Swinfen and Packington Parish Council

Information Technology (IT) Acceptable Use and Security Policy

Adopted: 13 May 2026

Review Date: May 2027

Responsible Officer: Parish Clerk

1. Purpose

This policy sets out the requirements for the secure, lawful, and appropriate use of information technology (IT) hardware, software, systems, and data used for Burntwood Town Council business. It is intended to ensure compliance with **Assertion 10 of the Annual Governance and Accountability Return (AGAR)**, which requires the Council to have proper arrangements for the use of digital technology, including cybersecurity, in place.

2. Scope

This policy applies to:

- All councillors
- All employees (including temporary and part-time staff)
- Contractors and consultants
- Volunteers
- Any other individuals granted access to Council IT systems or data

The policy covers all Council-owned or Council-managed IT equipment and systems, and any personal devices used to access Council information.

3. Legal and Regulatory Framework

This policy supports compliance with, but is not limited to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Local Government Transparency Code

4. Acceptable Use of IT Equipment and Systems

4.1 Council IT equipment and systems are provided for the purpose of conducting official Council business.

4.2 Limited incidental personal use is permitted provided that it:

- Does not interfere with Council duties
- Does not incur additional cost to the Council
- Does not breach this or any other Council policy

4.3 Users must not:

- Use Council systems for unlawful, fraudulent, or defamatory purposes
- Access, create, store, or transmit offensive, obscene, or discriminatory material
- Circumvent security controls or monitoring systems
- Install unauthorised software or hardware

5. Hardware Security

5.1 Council-owned devices (including computers, laptops, tablets, and mobile phones) must be:

- Used in accordance with this policy
- Protected from loss, theft, or damage
- Secured with passwords, PINs, or biometric protection where available

5.2 Devices must not be left unattended in public places unless securely locked.

5.3 Loss or theft of any Council device must be reported immediately to the Parish Clerk & Chairman of the Parish Council.

6. Software and Licensing

6.1 Only software that is:

- Lawfully obtained
- Properly licensed
- Approved by the Council or Parish Clerk
  may be installed or used on Council devices.

6.2 Users must not download or use pirated, cracked, or unauthorised software.

6.3 Software updates and security patches must be applied promptly where updates are managed by the user.

7. Access Control and Passwords

7.1 Access to Council systems and data must be limited to authorised users only.

7.2 Users must:

- Use strong, unique passwords
- Keep passwords confidential
- Not share accounts or login credentials

7.3 Multi-factor authentication must be used where available.

8. Data Protection and Information Security

8.1 Council data must be:

- Used only for legitimate Council purposes
- Stored securely
- Protected from unauthorised access, alteration, or disclosure

8.2 Personal data must be handled in accordance with the Council's Data Protection Policy.

8.3 Council information must not be stored on personal devices or personal cloud services unless expressly authorised and appropriately secured.

9. Email, Internet, and Cloud Services

9.1 Council email accounts must be used for Council business.

9.2 Users must remain vigilant against phishing, malware, and other cyber threats and must not:

- Open suspicious links or attachments
- Provide passwords or sensitive information in response to unsolicited requests

9.3 Only Council-approved cloud and file-sharing services may be used to store or share Council information.

10. Remote and Home Working

10.1 When working remotely, users must:

- Ensure screens are not visible to unauthorised persons
- Use secure internet connections
- Log out of systems when not in use

10.2 Public or unsecured Wi-Fi networks must not be used for accessing sensitive Council systems unless a secure connection (such as a VPN) is in place.

11. Monitoring and Compliance

11.1 The Council reserves the right to monitor the use of its IT systems where lawful and proportionate to do so.

11.2 Any suspected breach of this policy, data breach, or cybersecurity incident must be reported immediately to the Clerk.

12. Breaches of Policy

12.1 Breaches of this policy may result in:

- Withdrawal of access to IT systems
- Disciplinary action (where applicable)
- Referral to external authorities where a legal offence is suspected

13. Review and Approval

This policy will be reviewed at least annually, or sooner if required by changes in legislation, guidance, or technology.