RISBY PARISH COUNCIL
IT Policy

1. Introduction

Risby 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 and volunteers.

2. Scope

This policy applies to all individuals who use Risby Parish Council's IT resources including email accounts.

3. Acceptable use of IT resources and email

Risby Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks only. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

5. Data management and security

All sensitive and confidential 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.

6. Network and internet usage

Risby 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

Email accounts provided by Risby 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.

DRAFT

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

Risby Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others.

9. Mobile devices and remote Work

Mobile devices provided by Risby 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.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements.

12. Reporting security incidents

All suspected security breaches or any email-related security incidents or breaches should be reported immediately to the clerk.

13 Training and awareness

All employees and councillors will be kept updated about email security and best practices.

15. 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.

16. Contacts

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

Date: _____ Review date: _____

DRAFT