Hinderclay Parish Council IT Policy

1. Introduction

Hinderclay 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 all individuals who use Hinderclay Parish Council's IT resources, which may include computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Hinderclay Parish Council IT resources and email accounts are to be used for official Council-related activities and tasks. 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

Where possible, authorised devices, software, and applications will be provided by Hinderclay 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 Hinderclay 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.

6. Internet usage

Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Gov.uk email accounts are provided by Hinderclay Parish Council for all official communications and should only be used for official communications. Personal email accounts should not be used for official communications. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

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

Hinderclay Parish Council users are responsible for maintaining the security of their email accounts. Passwords are provided and should not be shared with others.

9. Mobile devices and remote Work

Mobile devices should be secured with passcodes and/or biometric authentication.

10. Email monitoring

Hinderclay 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.

11. 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.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

13. Training and awareness

Hinderclay Parish Council will provide resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and Councillors will receive training on email security and best practices.

14. Compliance and consequences

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

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.

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

Approved at the meeting held on _____

Signature: _____ Role: _____