IT, Digital Communications & Devices Policy

Version	Date of Adoption	Minute Reference	Review Date	Originator/Reviewer
2026	23.3.2026	2026-101	2027	G White

IT, Digital Communications & Devices Policy

1. Purpose & Scope

This policy supports the Council's obligations under Assertion 10: Digital & Data Compliance in the Annual Governance and Accountability Return (AGAR). It establishes standards for the secure use, protection, management, retention and disposal of digital data, IT systems, devices and communications.

This policy applies to councillors, officers, contractors and volunteers using **parish-council-owned devices, systems and digital services** for official parish council business.

2. Roles & Responsibilities

Council

• Retains ownership and control of Council IT infrastructure, digital systems and domains.
• Ensures adequate resources are provided to maintain appropriate cyber security and data governance arrangements.
• Reviews this policy at least annually.

Clerk / Responsible Financial Officer

• Implements and monitors compliance with this policy.
• Oversees device allocation, security arrangements and incident reporting.
• Liaises with the Council's IT provider and reports significant breaches to the Council.

Councillors, Staff and Authorised Users

• Must comply with this policy and use Council equipment and systems responsibly.
• Must ensure devices and information remain secure at all times.

IT Provider

• Maintains firewalls, antivirus protection, backups, patching and security monitoring in accordance with contractual arrangements.

3. Council Email & Digital Communications

All official Council communications must be conducted using Council-issued email accounts or authorised digital systems.

Personal email accounts must not be used for Council business except in exceptional and documented circumstances approved by the Clerk.

Strong passwords and multi-factor authentication must be used where available.

4. Data Protection, Privacy & Security

The Council is a Data Controller under UK GDPR and the Data Protection Act 2018.

Personal data must be processed lawfully, securely and only for authorised Council purposes.
Access to sensitive information must be restricted to those with a legitimate need.

Regular backups must be undertaken in accordance with the Council's IT support arrangements.

All actual or suspected data breaches or cyber incidents must be reported to the Clerk immediately.

5. Website, Accessibility & Online Publication

The Council shall retain control of its website domain and digital presence.
All statutory publications must be accurate, up-to-date and accessible.

The Council will seek to comply with recognised accessibility standards, including WCAG guidance, where reasonably practicable.

6. Use of Council Equipment, Devices & Remote Working

WPC-owned devices, including **mobile phones, tablets, laptops and desktop computers**, are provided strictly for authorised parish council business.

All users are responsible for the proper care, security and appropriate use of Council devices and must not share equipment with unauthorised persons or use devices for personal, political or commercial purposes.

Devices must be maintained with parish-council-approved security configurations, software updates and protective measures.

Any loss, theft, damage or suspected security incident must be reported to the Clerk immediately.

The Parish Council reserves the right to monitor usage of its devices and systems, in accordance with relevant legislation and internal procedures, and may recover Council-owned equipment at any time.

Devices must be kept physically secure when off-site and remote access to Council systems must only take place via secure, authorised connections.

All equipment must be returned promptly upon cessation of office, employment or authorised use.

7. Social Media & Online Conduct

Official Council social media accounts must remain under Council control.

Only authorised persons may publish content on behalf of the Council.

Digital messaging platforms must not be used for formal decision-making or to conduct Council business outside lawful meeting arrangements.

8. Training, Awareness & Policy Review

Councillors and staff will receive appropriate training on information security, digital governance and data protection responsibilities.

This policy will be reviewed annually, or sooner if required by legislative, technological or organisational change.

9. Non-Compliance

Failure to comply with this policy may result in withdrawal of device access, internal disciplinary action, or referral to regulatory authorities where appropriate.

10. Review & Amendment

This policy may be amended by resolution of the Council and will be reviewed at least annually to ensure continued effectiveness and compliance with statutory obligations.

Prepared by:
Mrs Gaynor White
Clerk to Worplesdon Parish Council