

Cranham Parish Council IT Policy January 2026

1. Introduction

Cranham 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 Cranham Parish Council's IT resources, including computers, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Cranham 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.

4. Device and software usage

Only approved software may be installed on council devices. Updates and security patches must be applied regularly.

5. Data management, security & confidentiality

All sensitive and confidential Cranham 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.

Personal data must be handled responsibly and in line with Data Protection laws (UK GDPR). Only keep information that is necessary and store it securely. The Clerk is the Data Protection Officer. The Council is registered with the ICO. Council information is confidential and should not be shared outside of the council unless authorised.

Downloading and sharing copyrighted material without proper authorisation is prohibited.

6. Email communication

Email accounts provided by Cranham Parish Council are for official communication only. Emails should be professional and respectful in tone. Only allocated .gov email accounts must be used for council business. The internet must not be used for illegal, or inappropriate activity. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments, or clicking on links. Do not open suspicious attachments, or links

7. Password and account security

Cranham 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.

8. Mobile devices and remote Work

Mobile devices provided by Cranham Parish Council should be secured with passcodes/ passwords. When working remotely, users should follow the same security practices as if they were in the office, ensuring devices are used in a secure environment and that data is protected.

9. Email monitoring

Cranham Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

10. Social Media & WhatsApp

Use of social media on council devices must be professional and respectful. Personal opinions should not be presented as council views. Always be mindful that messages sent on platforms such as WhatsApp can potentially be disclosed as part of a Subject Access Request response.

Always consider the Code of Conduct Policy in all communications, whether this be online, or in person.

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

Any suspected security incidents, data breaches, or lost devices must be reported immediately to the Clerk and Chairman. Further higher level reporting will then depend on the incident, with a plan for necessary action completed.

13. Compliance and consequences

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

14. Policy review

This policy will be reviewed every 3 years to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

14. Contacts

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

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