1. Introduction

Dormansland 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 Dormansland Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts, whether accessed via Council owned or personal equipment.

3. Acceptable use of IT resources and email

Dormansland Parish Council IT resources and email accounts are to be used for official council-related activities only. Use for personal activities is specifically prohibited. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Emails addressed to Council email addresses must not be forwarded (automatically or manually) to private a private email addresses or accounts.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Dormansland Parish Council for work-related tasks. Unauthorised installation of software on Council owned devices, including personal software, is strictly prohibited.

Where personal IT equipment is used for Council Activities, users should employ similar security protocols as would be employed were they using Council equipment. Upon ceasing to be a Member or Employee of the Council, all Council related data must be deleted.

5. Data management and security

All sensitive and confidential Dormansland Parish Council data should be stored and transmitted securely. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary. Any suspected data breach should be reported to the Clerk within 24 hours of becoming aware of the suspected breach to meet Information Commissioner's Office (ICO) reporting timelines.

6. Network and internet usage

Should Dormansland Parish Council provide network and internet connections, these should be used responsibly and efficiently for official purposes only. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Dormansland 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 aware that all emails received and sent from the Council's account may be subject to disclosure under the Freedom of Information Act 2000 or by a Subject Assess Request under GDPR regulations.

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

Dormansland Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong (such as 3 random words) and not shared with others. Regular password changes are encouraged to enhance security.

9. Mobile devices and remote Work

Mobile devices provided by Dormansland 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 a Council office.

10. Email monitoring

Dormansland 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 and be authorised by the Chair of the Council or Clerk.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements and in accordance with the Council's Data Retention Schedule. Regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches, incidents or loss of equipment 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

Dormansland Parish Council will provide regular training and resources to educate users about IT security best practices, data privacy and technology updates. All employees and councillors will receive regular 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.

16. Contacts

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

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

Date: _____

Signature: _____

Role: _____