Worplesdon Parish Council

IT / Digital & Data Policy

Adopted: [Date] | Next review: [Date]

1. Purpose & Scope

This policy supports the Council's obligations under Assertion 10: Digital & Data Compliance in the Annual Governance & Accountability Return (AGAR).
It sets standards for the use, protection, management, retention, and disposal of digital data, IT systems, and communications.
It applies to councillors, officers, contractors, volunteers, and all devices used for Council business.

2. Roles & Responsibilities

Council: Own/control domain(s) used for Council email and website; maintain IT infrastructure; review annually.
Clerk/Responsible Officer: Implement policy, manage security, report breaches.
Councillors/Users: Comply with policy, use approved accounts, keep devices secure.
IT Provider: Maintain firewalls, antivirus, backups, and security controls.

3. Council Email & Communications

All official communications must use Council email addresses (e.g. clerk@worplesdon-pc.gov.uk). Personal accounts must not be used for Council business except in exceptional, documented circumstances. Two-factor authentication and strong passwords are required.

4. Data Protection, Privacy & Security

The Council is a Data Controller under UK GDPR. Sensitive data must be handled securely, access limited, and backups taken regularly. All suspected breaches must be reported immediately to the Clerk.

5. Website, Accessibility & Online Publication

The Council must control its domain (preferably .gov.uk) and comply with WCAG 2.2 AA standards. All statutory documents must be accessible and current.

6. Use of Council Equipment, Devices & Remote Working

Devices supplied remain Council property and must be returned upon role change or leaving. Remote access must be via secure, approved systems.

Use of Personal Devices (BYOD – "Bring Your Own Device")
BYOD refers to councillors, staff, or volunteers using their own personal equipment – such as laptops, tablets, or mobile phones – to access or store Council emails, documents, or data.
If personal devices are used, they must:

- Have strong passwords and, if possible, encryption (BitLocker, FileVault).
- Run current antivirus and security updates.
- Not store or back up Council data to personal clouds (e.g. iCloud, Google Drive).
- Connect securely.
- Report any loss or compromise to the Clerk immediately.
- Delete all Council data when leaving the Council.

The Council may issue Council-owned equipment to avoid BYOD risks. Devices must always be physically secure when offsite.

7. Social Media & Digital Communications

Official accounts must be Council-controlled. Only authorised persons may post. WhatsApp or similar tools must not be used for decision-making.

8. Training, Awareness & Review

All members and staff must receive regular IT security and GDPR training. Policy reviewed annually or after major legislative or technological changes.

9. Non-Compliance & Disciplinary Measures

Breaches may result in disciplinary action or referral to the ICO for serious incidents.

10. Review & Amendment

This policy may be amended by Council resolution. Review at least annually or after major changes.

Prepared by: Mrs Gaynor White, Clerk to the Council