



Flitcham cum Appleton Parish Council

Information Technology Policy Internet & Email access for Employees & Councillors

1. Purpose

This IT Policy sets out the standards and responsibilities for the use of Flitcham Parish Council's information technology systems, email accounts, and digital data. Its aim is to ensure that all councillors and staff use IT securely, efficiently, and in accordance with data protection and legal requirements.

2. Scope

This policy applies to:

- All Parish Councillors
- Parish Clerk and any other staff or volunteers who use council IT systems or data
- Any devices (council-owned or personal) used to access council information

3. Acceptable Use

Councillors and staff must:

- Use Parish Council IT systems and data **only for legitimate council business**.
- Maintain professionalism in all written communication, including emails and social media.
- Keep login details and passwords **confidential**.
- Ensure that personal use of council devices or email accounts is **minimal and appropriate**.

The following are **not permitted**:

- Using council IT for political campaigning or personal gain
- Accessing, storing, or transmitting offensive, discriminatory, or illegal material
- Sharing council data or documents with unauthorised persons

4. Devices and Security

Councillors should report any **loss or theft** of a device containing council information immediately to the Clerk

- Devices used to access council data (laptops, tablets, phones) must be **password-protected**.
- Automatic screen lock must be enabled when devices are unattended.
- Security updates and antivirus software must be kept **up to date**.

5. Email and Communication

- Councillors must use their **official council email address** for all council business.
- Personal email accounts should **not** be used for council work.
- Emails and messages should be treated as official records and may be subject to **Freedom of Information** or **Data Protection** requests.

Be aware that emails can be disclosed under transparency and audit requirements

6. Data Protection and Confidentiality

- All councillors must comply with the **UK GDPR** and **Data Protection Act 2018**.
- Personal data (e.g. residents' names, contact details, complaints) must be kept **secure** and only used for council purposes.
- Information should not be stored indefinitely.

Confidential information must not be shared outside council meetings or with unauthorised parties.

7. Storage and File Sharing

- Council documents should be stored using approved, secure systems
- Files should be shared only with authorised users.
- Avoid downloading or storing confidential data on personal computers where possible.

8. Social Media and Online Conduct

When using social media:

- Be clear when expressing personal opinions — do **not** imply you speak on behalf of the council unless authorised.
- Do not post or share confidential council information.

Be respectful and avoid content that could damage the council's reputation.

9. Breaches of Policy

Any breach of this policy may lead to:

- Withdrawal of IT access privileges
- Reporting to the Monitoring Officer or Standards Committee for investigation
- Possible legal action in cases of data breach or misconduct

10. Review

This policy will be reviewed annually, or sooner if there are significant changes to legislation, technology, or council operations.

Signed: _____

Chair: Flitcham Parish Council

Date: _____

Clerk: _____