

Laverstoke and Freefolk Parish Council

Information Technology (IT) Policy

1. Purpose of this Policy

This IT Policy sets out how Laverstoke & Freefolk Parish Council manages, secures, and uses information technology, digital systems, and data.

Its purpose is to ensure:

- Compliance with AGAR Assertion 10 (Digital & Data Compliance)
- Compliance with data protection legislation (UK GDPR & Data Protection Act 2018)
- Security and integrity of council-owned information
- Clear guidance for councillors, staff, and contractors

This policy applies to:

- All councillors
- The Clerk / RFO
- Any volunteers or third parties handling council data

2. Council-Owned Domain, Email & Digital Accounts

The council uses a domain that it owns and controls: *laverstokeandfreefolk.org.uk*

2.1 Email Accounts

- All council business must be conducted through council-issued email accounts
- Personal email accounts **must not** be used for council business.
- Access to council email accounts must be protected by:
- Strong passwords
- Multi-factor authentication (MFA), where available

2.2 Account Control

- Accounts are created, monitored and disabled by the Clerk (or delegated officer).
- When a councillor or member of staff leaves
- Their council email account is closed.
- Data is transferred to the Clerk where appropriate.

3. Devices and Equipment

3.1 Council-Owned Devices

Where the council issues IT equipment (laptops, tablets, phones), the following applies:

- Devices must only be used for council business.
- Devices must be password-protected.
- Devices must be kept updated with security patches.
- Antivirus or equivalent protection must be active.

3.2 Personal Devices (BYOD)

If personal devices are used for council business:

- They must be password-protected.
- They must have up-to-date security updates.
- Council data must be stored only in council-approved applications (e.g., council email, council-managed cloud storage).
- If a device is lost or stolen, it must be reported immediately to the Clerk.

The council reserves the right to require the secure deletion of council data from personal devices when necessary.

4. Data Storage, Access & Backup

4.1 Storage Locations

Council data must be stored:

- On council-managed cloud storage: Laverstoke & Freefolk PC One Drive
- On council-owned devices where appropriate
- Paper records must be held securely

Data **must not** be stored on:

- Unencrypted USB sticks
- Personal cloud accounts
- Social media accounts (other than public postings)

4.2 File Access

- Access to digital files is authorised by the Clerk.
- Shared drives must follow a clear folder structure.

4.3 Backups

Backup arrangements:

- Cloud-based systems with automatic backup

5. Data Protection & GDPR

The council maintains:

- A Data Protection Policy
- An Information Asset Register / Data Audit
- A Privacy Notice – see website
- A Data Retention Schedule

All councillors and staff must comply with:

- UK GDPR principles
- Confidentiality obligations

Personal data must not be shared via personal email or unsupported applications.

6. Website & Accessibility

The council website must:

- Comply with WCAG 2.2 AA accessibility standards
- Publish a valid, reviewed Accessibility Statement
- Publish transparency and financial information as required by law
- Accessibility checks must be carried out at least annually.

7. Security Requirements

7.1 Passwords

- Must be strong and not reused across services.
- Should be changed if a breach is suspected.
- Must not be shared.

7.2 Updates & Patching

- Devices and software must be updated promptly.
- Unsupported software must not be used.

7.3 Network Security

- Public Wi-Fi should be avoided when accessing sensitive information unless a secure connection (e.g., VPN) is used.

8. Incident Reporting

Any of the following must be reported immediately to the Clerk:

- Lost or stolen devices

- Suspected hacking or phishing
- Accidental sharing of personal data
- Website or email security issues

Data breaches must be logged and managed in accordance with GDPR requirements.

9. Leaving the Council

When a councillor or staff member leaves:

- Access to council email and digital services is removed.
- Any council data on personal devices must be deleted.
- Council-owned devices must be returned.
- Handover of files or information must be completed.

10. Review and Approval

This IT Policy was approved by Laverstoke & Freefolk Parish Council on:

Date: 9.12.25

This policy will be reviewed annually in May or sooner if required.