

Chepping Wycombe Parish Council – IT Security & Acceptable Use Policy

This policy applies to **all staff members and councillors** of Chepping Wycombe Parish Council. Some elements are relevant only to members of staff using council-issued digital devices, whilst other elements apply only to councillors using their own personal devices to conduct council business. Several items apply to both staff and councillors – these are clearly marked within the document.

The policy sets out the rules for secure and responsible use of the Council's IT systems, data, and digital communications.

Policy Items Applicable to CWPC Staff and Councillors

1. Passwords

- **Creation & Format:** Passwords must be at least 8 characters and include upper- and lower-case letters, numbers, and special characters.
- **Confidentiality:** Passwords are strictly personal and must not be shared.
- **Forgotten or Compromised Passwords:** Staff or councillors must immediately notify the Clerk if they suspect their password has been compromised.
- **Document Protection:** Passwords for protected documents must be transmitted separately (e.g. by phone call, not email).
- **Multi-Factor Authentication (MFA)** should be in place for all relevant staff.

2. Use of Public WiFi

- When using public Wi-Fi, staff and councillors using their council emails must use a VPN (Virtual Private Network).

3. Mobile Phone Texting / SMS

- Neither staff nor councillors should send official Council communications via SMS or text message.
- All official communications must be via email or via postal correspondence.

4. Email Use

- Emails must be written professionally and may be treated as formal records.
- Staff and councillors must not make unauthorised commitments on behalf of the Council.
- Business-critical information must not be stored solely in inboxes; it should also be saved to shared systems.
- Out-of-office replies for both staff and councillors should include alternative contacts, and one of these should be the Clerk of the Council.

5. USB Drives & Portable Devices

- Use of USB drives is discouraged due to risk of loss or theft.
- Only **encrypted USB drives** authorised by the Council may be used. These must be password-protected and never left unattended in public spaces.

Policy Items Applicable to CWPC Staff

6. Computer Usage

- Council computers lock automatically after 5 minutes of inactivity, but staff must still lock their devices whenever leaving their desks.
- Computers must be shut down daily.
- All work should be saved to designated shared drives or approved systems, not personal devices.

7. Emergency System Access:

- In an emergency, the Clerk can arrange access to staff email accounts via Redsquid.
- If the Clerk's email needs to be accessed, the Deputy Clerk may obtain access with approval from the Chair of the Council.

8. Internet Use & Firewall

- Work internet access is restricted to business purposes and limited personal use within this policy.
- Inappropriate, offensive, or illegal sites must not be accessed.

- The Council's **BitDefender firewall** is updated **monthly**. Firewall security reviews (including open port checks and password updates) are conducted regularly by Redsquid, the council's IT security provider.

9. Software

- For additional cyber protection, staff cannot download or install external software on Council systems. Only authorised applications may be used.

10. System Access Controls – Staff Departures

- When staff leave the Council, Redsquid will remove all system access within **24 hours**.
- Laptop devices of former staff members which are not in active are stored in a safe and collected securely by Redsquid to be wiped of all data.

11. Financial & Sensitive Data

- Sensitive financial information, including salary data, is stored on a **separate computer** for additional protection.
- This system, like all Council laptops and devices, must be protected by **multi-factor authentication (MFA)**.
- CWPC maintains regular, automated backups and tests restoration processes regularly.

12. Misuse of IT

Misuse of IT systems may result in disciplinary or formal Council action. Examples include:

- Sharing or attempting to discover another user's password.
- Attempting to bypass security controls.
- Installing or running malicious software.
- Using Council systems abusively or unlawfully.
- Leaving laptops unattended in public.
- Wasting Council IT resources.

13. Cloud-Based File Sharing

- Large files must be shared only using the Council's approved WeTransfer account.
- All WeTransfer links must have a time-limit set on access.

14. Emergency IT Procedures

- In case of sudden staff absence: the Clerk (or Deputy Clerk, if appropriate) will set up out-of-office replies or arrange limited email forwarding via Redsquid.
- Virus incident: any affected machine must be disconnected from the network immediately and reported to IT.
- Cyber-attack or data breach: escalate immediately to the Clerk of the Council who will liaise with Redsquid as appropriate.

Policy Items Applicable to CWPC Councillors

15. Councillor Devices

- Councillors are expected to use their own personal devices for Council duties.
- Councillors must ensure that their devices are kept secure, with up-to-date antivirus protection and strong passwords in place.