Chelford Parish Council
IT and Email Policy

1 Introduction

1.1 Chelford Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations and communications.

1.2 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

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

3 Acceptable use of IT resources and email

3.1 Chelford 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

4.1 Where possible, authorised devices, software and applications will be provided by Chelford Parish Council to employees for the purposes of undertaking work-related tasks.

4.2 Chelford Parish Council does not provide computer equipment to councillors but will consider requests by councillors for assistance in training to acquire the necessary skills to execute tasks requiring technology.

5 Data management and security

5.1 All sensitive and confidential Chelford 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.

5.2 Employees and councillors should be mindful of the provisions contained within the Council's policies relating to privacy; subject access; freedom of information; information and data retention and disposal and social media.

6 Email communication

6.1 All employees and councillors are provided with a council email address and must use this for all council business.

6.2 Councillors are reminded that any email sent or received in their capacity as a Parish Councillors is Council data and any emails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act.

6.3 Councillors must ensure that any personal devices used to access council systems (including email and data) are password protected and access is restricted solely to the member.

6.4 Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

7 Password and account security

7.1 Chelford Parish Council email account 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.

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

8 Portable devices

8.1 All portable devices which have access to Chelford Parish Council email accounts and data must be protected to prevent unauthorised access. This can be by use of passwords, passcodes or other biometric measures as applicable.

8.2 Particular care must be taken when using removable media to transmit data as such media are easily lost or intercepted. Any sensitive information (including personal data, confidential documents or data which could impact on the rights or reputation of any person or organisation including the Council) placed on removable media must be suitably password protected or encrypted.

9 Email monitoring

9.1 Chelford 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

10.1 Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain and organised inbox.

10.2 Employees and councillors should refer to the Information and data retention and disposal policy when undertaking reviews of stored data.

11 Reporting security incidents

11.1 All councillors, employees or volunteers must report any incidents which could pose a risk to the council's systems or data security to the Clerk without delay. This includes but is not limited to:

- lost devices
- potential risk arising from phishing emails/websites
- passwords having been shared
- unauthorised access to systems.

12 Compliance and consequences

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

12.2 Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited.

13 Policy review

13.1 This policy will be reviewed annually to ensure its relevant and effectiveness. Updates may be made to address emerging technology trends and security measures.

14 Contacts

14.1 For IT related enquiries or assistance users can contact the Clerk.

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

Adopted: 12/06/25

Next review: May 2026