Information Technology (IT) Policy

Assertion 10 Compliance

Adopted: January 2026

Review Date: January 2027

1. Purpose

This policy explains how councillors, the clerk, and any other staff should conduct Council business in a secure and legal way when using IT equipment and software. It covers both Council-owned and personal equipment used for Council business.

This policy supports compliance with Assertion 10 of the Annual Governance Statement as set out in the Practitioners' Guide.

2. Scope

This policy applies to:

- All councillors
- The Parish Clerk and any employees
- Contractors and volunteers with access to Council IT systems
- Anyone using personal devices for Council business

3. Email

3.1 Official Email Accounts

All Council business must be conducted using official Council email addresses on the Council's domain (figheldeanparishcouncil.gov.uk). Personal email accounts (such as Gmail, Outlook, Yahoo) must not be used for Council business.

3.2 Email Security

Email users must:

- Use strong, unique passwords for email accounts
- Enable two-factor authentication where available
- Be vigilant about phishing emails and suspicious attachments
- Not click on links in unexpected emails
- Report suspicious emails to the Parish Clerk
- Ensure sensitive information is only sent to intended recipients

3.3 Email Retention

Emails relating to Council business should be retained in accordance with the Council's retention schedule. The Parish Clerk is responsible for maintaining an archive of important Council correspondence.

4. Passwords

Strong passwords are essential for protecting Council information. All users must:

- Use passwords of at least 12 characters

- Include a mix of upper and lower case letters, numbers and symbols
- Not use easily guessable information (names, birthdays, common words)
- Use different passwords for different accounts
- Change passwords immediately if a breach is suspected
- Never share passwords with others
- Consider using a password manager

5. Use of Personal Devices

Where councillors or staff use personal devices (computers, tablets, phones) for Council business, they must:

- Keep the device's operating system and software up to date
- Use antivirus/security software
- Enable device encryption where possible
- Use a PIN, password or biometric lock on the device
- Ensure Council data is stored securely and backed up
- Delete Council data from personal devices when no longer needed
- Report any loss or theft of devices containing Council data immediately

6. Council-Owned Equipment

Where the Council provides IT equipment:

- Equipment must only be used for Council business
- Users must not install unauthorised software
- Equipment must be kept secure and not left unattended in public places
- Any faults or damage must be reported to the Parish Clerk
- Equipment must be returned when no longer needed

7. Data Backup

The Parish Clerk is responsible for ensuring that important Council data is regularly backed up. Backups should be:

- Performed at least weekly
- Stored securely, preferably in a different location or cloud service
- Tested periodically to ensure data can be recovered
- Protected with encryption where appropriate

8. Software and Licensing

All software used for Council business must be properly licensed. Pirated or unlicensed software must not be used. The Parish Clerk will maintain a record of software licenses.

9. Website

The Council website (figheldean.org) is a key public information resource. The Parish Clerk or designated person is responsible for:

- Keeping website content accurate and up to date
- Ensuring compliance with accessibility requirements (WCAG 2.2 AA)
- Maintaining website security (updates, secure hosting, SSL certificate)
- Publishing required transparency information

- Securing access credentials to the website

10. Social Media

If the Council uses social media:

- Official Council accounts must be clearly identified as such
- Posts must be factual and professional
- Personal opinions must not be expressed through official accounts
- Access credentials must be managed securely
- Councillors using personal social media should be aware that comments on Council matters may be seen as official statements

11. Security Incidents

Any IT security incident must be reported immediately to the Parish Clerk. This includes:

- Suspected virus or malware infection
- Loss or theft of devices
- Unauthorised access to systems or data
- Phishing attacks
- Any breach of this policy

The Parish Clerk will assess incidents and take appropriate action, including reporting to the ICO if a personal data breach has occurred.

12. Training

Councillors and staff will be made aware of this policy and will receive guidance on IT security as appropriate.

13. Review

This policy will be reviewed annually or following any significant IT changes or security incidents.

Document Control

Adopted by Council: January 2026