Information Technology (IT) Policy

Dawley Hamlets Parish Council

Created: February 2026

DRAFT

1. Purpose

This policy sets out how Dawley Hamlets Parish Council manages, uses, and protects its information technology systems. It ensures:

- compliance with UK GDPR and the Council's Data Protection Policy
- secure and efficient working practices
- protection of council data, equipment, and reputation
- clarity for councillors, staff, and volunteers about their responsibilities

This policy should be read alongside the Council's Standing Orders, Code of Conduct, Data Protection Privacy Policy, and Social Media Policy.

---

2. Scope

This policy applies to:

- All councillors
- The Clerk/RFO and any other employees
- Volunteers or contractors who access council systems or data

It covers all devices, accounts, software, and data used for council business, whether owned by the Council or personally owned.

---

3. Roles and Responsibilities

The Council

- Approves this policy and reviews it annually.
- Ensures adequate budget provision for secure IT systems and support.
- Ensures that IT arrangements support transparency, accessibility, and good governance.

Clerk / Responsible Financial Officer

- Acts as the operational Data Controller for day-to-day purposes.
- Manages council-owned devices, accounts, and backups.

- Ensures compliance with GDPR and the Council’s Data Protection Policy.
- Maintains secure storage of council records, including digital archives.
- Reports any data breaches to the Council and, where required, the ICO.

Councillors

- Use council systems responsibly and in line with this policy.
- Protect confidential and sensitive information.
- Use official council email accounts for all council business.
- Report any IT concerns or incidents promptly to the Clerk.

---

4. Devices and Equipment

Council-Owned Devices

Where the Council provides devices (e.g., laptop, tablet, phone):

- Devices must be password-protected.
- Automatic updates must be enabled.
- Anti-virus and security software must be active.
- Devices must not be shared with family or friends.
- Devices must be returned to the Clerk when a councillor leaves office or an employee leaves employment.

Personal Devices

Where councillors or staff use their own personal devices (such as a personal laptop, tablet, or mobile phone) to carry out council business:

- The device must be password-protected.
- It must have up-to-date security and anti-virus software.
- Council documents must only be stored in approved locations (e.g., OneDrive/SharePoint), not saved directly onto the device.
- If the device is lost, stolen, or compromised, the Clerk must be informed immediately.
- Personal devices must not be shared with family members if they contain or access council information.

DRAFT

5. Accounts, Passwords, and Access

Email Accounts

- All councillors and staff must use their official **@dawleyhamlets-pc.gov.uk** email address for council business.
- Personal email accounts must not be used for council work.
- Email accounts are closed when a councillor leaves office or an employee leaves employment.

Passwords

- Must be strong (a mix of letters, numbers, symbols).
- Must not be shared.
- Must be changed if a breach is suspected.
- The Clerk may require password resets following a security incident.

Access Control

- Access to systems is granted only as needed for the role.
- Administrative access is restricted to the Clerk and authorised support providers.
- Former councillors and staff must not retain access to any council systems.

DRAFT

---

6. Data Storage, Backup, and Retention

- Council documents must be stored in approved cloud storage (e.g., OneDrive/SharePoint) or on council-owned devices.
- The Clerk must ensure regular backups of key documents.
- USB sticks should be avoided unless encrypted.
- Data must be stored securely and retained only for as long as necessary in line with UK GDPR.
- Records required for audit or statutory purposes must be stored securely and accessibly.

---

7. Software and Applications

- Only approved software may be installed on council-owned devices.
- Unlicensed or pirated software is strictly prohibited.

DRAFT

- Cloud services (e.g., Dropbox, Google Drive) may only be used if they are secure, reputable and compliant with UK GDPR.
- The Clerk must maintain a record of software licences where applicable.

---

8. Internet and Email Use

- Council email must be used professionally and in line with the Code of Conduct.
- Emails must be written with awareness that they may be subject to FOI requests.
- Offensive, discriminatory, or inappropriate content is prohibited.
- Councillors must not use council systems for political campaigning.
- Personal use of council devices must be minimal and appropriate.

---

9. Cybersecurity

- All users must take reasonable steps to protect council data.
- Phishing emails must be reported to the Clerk.
- Links and attachments should only be opened if the sender is trusted.
- Public Wi-Fi should not be used for accessing confidential information unless a secure VPN is used.
- The Clerk may require cybersecurity training where appropriate.

---

10. Social Media and Online Presence

- The Council's social media accounts may only be accessed by authorised persons.
- Personal social media must not be used to conduct official council business.
- Councillors must follow the Council's Social Media Policy.
- Content posted on behalf of the Council must be factual, neutral, and in line with council decisions.

---

11. Data Protection and Confidentiality

- All users must comply with the Council's Data Protection Privacy Policy and UK GDPR.
- Personal data must only be accessed for legitimate council purposes.
- Confidential information must not be shared outside authorised channels.

- Documents containing personal data must not be stored on unapproved devices or platforms.

---

12. Incident Reporting

Users must report immediately to the Clerk:

- Lost or stolen devices
- Suspected data breaches
- Malware or suspicious activity
- Unauthorised access to accounts
- Any accidental disclosure of personal data

The Clerk will manage any suspected data breach in line with UK GDPR requirements, including notifying the ICO where required.

---

13. Disposal of Equipment

- Old devices must be securely wiped before disposal.
- Storage media must be destroyed or professionally erased.
- Disposal must comply with the Council's Retention and Disposal Schedule.

---

14. Review

This policy will be reviewed annually or sooner if:

- Legislation changes
- New systems are introduced
- A significant incident occurs
- The Council's governance arrangements change

DRAFT