CLAYDON WITH CLATTERCOTE PARISH COUNCIL

IT POLICY

Introduction

Claydon with Clattercote 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.

Scope

This policy applies to all individuals who use the Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

Acceptable use of IT resources and email

Claydon with Clattercote 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.

Device and software usage

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

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

To protect Councillors and Council systems from potential data breaches and malware, users must not plug personal, or unverified, USB memory sticks into council-owned devices.

USB memory sticks provided by third parties, including developers or contractors, will not be accommodated or used on council-owned devices. This precaution is in place to safeguard against potential malware, data breaches, and hardware reliability issues.

Data management and security

All sensitive and confidential 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.

Network and internet usage

Downloading and sharing copyright material without proper authorisation is prohibited.

Email communication

Email accounts provided by the 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.

Caution should be taken with attachments and links to avoid phishing and malware. The source should be verified before opening any attachments or clicking on links.

Password and account security

The 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.

Mobile devices and remote work

Mobile devices provided by the 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.

Email monitoring

The 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. A separate social media and electronic communication policy has been adopted.

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.

Reporting security incidents

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.

Training and awareness

The 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.

Compliance and consequences

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

Contacts

For IT-related enquiries or assistance, users can contact the Clerk – clerk@claydonwithclattercote-pc.gov.uk.

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, the Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

This policy was adopted at a meeting of the Parish Council on 8th September 2026 (Minute Reference 47.26f) to be reviewed in two years or sooner should circumstance or legislation dictate.