Woodstock Town Council
Data Protection Policy

1. Introduction

Woodstock Town Council ("the Council") is committed to protecting the privacy and security of personal data in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). This policy sets out how the Council collects, uses, stores, and protects personal data and ensures councillors and the Clerk understand their legal responsibilities. This policy requires the Clerk to consider data protection legislation and best practices before starting any new data processing activity to ensure that relevant compliance steps are addressed.

2. Definitions

- The GDPR: Regulation (EU) 2016/679 on the protection of natural persons with regard to personal data processing.
- Data Protection Legislation: The Data Protection Act 2018 and the GDPR as retained in UK law.
- Personal Data: Any information relating to an identified or identifiable living individual.
- Data Subject: An individual whose personal data is processed.
- Processing: Any operation performed on personal data, including collection, storage, use, sharing, deletion, etc.
- Data Controller: The person or body that determines the purposes and means of processing personal data.
- Data Processor: A person or body that processes personal data on behalf of a data controller.
- Sensitive Personal Data: Includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, or criminal offences.
- Council Purposes: The legitimate functions of the Council, including service delivery, administration, governance, and legal compliance.

3. Scope

This policy applies to:

- All councillors
- The Clerk and any staff, volunteers or contractors
- All personal data processed by or on behalf of the Council

This policy supplements other Council policies, such as IT, internet, and email use.

4. Data Controller

The Town Clerk is designated as the Data Controller for Woodstock Town Council and is responsible for the implementation of this policy.
Clerk's Contact Details:
Town Hall, Market Place, Woodstock, OX20 1SL
Tel: 01993 811216
Email: clerk@woodstock-tc.gov.uk
The Clerk will receive appropriate training and maintain awareness of relevant legislation.

5. Responsibilities of the Data Controller

The Clerk will:

- Keep the Council informed of data protection responsibilities and risks
- Review all data protection procedures and policies regularly

Date Adopted:	02.09.2025	**Minute Number:**	WTC 25/09/11 b
Updated:		**Minute Number:**	
Review Date:		**Minute Number:**	

- Respond to data protection queries from councillors and staff
- Assist with training and awareness
- Oversee the handling of data subject requests
- Vet third-party processors and approve data-sharing agreements
- Ensure all systems and services meet acceptable security standards
- Approve privacy notices and assess third-party services (e.g. cloud storage)
- Maintain the Council's data register and audit trail

6. Collecting and Processing Personal Data

Personal data must only be collected where there is a valid legal basis under the GDPR. These include:

- Consent – freely given, specific, informed, and unambiguous
- Contractual necessity
- Legal obligation
- Vital interests
- Public task – carried out in the public interest or official authority
- Legitimate interests

7. Data Protection Principles

The Council will adhere to the six data protection principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

8. Privacy Notices

The Council will issue privacy notices to:

- Staff, councillors, contractors, volunteers
- Residents and service users

These notices will explain:

- What data is collected and why
- How it is collected and stored
- Who it may be shared with
- Retention periods
- Data subject rights and contact details

9. Sensitive Personal Data

Processing sensitive data requires additional safeguards. Explicit consent will usually be required, unless:

- The processing is required by law
- The data subject cannot give consent (e.g., emergencies)

All processing will be documented with justification.

10. Criminal Record Checks

Criminal record checks will only be conducted where legally justified. Consent alone is insufficient.

11. Data Accuracy and Relevance

The Council will:

- Ensure data is accurate and up to date
- Only process data necessary for a specified purpose
- Permit individuals to request corrections to their data

12. Data Security

The Council will apply appropriate technical and organisational measures to protect personal data.
Storage standards include:

Date Adopted:	02.09.2025	**Minute Number:**	WTC 25/09/11 b
Updated:		**Minute Number:**	
Review Date:		**Minute Number:**	

- Printed data locked away; shredded when no longer needed
- Computers protected by strong, regularly changed passwords
- Secure cloud and backup systems approved by the Clerk
- No data storage on unprotected mobile devices
- Security software and firewalls on all servers

13. Data Retention

Personal data must not be retained longer than necessary. Retention will follow the Council's retention guidelines and be justified in the data register.

14. Subject Access Requests (SARs)

Data Subjects may request access to personal data held about them. Requests must be made to the Clerk and will be fulfilled within one month, provided there is no undue burden or conflict with other individuals' rights.

15. Right to Erasure

Data Subjects may request deletion of their data. The Council will comply unless an exemption applies (e.g. legal obligation).

16. Privacy by Design and Default

The Clerk must consider privacy at the design stage of any project. Data protection should be built into processes and systems, using minimum necessary personal data.

17. Data Audits and Register

The Clerk will maintain a data register, which records:

- What data is held
- Where it is stored
- How it is used
- Who is responsible
- Retention schedules and relevant laws

Regular audits will be conducted.

18. Reporting Data Breaches

All councillors and staff must report actual or suspected data breaches to the Clerk immediately. The Clerk will:

- Investigate the incident
- Record the event in the compliance register
- Notify the Information Commissioner's Office (ICO) where required within 72 hours

19. Monitoring and Review

The Clerk will monitor adherence to this policy and report concerns to the Council. The policy will be reviewed annually or following changes in legislation.

20. Consequences of Non-Compliance

Breaches of this policy may result in:

- Disciplinary action
- Investigation by regulatory authorities
- Reputational and financial harm to the Council

All councillors, volunteers and staff must familiarise themselves with this policy and comply with its requirements.

Date Adopted:	02.09.2025	**Minute Number:**	WTC 25/09/11 b
Updated:		**Minute Number:**	
Review Date:		**Minute Number:**	