Claygate Parish Council IT and Email Policy

1. Introduction

Claygate 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 councillors, employees, volunteers, and contractors.

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

2. Scope

This policy applies to all individuals - councillors, employees, volunteers, and contractors - who use Claygate Parish Council's IT resources, including computers, networks, software, mobile devices, telephones, data, and email accounts.

3. Related Policies

This policy should be read in conjunction with the Council's Data Protection Policy, Disciplinary Policy, Communications and Social Media Policy and any other relevant policies.

4. Acceptable use of IT resources

Claygate Parish Council IT resources are provided for Council purposes only. All computer and electronic hardware should be treated with good care at all times. All portable equipment must be stored safely and securely when not in use.

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

Mobile devices provided by Claygate 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.

5. Use of own devices

The Council recognises that some councillors may wish to use their own smartphones, tablets, laptops etc for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's network or to store data on the council's server or access data in other services.

Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, etc) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

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

Sensitive personal data should never be saved on councillors', staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

6. Data management and security

All sensitive and confidential Claygate 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.

7. Password and account security

Claygate Parish Council users are responsible for maintaining the security of their accounts and passwords. Multi-factor authentication should be enabled where possible. Passwords should be strong, stored in an encrypted password manager and not shared with others. Regular password changes are encouraged to enhance security.

8. Email communication

All email communication on council-related business **must** use an official Claygate Parish Council email address using the council-owned domain ie.name@claygateparishcouncil.gov.uk

The use of free email services (gmail, hotmail, yahoo, etc) is prohibited for council business.

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

Email mail accounts provided by Claygate 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 contained in an encrypted attachment. The encryption key must be transmitted separately to recipients, preferably via an end-to-end encrypted messaging service, such as WhatsApp, or, if using such a service is not practical, a text (SMS) message. On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors and staff should decide which is the optimum channel of communication to complete their tasks quickly and effectively.

9. Email monitoring

Claygate 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. 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.

11. 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.

12. Training and awareness

Staff and councillors will receive regular training on IT security, GDPR, best practices, privacy concerns, and technology updates.

13. Compliance and consequences

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

14. 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.

Approved: 25 March 2026