

Corby Glen Parish Council Information Technology Policy

1. Introduction

Corby Glen parish council recognises the importance of effective and secure information technology (IT) and email usage in supporting its operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT and email by council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use Corby Glen parish council's data, and email accounts.

3. Acceptable use of IT resources and email

Corby Glen parish council email accounts and data are to be used for official council-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights.

4. Device and software usage

Where computers that are used for council business are also used by other users a separate passworded logon account must be created to store any council related files and email. When the dedicated Corby Glen Parish Council account is not in use it must be closed and logged out.

5. Data management and security

All sensitive and confidential Corby Glen parish council data should be stored and transmitted securely using approved methods. Regular data backups should be performed every month and the data stored on a detachable hard drive kept in a secure location. To prevent data loss, and secure data destruction methods should be used when necessary.

6. Network and internet usage

Downloading and sharing copyrighted material and official or confidential council emails, without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Corby Glen 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.

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

8. Password and account security

Corby Glen 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.

10. Email monitoring

Corby Glen parish council reserves the right to monitor corbyglen.com domain email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the DPA2018 Data Protection Act and GDPR(General Protection Data Regulations)

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Emails should be reviewed regularly & unnecessary emails deleted to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Parish Clerk for investigation and resolution.

13. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT and email access and further consequences as deemed necessary.

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.

15. Contacts

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

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

Date: _____

Signature: _____

Role: _____