INFORMATION TECHNOLOGY

St Margaret's at Cliffe Parish Council

This policy ensures councillors securely use council-issued Chromebooks and Google Workspace for all council-related communication and file storage, safeguarding data through cloud-based services and strict device security measures.

Table of Contents

Date of policy	13th May 2025
Approving committee	St Margaret's at Cliffe Parish Council
Date of committee meeting	12th May 2025
Supersedes	Not applicable
Policy effective from	13th May 2025
Date for next review	May 2026

1. Introduction

This IT Policy is designed to ensure the proper use of technology by all Parish Councillors, protecting council data, systems, and devices from unauthorised access, while ensuring all communications and files are stored securely within our Google Cloud environment. All councillors are required to follow these guidelines when using council-provided equipment and services.

2. Scope

This policy applies to:

- All councillors provided with council-issued devices (Chromebooks).
- Use of Google Workspace applications, including Google Mail, Google Chat, and Google Drive.
- The handling of council data and communications, regardless of the device used (council-issued or personal devices).

3. Device and Account Security

Councillors are responsible for the security of their council-issued Chromebooks and personal devices used to access council emails or files. The following measures must be followed:

- **Secure Login**: Ensure login credentials (usernames and passwords) are kept confidential. Do not write down passwords or store them in places where they could be easily accessed by unauthorised individuals.
- **Lock Devices**: Chromebooks and any personal devices used to access council accounts must be locked when not in use. Set automatic screen locks after a period of inactivity.
- **Storage of Devices**: Devices should be stored securely when not in use. Do not leave Chromebooks or personal devices unattended in public or easily accessible areas where they could be stolen or tampered with.
- **Lost or Stolen Devices**: Report any lost or stolen devices immediately to the Parish Clerk to ensure accounts can be locked, and the device can be remotely wiped if necessary.

4. Use of Google Workspace

The Parish Council has adopted Google Workspace as its primary communication and collaboration platform. The following policies apply:

- **Email and Chat**: Councillors must use the Google Mail and Google Chat client / applications for all council-related communications. These tools are accessible through the Chromebook and other personal devices, but emails must not be downloaded or synced to local storage (such as local desktops or phone storage).
- **No Local Download of Emails**: To maintain security, councillors must not download council-related emails or attachments to local desktops, laptops, or mobile devices. Email access should remain cloud-based via the Google application or web interface only.

5. File Storage

Councillors must only save documents and files related to council business on the Google Drive cloud service:

- **Cloud-Only Storage**: All council-related documents and data must be saved and stored exclusively on Google Drive, ensuring they remain secure and accessible to authorised users.
- **No Local Storage**: Councillors should not download or store files on local device storage, such as Chromebook or personal device hard drives or external storage (e.g., USB drives).

6. Access Control

- **Account Access**: Councillors must ensure no unauthorised person can access their council email, Google Drive, or other Google Workspace applications. Do not share login credentials or allow others to use council-issued devices for personal or unauthorised use.

7. Device Maintenance

- **Software Updates**: Ensure your Chromebook is regularly updated to the latest software version to protect against security vulnerabilities.
- **Antivirus Protection**: Personal devices used to access council data should have up-to-date antivirus software installed where applicable, though Chromebooks come with built-in security measures.

8. Data Protection

Councillors must adhere to data protection principles when handling personal or sensitive council information:

- **Confidentiality**: Information should only be accessed by authorised users.
- **Data Breaches**: Any suspected data breach must be reported to the Parish Clerk immediately.

9. Accepting Electronic Correspondence

The Parish Council recognises the efficiency and environmental benefits of electronic communication. To maintain consistency, security, and professionalism, the following guidelines must be followed when accepting and handling electronic correspondence:

- **Official Email Use**: All council-related electronic correspondence must be conducted using the councillor's official Google Mail account. Councillors must not use personal email addresses for any council business.
- **Acknowledging Correspondence**: Councillors are expected to acknowledge receipt of important electronic correspondence in a timely manner. Where necessary, they should ensure the appropriate follow-up actions are taken and the relevant stakeholders are informed.
- **Confidential Information**: If electronic correspondence contains sensitive or confidential information, councillors must ensure it is handled securely. This includes:
    - Not forwarding emails to unauthorised individuals.
    - Storing any sensitive information on Google Drive, rather than downloading attachments or storing them locally.
- **Attachments and Links**: Councillors should exercise caution when opening attachments or clicking on links in emails from unknown or unverified sources. If an email appears suspicious or contains unfamiliar content, it should be reported to the Parish Clerk before opening.

- **Retention of Electronic Records**: All council-related emails and electronic correspondence should be stored in the Google Mail account for proper record-keeping.
- **Handling of Personal Data**: When receiving electronic correspondence that includes personal data, councillors must ensure they comply with GDPR regulations. Personal data should be handled securely and stored in Google Drive with appropriate access controls.

By adhering to these guidelines, councillors ensure electronic correspondence is managed efficiently, securely, and in accordance with the council's communication protocols.

10. Acknowledgement of Policy

By using council-issued Chromebooks or accessing council accounts through personal devices, councillors confirm they:

- Understand and agree to the terms of this IT Policy.
- Will not store or download emails, attachments, or files locally on devices.
- Will take appropriate measures to secure council-issued devices and personal devices used for council business.
- Will save all council-related files on Google Drive, avoiding local storage.