

Clint-Cum-Hamlets Parish Council IT Policy

1. Introduction

Clint-Cum-Hamlets 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 the Clerk who uses Clint-Cum-Hamlets parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

It also applies to councillors who receive, send and retain emails in their personal accounts and who therefore have responsibility for the security of data stored in this way.

3. Acceptable use of IT resources and Email

Clint-Cum-Hamlets parish council IT resources and the account issued to the clerk is 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. The user 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 Clint-Cum-Hamlets parish council for work-related tasks.

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

5. Data management and security

All sensitive and confidential Clint-Cum-Hamlets 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. Data backups are prescribed by the council, using OneDrive.

6. Network and internet usage

Clint-Cum-Hamlets 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

The main council account provided by Clint-Cum-Hamlets parish council is 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.

The Clerk must be cautious with attachments and links to avoid phishing and malware. The source of an email will be verified before opening any attachments or clicking links.

8. Password and account security

The Clerk is responsible for maintaining the security of the account & passwords. Passwords should be strong & not shared with others (unless required by the council's business continuity plan). Regular password changes are encouraged to enhance security.

9. Mobile devices and remote Work

Mobile devices provided by Clint-Cum-Hamlets parish council should be secured with passcodes and/or biometric authentication. When working remotely, the Clerk should follow the same security practices as if they were in the office.

10. Monitoring

Clint-Cum-Hamlets parish council reserves the right to monitor communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted by the Council in accordance with the Data Protection Act and UK GDPR.

11. Retention and archiving

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

12. Councillors

Councillors have not been issued with council owned email accounts.

Councillors will ensure that no other person is given access to their personal accounts, where personal data issued by the parish council may be stored.

Downloading and sharing any confidential information provided by the parish council or emails that contain personal data is prohibited without the authorisation of the council.

Downloading and sharing copyrighted material without the authorisation of the council is prohibited.

Councillors understand that if an investigation was necessary, ie relating to a security breach reported to the Information Commissioner's Office (ICO), there is a right for the ICO to interrogate their personal emails.

13. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the council for investigation and resolution. This provision applies to both Clerk and Councillors. If the council feel there has been a breach it would be immediately reported to the ICO.

14. Training and awareness

Clint-Cum-Hamlets parish council will provide regular training and resources to educate its officer(s) and councillors about IT security best practices, privacy concerns, and technology updates.

15. Compliance and consequences

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

16. 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.

17. Contacts

All staff and councillors are responsible for the safety and security of Clint-Cum-Hamlets parish council's IT and Email systems. By adhering to this IT and Email Policy, Clint-Cum-Hamlets parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Date: _____ 02.06.26 _____

Signature: G. Walker _____

Role: _____ Chair _____