SHALDON PARISH COUNCL

INFORMATION TECHNOLOGY (IT) POLICY

ADOPTED 23 SEPTEMBER 2025
NEXT REVIEW MAY 2026

1. Purpose

This policy sets out the rules and procedures for the use of IT systems, email and digital resources by councillors, staff, and volunteers of Shaldon Parish Council. It ensures security of information, legal compliance, cyber security and effective operation of Council business.

2. Scope

This policy applies to all users of council-owned IT equipment, personal devices used for council business, council email accounts and the Council website.

3. Policy Statements

a Authority Owned Email Accounts

- All Council business must, wherever practicable, be conducted using Council-owned email accounts (e.g. name.surname@shaldonparishcouncil.gov.uk).
- Personal email accounts must not be used for confidential Council business.
- Email accounts and digital data are to be managed in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA).

b Data Protection and Security

- Personal data held by the Council must be protected by appropriate technical and organisational measures.
- Data must be stored securely, accessed only by authorised individuals and shared only for legitimate Council purposes.
- Council records must be retained and disposed of according to legal requirements.
- Users must ensure devices used for Council business are password protected and secure.

c Cyber and Device Security

- All devices used for Council business (whether Council-owned or personal) must:
- Be protected by strong passwords or biometric security.
- Be kept updated with latest operating system and security patches.

- Use screen locks or automatic timeouts when not in use.
- Not be left unattended or unsecured in public locations.
- Passwords must not be shared or reused across systems.
- Passwords must not be shared or reused across systems.
- Only authorised users may access Council systems and data.
- Users must be vigilant to phishing, suspicious emails and online scams and report any such incidents to the Clerk/RFO immediately.
- Any suspected cyber-attack, data breach, or loss/theft of a device containing Council data must be reported to the Clerk/RFO without delay. The Clerk/RFO will determine whether notification to the ICO is required.

d **Website Management and Accessibility**

- The Council's website is managed to ensure compliance with the Public Sector Bodies (websites and Mobile Applications) (No.2) Accessibility Regulations 2018 and meets Web Content Accessibility Guidelines (WCAG) 2.2 AA standard.
- Required documents and information are published in accessible formats and an accessibility statement is maintained and reviewed regularly.

e **Use of Personal Devices**

- Personal devices may be used or Council business only if they comply with this policy, including secure passwords, regular updates, and the secure deletion of Council data when no longer required.
- Council data should not be stored on unencrypted or public cloud services without authorisation.

f **Information Management**

- All Council records and communications must be retained in accordance with Council retention policies and relevant legislation (e.g. Freedom of Information Act 2000, Local Government Act 1972).
- Users must not use Council IT systems or resources for personal or non-Council business.

g **Training and Awareness.**

The Clerk/RFO is responsible for ensuring all users are aware of this policy and receive appropriate data protection and IT/cyber security training as required.

Cyber security advice and resources will be shared with staff, councillors and volunteers annually or when significant risks arise.

h **Compliance and Review**

Breaches of this policy may result in disciplinary action and ust be reported to the Clerk/RFO and where relevant to the Information Commissioner's Office.

This policy will be reviewed every three years, or sooner if required by changes in legislation, guidance, or best practice.

Adopted 23 September 2025
Next Review May 2026