifications where required.
- Maintaining appropriate records of processing activities.

5.3 Councillors and staff

All Councillors and staff must:

- Handle personal data in accordance with this policy.
- Maintain confidentiality.
- Report suspected data breaches immediately.
- Participate in relevant data protection training.

Councillors may act as data controllers in their own right in certain circumstances (for example, constituency casework) and are responsible for complying with data protection requirements in those contexts.

6. Data security

The Council will implement appropriate technical and organisational measures to protect personal data, including:

- Secure storage of paper records
- Access controls for electronic systems
- Password protection and secure authentication
- Use of encrypted systems and secure cloud providers where appropriate
- Regular review of access permissions

All personal data must be protected against unauthorised access, loss, destruction, or disclosure.

7. Data sharing and processors

Where the Council shares personal data with third parties or uses service providers (data processors), it will:

- Ensure appropriate contracts or Data Processing Agreements are in place.
- Confirm that adequate security measures are implemented.
- Share only the minimum data necessary.

Personal data will not be transferred outside the UK unless appropriate safeguards are in place.

8. Individual rights

Individuals have rights under UK GDPR, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (in certain circumstances)
- The right to restrict processing

- The right to data portability (where applicable)
- The right to object
- Rights relating to automated decision-making and profiling

The Council's procedures, including the SAR Procedure, ensure these rights are respected.

9. Data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

All suspected data breaches must be reported immediately to the Chief Executive Officer.

Where required, the Council will notify the ICO within 72 hours of becoming aware of a reportable breach and will inform affected individuals where there is a high risk to their rights and freedoms.

A record of all breaches and near misses will be maintained.

10. Records management and retention

Personal data will be retained in accordance with the Council's Retention and Disposal Policy.

Data will not be kept longer than necessary and will be securely disposed of when no longer required.

Audio or visual recordings of Council meetings will be retained and disposed of in accordance with the Council's Retention and Disposal Policy and Standing Orders.

11. Training and awareness

The Council will ensure that Councillors and staff receive appropriate data protection awareness training and updates as required.

12. Monitoring and review

This policy will be reviewed annually, or sooner if required due to changes in legislation, guidance, or Council practices.