



Model Policy (UK GDPR and Data Protection Act 2018)

Document Title: Data Protection Policy

Organisation: Shipston Town Council

Version: 1.0

Approved By: Full Council – Monday 13th July 2026

Review Date: Annually

Policy Owner: Town Clerk

1. Policy Statement

Shipston Town Council is committed to ensuring that personal data is handled lawfully, fairly, transparently, and securely in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, and other relevant legislation.

The Council holds and processes information about employees, councillors, residents and customers and other data subjects for administration and commercial purposes

The Council recognises its responsibilities as a Data Controller and is committed to protecting the rights and freedoms of individuals whose personal data it processes.

This policy applies to all councillors, employees, contractors, volunteers, and any other persons acting on behalf of the Council.

2. Purpose

The purpose of this policy is to:

- Ensure compliance with UK GDPR and data protection legislation.
- Protect personal data held by the Council.
- Promote good practice in the handling of personal information.
- Clarify roles and responsibilities relating to data protection.
- Reduce the risk of data breaches and associated penalties.

3. Scope

This policy applies to:

- Personal data held electronically and in paper records.
- Information relating to residents, employees, councillors, suppliers, contractors, volunteers, and service users.
- All Council activities involving the collection, storage, use, disclosure, retention, or destruction of personal data.

4. Definitions

Personal Data

Any information relating to an identified or identifiable living individual.

Examples include:

- Name
- Address
- Telephone number
- Email address
- National Insurance number
- Payroll information
- Photographs where individuals can be identified

Special Category Data

Information requiring additional protection, including:

- Health information
- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Biometric or genetic data

Processing

Any operation performed on personal data including:

- Collection
 - Recording
 - Storage
 - Retrieval
 - Consultation
 - Disclosure
 - Erasure
-

5. Data Protection Principles

Shipston Town Council shall ensure personal data is:

a) Lawful, Fair and Transparent

Personal data shall be processed only where there is a lawful basis and individuals are informed how their data will be used.

b) Collected for Specific Purposes

Data shall only be collected for legitimate Council purposes and not used incompatibly with those purposes.

c) Adequate, Relevant and Limited

Only information necessary for Council business shall be collected and processed.

d) Accurate and Up to Date

Reasonable steps shall be taken to ensure personal data is accurate and corrected where necessary.

e) Kept No Longer Than Necessary

Data shall be retained in accordance with the Council's Retention and Disposal Schedule.

f) Secure

Appropriate technical and organisational measures shall be implemented to protect personal data.

g) Accountable

The Council shall be able to demonstrate compliance with data protection legislation.

6. Lawful Bases for Processing

The Council will process personal data only where one or more lawful bases apply:

- Consent
- Performance of a contract
- Compliance with a legal obligation
- Protection of vital interests
- Performance of a task carried out in the public interest or under official authority
- Legitimate interests (where applicable)

The most common lawful basis used by the Council will be Public Task and Legal Obligation.

7. Individual Rights

The Council shall respect and facilitate the rights of data subjects, including:

Right to be Informed

Individuals have the right to know how their data is collected and used.

Right of Access

Individuals may request copies of their personal data through a Subject Access Request (SAR).

Right to Rectification

Individuals may request correction of inaccurate information.

Right to Erasure

Individuals may request deletion of personal data where appropriate.

Right to Restrict Processing

Processing may be limited in certain circumstances.

Right to Data Portability

Where legally applicable, data may be provided in a suitable electronic format.

Right to Object

Individuals may object to processing in specific circumstances.

Rights Related to Automated Decision-Making

The Council does not generally undertake automated decision-making or profiling.

8. Subject Access Requests (SARs)

Making a Request

Requests may be made in writing, by email, or verbally.

Response Time

The Council will respond within one month of receiving a valid request.

Verification

Proof of identity may be required before information is disclosed.

Charges

SARs will normally be provided free of charge unless requests are manifestly unfounded or excessive.

9. Information Security

The Council shall implement appropriate security measures including:

Physical Security

- Locked offices and filing cabinets
- Secure disposal of confidential waste
- Controlled access to premises

Electronic Security

- Password protection
- Multi-factor authentication where available
- Anti-virus protection
- Firewalls
- Secure backups
- Access controls

Staff Awareness

All councillors and employees shall receive appropriate data protection guidance and training.

10. Data Sharing

The Council shall only share personal data when:

- Required by law
- Necessary for Council functions
- The individual has consented
- There is another lawful basis under UK GDPR

Where personal data is shared with third parties, appropriate agreements or contracts shall be in place where required.

11. Data Processors

Where third-party organisations process data on behalf of the Council, the Council shall ensure:

- Appropriate due diligence is undertaken.
 - Written contracts are in place containing UK GDPR-compliant clauses.
 - Adequate security measures are maintained.
-

12. Retention and Disposal

Personal data shall only be retained for as long as required.

The Council shall:

- Maintain a Retention and Disposal Schedule.
 - Securely destroy paper records when no longer required.
 - Permanently delete electronic records in accordance with agreed procedures.
-

13. Data Breaches

Reporting

All actual or suspected personal data breaches must be reported immediately to the Town Clerk.

Investigation

The Council shall assess:

- Nature of the breach
- Categories of data involved
- Number of individuals affected
- Potential impact and risks

ICO Notification

Where required, breaches shall be reported to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

Affected Individuals

Where there is a high risk to individuals' rights and freedoms, affected persons will be informed promptly.

14. Councillors' Responsibilities

Councillors must:

- Only access information required for Council duties.
- Keep personal data confidential.
- Use Council-approved systems where possible.

- Store information securely.
- Promptly report data breaches.
- Delete or return Council information when no longer required.

Personal data held on private devices must receive appropriate protection and be deleted when no longer needed.

15. Employee Responsibilities

Employees must:

- Follow this policy and related procedures.
- Handle personal data securely.
- Maintain confidentiality.
- Attend relevant data protection training.
- Report suspected breaches immediately.

Failure to comply may result in disciplinary action.

16. Privacy Notices

The Council shall maintain suitable Privacy Notices explaining:

- What information is collected.
- Why it is collected.
- How it is used.
- Who it may be shared with.
- Retention periods.
- Individuals' rights.

Privacy Notices shall be available on the Council website and provided where appropriate.

17. Monitoring and Compliance

The Town Clerk shall monitor compliance with this policy by:

- Reviewing procedures regularly.

- Maintaining records of processing activities where required.
 - Investigating incidents.
 - Providing advice and training.
-

18. Review

This policy shall be reviewed:

- Annually;
 - Following significant legislative changes;
 - Following major organisational changes; or
 - After a significant data breach.
-