



Constantine Parish Council

Nicola Drewett – Clerk & RFO
Constantine Parish Council
10 Claremont Road
Redruth
Cornwall
TR15 1LP

Email: clerk@constantine-pc.gov.uk

Website: www.constantine-pc.gov.uk

Tel: 07396 864919

IT POLICY

1. Introduction

Constantine Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

3. Acceptable use of IT resources and email

Constantine Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided such use does not incur additional costs to the Council, or adversely affect the performance or security of the IT systems, it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Constantine Parish Council for work-related tasks.

All software installations must be approved and logged by the Clerk or designated IT contractor. Open-source software must be vetted for security.

All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

Equipment should not be dismantled or reassembled without seeking advice.

Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Clerk.

5. Data management and security

All sensitive and confidential Constantine Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

**The Council is required to adopt a data retention policy aligned with UK GDPR, and all data must be classified and stored in secure, backed-up environments.*

Personal data relating to councillors, staff, and other authorised users, associates, residents, external stakeholders should not be sent or saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen.

6. Network and internet usage

Constantine Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Members cannot use personal email accounts for Council business. Councillors will be issued with official council email addresses. Accounts provided by Constantine Parish Council are for official communication only. Emails should be professional and respectful in tone.

Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

Constantine Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security. Two-factor authentication (2FA) should be used where supported.

9. Mobile devices and Remote Work

Mobile devices provided by Constantine Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office. Use of secure, Council-authorised VPNs or remote desktop solutions is mandatory. Public Wi-Fi should not be used unless a VPN is in place

10. Monitoring

The Council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed such monitoring may take place. Any monitoring will be proportionate and comply with the relevant data protection and privacy laws.

11. Retention and archiving

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

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any suspicious activity or phishing emails immediately. All incidents must be logged and reviewed within 5 working days.

13. Training and awareness

Constantine Parish Council will provide regular training and resources to educate Employees about IT security best practices, privacy concerns, and technology updates. All employees will receive regular training on email security and best practices and Councillors will be offered the opportunity to undertake relevant training.

14. Copyright

Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

15. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

16. Contacts

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

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

Adopted at Full Council on 16th June 2026.

To be reviewed annually at the Parish Council Annual Meeting.

