

Chipperfield Parish Council

IT and Email Usage Policy

1. Introduction

Chipperfield Parish Council recognises the critical role that secure and effective information technology (IT) and email systems play in supporting its operations, communication, and overall business functions.

This policy outlines the responsibilities and acceptable use of IT resources and email by all council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals using Chipperfield Parish Council's IT assets, including computers, networks, software, mobile devices, data, and email systems.

3. Acceptable Use of IT Resources and Email

Council-provided IT resources and email accounts must be used primarily for official council-related activities.

Limited personal use is permitted, provided it does not interfere with work responsibilities or violate this policy. Users must:

- Adhere to ethical and professional standards
- Respect copyright and intellectual property rights
- Refrain from accessing inappropriate, offensive, or unlawful content

4. Device and Software Usage

Where appropriate, the Council will provide authorised devices, software, and applications for work purposes.

The unauthorised installation of software—including personal applications—on council devices is strictly prohibited due to security risks.

5. Data Management and Security

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

Users are responsible for:

- Performing regular data backups
- Using secure methods for data disposal
- Protecting information in line with data protection legislation

6. Network and Internet Usage

The Council's network and internet access must be used responsibly and efficiently for legitimate council-related purposes.
Downloading or sharing copyrighted material without appropriate authorisation is strictly prohibited.

7. Email Communication

Council-issued email accounts are intended for official communication only. Users must:

- Maintain a professional and respectful tone
- Avoid sending sensitive information unless properly encrypted
- Exercise caution with attachments and hyperlinks to prevent phishing or malware threats
- Verify the legitimacy of sources before opening content

8. Password and Account Security

All users are responsible for securing their accounts. Best practices include:

- Creating strong, unique passwords
- Not sharing passwords with others
- Changing passwords regularly to improve account security

9. Mobile Devices and Remote Work

Mobile devices provided by the Council must be protected using passcodes and/or biometric authentication.

When working remotely, users must follow the same security protocols as when working on-site.

10. Email Monitoring

Chipperfield Parish Council reserves the right to monitor email communications to ensure compliance with this policy and applicable laws.

Monitoring will be conducted in line with the Data Protection Act and the General Data Protection Regulation (GDPR).

11. Retention and Archiving

Emails must be retained and archived in accordance with legal and regulatory requirements. Users should routinely review and delete unnecessary emails to maintain an organised inbox.

12. Reporting Security Incidents

All suspected IT or email security incidents must be reported immediately to the designated IT point of contact.

Any phishing attempts, data breaches, or suspicious email activity must be reported to the IT administrator without delay.

13. Training and Awareness

The Council will provide regular training and resources to promote awareness of IT security best practices, privacy requirements, and emerging technological risks.

All councillors and employees will participate in ongoing training to maintain good cybersecurity hygiene.

14. Compliance and Consequences

Failure to comply with this policy may result in:

- Suspension of IT access
- Disciplinary action
- Further legal or contractual consequences, depending on the nature of the breach

15. Policy Review

This policy will be reviewed annually to ensure it remains effective and up to date with technological advancements and evolving security standards.

16. Contacts

For IT-related enquiries or support, please contact the Clerk at:
parishclerk@chipperfield.org.uk

All staff, councillors, and authorised users are responsible for safeguarding the Council's IT infrastructure and email systems.

By following this policy, we help maintain a secure and effective digital environment in support of the Council's objectives.

Date: _____

Signature: _____

Role: _____