



COMPTON MARTIN PARISH COUNCIL

INFORMATION TECHNOLOGY AND CYBER SECURITY POLICY

Introduction

Compton Martin Parish Council (CMPC) recognises the importance of effective and secure information technology and email usage in supporting its business, operations, and communications. The risk of data theft, scams, and security breaches can have a detrimental impact on the council's systems, technology infrastructure, and reputation. As a result, Compton Martin Parish Council has created this policy to outline security measures to ensure information remains secure and protected.

Purpose of the IT Policy

- Protect Compton Martin Parish Council's data, systems, and infrastructure.
- Outline the protocols and guidelines that govern cyber security and IT resource use.
- Define acceptable and unacceptable use for council and personal use.
- Provide clear procedures for data management, device use, email use.
- Outline the council's process for policy violations.

Scope

This policy applies to all Compton Martin Parish Council councillors, employees, volunteers and suppliers with access to the council's electronic systems, networks, software, data, devices, and email accounts. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Acceptable Use of IT Resources and Email

Compton Martin Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted of IT resources, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical and legal standards, respect copyright and intellectual property rights, and avoid accessing inappropriate content or offensive content.

Device and Software Usage

CMPC provides authorised devices, software, and applications for work-related tasks for the Clerk. CMPC provides the Clerk with a computer, Microsoft package, antivirus software etc to enable them to undertake their responsibilities.

- Unauthorised installation of software, including personal software, is strictly prohibited.
- All council-owned and personal devices accessing council data must be password protected.
- Devices must be secured or locked when left unattended.
- Regular software and security updates must be applied to all council-owned devices.

Data Management and Security

- All sensitive and confidential data must be stored and transmitted securely using approved methods.

- Regular data backups must be performed for non-cloud-based services and secure data destruction methods must be used when necessary.

Network and Internet Usage

- CMPC networks and internet connections should be used responsibly and primarily for official purposes.
- Downloading and sharing copyrighted materials without proper authorisation is prohibited.

Email Security and Communication

- CMPC issues all councillors and clerk with official CMPC email accounts on the @comptonmartinparishcouncil.gov.uk domain.
- Email accounts provided by CMPC via the comptonmartinparishcouncil.gov.uk domain must be used for all council business.
- Council business-related emails must not be sent from personal email accounts.
- All Councillors and staff must comply with CMPC's IT and Cyber Security Policy and use of council-owned email accounts for all official business. These policies ensure that communications are conducted in a manner consistent with the Council's standards and legal obligations.
- Emails must be professional and respectful.
- Be cautious with attachments and links to avoid phishing and malware. Verify the legitimacy of email senders and be cautious of suspicious emails and attachments, before clicking on links.

Password and Account Security

- Users are responsible for maintaining the security of their accounts and passwords.
- Passwords must be strong and changed regularly.
- Passwords must not be shared with others.

Mobile Devices and Remote Working

Council-issued mobile devices (such as laptops) must be secured with passcodes and/or biometric authentication.

Retention and Archiving

- Emails must be retained and archived in accordance with legal and regulatory requirements.
- Regularly review and delete unnecessary emails to maintain an organised inbox.
- Councillor email accounts are deleted and no archive kept where an elected Member (Councillor) ceases to be a Councillor.

Reporting Security Incidents

All suspected security breaches or incidents must be reported immediately to the Clerk and will be dealt with according to CMPC's Data Protection and Data Security Policy.

Training and Awareness

CMPC will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

Compliance and Consequences

Breach of this policy may result in the suspension of IT privileges and further consequences including disciplinary action in the case of employees, and the Code of Conduct processes for Councillors, as deemed appropriate.

Policy Review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technological trends and security measures, JPAG requirements and other externally appropriate requirements.

Contacts

For IT-related enquiries or assistance, users can contact the clerk.

All staff and councillors are responsible for the safety and security of CMPC's IT and email systems. By adhering to this IT and Email Policy, Compton Martin Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.