



Langford Parish Council IT Policy

1. Introduction

Langford Parish Council recognises that the effective and secure use of information technology (IT) and email is essential to its operations, communications, and service delivery. This policy sets out the rules, responsibilities, and standards for the proper use of IT resources and email by council members, employees, volunteers and contractors.

2. Scope

This policy applies to all individuals who use Langford Parish Council IT resources, including computers, laptops, mobile devices, networks, software, devices, data, and email accounts, whether provided by the Parish Council or used on its behalf.

3. Acceptable use of IT resources and email

Langford Parish Council IT resources and email accounts are to be used for official Council business. Limited personal use is permitted, provided it does not interfere with work responsibilities or breach any part of this policy, create additional cost, or give rise to a security risk. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing material that is offensive, discriminatory, or otherwise unsuitable in a work environment.

4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by the Parish Council for work. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns, and users must not install, remove, or alter software on Council devices without prior authorisation from the Clerk or designated IT contact.

5. Data management and security

All sensitive and confidential Langford Parish Council data should be stored and transmitted securely using approved methods only. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary. All Parish Council information must be stored, accessed, transmitted, retained, and disposed of securely in accordance with Parish Council procedures.

6. Network and internet usage

Langford Parish Council's network and internet connections should be used responsibly and efficiently for official purposes and must not be used for unauthorised downloads, excessive personal use, or any activity that could compromise security, reduce performance, or damage the Council's reputation. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Langford Parish Council are for official communication only unless otherwise authorised. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted or another approved secure method used. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links and report suspicious emails promptly.

8. Password and account security

Langford Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others, must be kept confidential, and must be changed immediately if compromise is suspected. Regular password changes are encouraged to enhance security and users must comply with any Parish Council requirements for password resets or multi-factor authentication.

9. Mobile devices and remote Work

Mobile devices provided by Langford 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, including using secure internet connections, locking devices when not in use, ensuring that unauthorised persons cannot access Council information.

10. Email monitoring

Langford Parish Council reserves the right to monitor email communications and other IT use where necessary for legitimate business purposes, including security, compliance, and incident investigation. Monitoring will be conducted in accordance with the Data Protection Act and GDPR, and must be proportionate and limited to what is necessary.

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, subject to the Council's retention arrangements and any obligation to preserve records.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately. This includes suspected phishing, malware, accidental disclosure of information, or lost devices.

13 Training and awareness

Langford Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices, and all users are expected to complete required training and keep their knowledge up to date.

14. Compliance and consequences

Breach of this IT Policy may result in the suspension of IT privileges and further consequences as deemed appropriate, including disciplinary or other action where necessary.

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, changes in legislation, guidance or working practices.

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 Langford Parish Council's IT and email systems. By adhering to this IT Policy, Langford Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Date: _____

Signature: _____

Role: _____