Cranleigh Parish Council

EMAIL AND INTERNET USAGE POLICY

1. Introduction

The 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 individuals who use Cranleigh Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Network and Internet Usage

Cranleigh 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.

3.1 Staff members are encouraged to use the internet responsibly as part of their official and professional activities.

3.2 Information obtained via the internet and published in the name of the Council must be corroborated as accurate and valid according to recognised government, educational, or standards of UK Publishing regulations.

3.3 Information obtained via the internet and published in the name of the Council must be relevant and professional. A disclaimer must be stated where personal views are expressed.

3.4 The use of the internet to access and/or distribute any kind of offensive material will not be tolerated and staff may be subject to disciplinary action.

3.5 The equipment, services and technology used to access the internet must only be those authorised for this purpose by the council, or the property of the council. The council reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

4. Unacceptable use of the Internet

4.1 Unacceptable use of the internet by staff members includes, but is not limited to:

- sending or posting discriminatory, harassing or threatening messages or images
- using computers to perpetrate any form of fraud, and/or software, film or music piracy
- obtaining, using or disclosing another staff member's password without authorisation
- sharing confidential material or proprietary information outside of the council
- hacking into unauthorised websites
- sending or posting information that is defamatory to the council, its services, councillors and/or members of the public
- introducing malicious software onto council computers and/or jeopardising the security of the council's electronic communication systems
- sending or posting chain letters, solicitations or advertisements not related to Council business or activities
- passing off personal views as those representing the Council
- accessing inappropriate internet sites, web pages or chat rooms
- Creating accounts on Social Media or other services on behalf of the council without the authorisation of the Council or responsible officer.

4.2 If a staff member is unsure about what constitutes acceptable internet usage, then he/she should ask his/her line manager for further guidance and clarification

5. Email

Cranleigh Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided 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.

Email accounts provided by Cranleigh 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.

5.1 Use of email is encouraged as it provides an efficient system of communication.

5.2 Email should be regarded as written paper documents for the purposes of production, use, retention and disclosure and can be called upon under the Freedom of Information Act 2000. Personal information should be kept in accordance with the principles established in the Data Protection Act 1998.

5.3 The Council reserves the right to open any email file stored on the Council's computer system to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

5.4 The following guidelines for email use should be observed by all staff members and councillors:

- use appropriate language to avoid unintentional misunderstandings
- respect the confidentiality of information contained within emails, even if encountered inadvertently
- Quarantine any email received if there is any doubt regarding the authenticity of a message and verify the authenticity of the sender, without risk to the council by contacting them directly.
- do not open any attachment unless certain of the authenticity of the sender
- only copy emails to others where appropriate, certain of the authenticity of the sender and necessary
- emails which create obligations or give instructions on behalf of the council must be sent by officers only, not councillors
- emails must comply with common codes of courtesy, decency and privacy
- emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

6. <u>Reporting and Sanctions</u>

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

6.1 If a Councillor receives an email from a staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the Council's formal disciplinary procedure, or refer the matter to the Personnel Committee depending on the severity of the event.

6.2 If a staff member receives an email from another staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the Council's formal disciplinary procedure, or refer the matter to the Personnel Committee depending on the severity of the event.

6.3 If a staff member receives an email from a Councillor which they believe is contrary to the guidance provided in this policy, the staff member is entitled to consider use of the Council's grievance policy and/or report the issue through the procedures outlined in the Member's Code of Conduct.

7. <u>Security</u>

All sensitive and confidential Cranleigh 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.

Only software purchased by the council shall be installed on the Council's computer system. Software licences shall be retained. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

7.1 If a council officer's or councillor's computer is compromised by malicious, or foreign sovereign insurgency, the officer or councillor must immediately contact the councils IT and IT security team and disconnect their device from any threat to the councils network and systems.

7.2 Any breach of security perceived by any councillor or officer of the Council's IT systems by virtue of incursion by malicious software, or third parties must be reported to the Responsible Officer and the council's IT and network support provider: Netcom It Solutions Limited 01403 252995.

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

8. Password and Account Security

Cranleigh 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.

9. Mobile devices and Remote Work

Mobile devices provided by Cranleigh 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.

10. Training and Awareness

Cranleigh Parish Council 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.

11. Compliance and Consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

12. 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.

13. Contacts

For IT-related enquiries or assistance, users can contact the Clerk in the first instance.
All staff and councillors are responsible for the safety and security of Cranleigh Parish Council's IT and email systems. By adhering to this IT and Email Policy, Cranleigh Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

July 2025

Policy Review Date: October 2026