West Swindon Parish Council

IT and Digital Compliance Policy 2025

Adopted: May 2025

1. Purpose & Scope

This policy sets out the standards and procedures governing the use of information technology and digital systems by West Swindon Parish Council. It aligns with Assertion 10 of the Joint Practitioners' Guide 2025, ensuring that the Council manages its digital services, email systems, website, and data securely, efficiently and in compliance with UK GDPR, the Data Protection Act 2018, and accessibility legislation.

This policy applies to all Councillors, staff, contractors, and volunteers who use or have access to the Council's IT systems, emails, or digital information. *(Noted that volunteers do not currently directly access the Parish Council's IT systems)*

2. Governance, Roles & Accountability

The Parish Council is the data controller for all information it holds. The Clerk is responsible for overseeing IT systems, ensuring compliance with data protection and security standards, maintaining an IT asset register, and liaising with external providers.

West Swindon Parish Council manages its IT systems and website in-house, with domain registration, hosting and technical support secured through external providers. Six members of staff have day-to-day access to Parish Council computers and official email accounts.

3. Official Email & Communication

All official communications must use Council-provided email addresses under the westswindon-pc.gov.uk domain. Personal email accounts must not be used for Council business. Emails must be professional, factual, and compliant with data protection principles. Staff will use standardised signatures.

Email accounts will be monitored for compliance with policy, and records will be retained in line with approved retention schedules. West Swindon Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security. The Clerk can assist any users with password issues or resets. Councillors are provided with westswindon-pc.gov.uk email addresses and are requested to use these for any Parish Council related correspondence to maintain accountability and transparency.

4. Website Accessibility & Digital Presence

The Parish Council maintains its website on the official .gov.uk domain. The website must comply with the Web Content Accessibility Guidelines (WCAG 2.2 AA) standard and include a clear accessibility statement. The Support Officer within the Parish Team oversees website content, accuracy, and updates.

5. Device, Access & Password Controls

All devices used for Council work must be password protected and encrypted where possible. Staff must not install unapproved software or alter security configurations. Two-factor authentication should be used on key systems e.g. SharePoint or Microsoft from a personal computer

6. Data Management, Security & Backups

Council data must be securely stored, regularly backed up, and only accessible to authorised users. Backups must be encrypted and tested periodically. Data retention and disposal must follow statutory requirements.

7. Training, Awareness & Review

All staff and Councillors will be encouraged to access training on this policy and cybersecurity awareness. This policy will be reviewed annually or sooner if technological or regulatory changes require it.

8. Incident Management & Breach Reporting

Any suspected or actual data breaches must be reported immediately to the Clerk. Incidents will be investigated, documented, and, where necessary, reported to the ICO within 72 hours.

9. Compliance & Enforcement

Compliance with this policy is mandatory. Failure to follow its provisions may result in disciplinary action or withdrawal of IT access. Serious breaches may be referred to external authorities where required by law.

This document should be read alongside the Parish Council's Data Protection Policy, Retention Policy, and Social Media Policy.