STOTFOLD TOWN COUNCIL

INFORMATION AND DATA PROTECTION POLICY – 2025

VERSION 2

1. Purpose and Scope

This policy sets out how the Council protects and manages its information assets, including personal data, in line with the UK General Data Protection Regulation (GDPR), Data Protection Act 2018, and sector best practice (JPAG, NALC, SLCC).

It applies to all councillors, staff, contractors, and volunteers handling Council information, whether held electronically or on paper.

2. Legal and Regulatory Framework

The Council is committed to complying with:

- UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- AGAR requirements (including Assertion 10: Digital and Data Compliance)
- Relevant guidance from the Information Commissioner's Office (ICO), JPAG, NALC, and SLCC

3. Roles and Responsibilities

- The Clerk is responsible for day-to-day information security and data protection.
- All users must follow this policy and report any security incidents or data breaches immediately.
- Data Protection Officer (DPO):
  As of 2025, parish and town councils are exempt from the legal requirement to appoint a DPO under Section 7 of the Data Protection Act 2018. However, the Council may appoint a DPO as good practice. If appointed, the DPO will advise on data protection obligations, monitor compliance, and act as the contact point for the ICO.

4. Data Protection Principles

The Council will ensure that personal data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Kept only as long as necessary
- Processed securely

5. Information Security

The Council will ensure:

- Confidentiality: Information is accessible only to authorised users.
- Integrity: Information is accurate and complete.
- Availability: Information is accessible to authorised users when required.

6. Asset Inventory and Classification

- The Council maintains an up-to-date inventory of all information assets, including:
  - Computers, laptops, and mobile devices

    - Software and cloud services
    - Paper records
    - Backups and portable media
- Each asset is classified by sensitivity and protected accordingly.

7. Access and User Management

- Access to information is restricted to those who need it for Council business.
- All devices and systems are password-protected with strong, unique passwords.
- Access is removed promptly when a user leaves or changes role.
- Use of council-owned email accounts (preferably .gov.uk) is mandatory for Council business.

8. Data Handling, Retention, and Sharing

- Personal data is collected, used, and retained only as necessary for Council purposes, in line with the Council's Privacy Notice and Document Retention Policy.
- Data is not shared with third parties except as required by law or with consent.
- Backups are taken regularly, stored securely (including offsite/cloud), and tested periodically.
- Data is securely deleted or destroyed when no longer required.

9. Digital and Data Compliance (AGAR Assertion 10)

The Council will:

- Comply with all relevant digital and data protection laws, including the UK GDPR and Data Protection Act 2018.
- Maintain an up-to-date inventory of all digital assets and ensure appropriate security controls are in place.
- Restrict access to digital systems to authorised users and require the use of council-owned email accounts for council business.
- Encrypt sensitive data and ensure regular, secure backups.
- Conduct regular risk assessments and provide ongoing training to all users.
- Maintain clear procedures for reporting and responding to data breaches or cyber incidents.
- Review digital and data compliance annually and as part of the AGAR process.

10. Technical and Physical Security

- All computers are protected by up-to-date anti-virus and firewall software.
- Regular software and security updates are applied.
- Data is encrypted where possible, especially on portable devices and backups.
- Paper records are stored in locked cabinets or rooms.
- Devices and media are securely wiped or destroyed before disposal.
- Security Policy implemented and maintained, including Multi-Factor Authentication.

11. Incident Management and Breach Reporting

- All security incidents, including data breaches, must be reported immediately to the Clerk (or DPO, if appointed).
- Serious incidents are reported to the Council and, where required, to the Information Commissioner's Office (ICO) within 72 hours.
- The Council maintains a log of all incidents and reviews lessons learned.

12. Training and Awareness

- All staff, councillors, and volunteers receive regular training on information security and data protection.
- The policy is reviewed and updated at least every two years, or sooner if required by law or following an incident.

13. Review and Audit

- The Council conducts regular data audits and risk assessments.
- Compliance with this policy is monitored, and improvements are made as needed.
- This policy will be reviewed every two years, or more frequently if required by changes in legislation or following a security incident.

14. Related Policies

This policy should be read in conjunction with:

- Privacy Notice
- Document Retention Policy
- Information Security Asset Inventory

Glossary

- AGAR — Annual Governance and Accountability Return
- DPO — Data Protection Officer
- GDPR — General Data Protection Regulation
- ICO — Information Commissioner's Office
- JPAG — Joint Panel on Accountability and Governance
- NALC — National Association of Local Councils
- SLCC — Society of Local Council Clerks

Revision History:

Version	Date	Notes
1	March 2025	Replaced the previous policy - Information and Data Protection Policy – 2018
2	November 2025	Review and merged with information security policy to adhere to new AGAR assertion 10 Digital and Data Compliance