Llanyblodwel Parish Council IT Policy

1. Introduction

Llanyblodwel 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 Llanyblodwel parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Llanyblodwel parish council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. 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 Llanyblodwel 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 Llanyblodwel 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. Please refer to the Data Retention Policy for more information.

6. Network and internet usage

Llanyblodwel 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 Llanyblodwel Parish Council are to be used solely for official Council business. All emails must be professional, respectful, and appropriate in tone.

Confidential or sensitive information must not be sent via email unless the communication is encrypted or secured through approved means.

All written communication with Councillors, including the issuing of agendas and summons to meetings, must be conducted via Council-issued .gov.uk email accounts. The use of personal email accounts for Council business is strictly prohibited, as it presents unacceptable security and data protection risks. All Councillors are required to use their official .gov.uk email addresses when conducting Council-related communications.

Users must exercise caution when handling email attachments and links. Be alert to phishing attempts and malware threats. Always verify the source of an email before opening attachments or clicking on links.

8. Password and account security

Llanyblodwel 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.

9. Mobile devices and remote Work

Mobile devices provided by Llanyblodwel 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.

10. Bring Your Own Device (BYOD)

Llanyblodwel Parish Council recognises that Councillors will be using their own personal devices such as laptops, tablets or smartphones for Council-related duties as the Council does not currently supply such devices to Councillors. The Council has a duty to ensure that all data, especially personal and sensitive data, is processed securely and in compliance with relevant legislation.

10.1 Purpose

This section sets out the conditions under which personal devices may be used for Council work, to protect the Council's data and systems and to ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable legislation.

10.2 Scope

This policy applies to all Councillors, staff and contractors who access Council information or systems using their own devices.

10.3 Acceptable Use

- Personal devices may be used to access Council emails, documents and communications, provided that appropriate security measures are in place (see 10.4).
- Users must not store Council data permanently on personal devices. Wherever possible, documents should be accessed through secure cloud-based services (e.g. Microsoft 365).
- Council data must not be shared via unauthorised apps or services (e.g. personal Dropbox or Google Drive accounts).

10.4 Security Requirements

Any personal device used for Council business must:

- Be protected with a strong password, PIN, or biometric lock.

- Have up-to-date antivirus and anti-malware protection.
- Be kept updated with the latest operating system and security patches.
- Support remote wipe capability, where feasible, in the event of loss or theft.
- Not be shared with unauthorised individuals (e.g. family members) when used for Council business.

10.5 Data Protection and Privacy

- All users are responsible for ensuring that any Council-related data accessed or processed on their personal devices is handled in accordance with the Council's Data Protection Policy.
- Personal data relating to residents or third parties must not be downloaded or stored on personal devices unless strictly necessary and must be deleted as soon as it is no longer needed.

10.6 Loss or Breach

- Any loss or suspected breach of a personal device used for Council business must be reported immediately to the Clerk.
- The Council reserves the right to investigate security breaches and, where necessary, require the user to cease using their personal device for Council work.

10.7 Consent and Review

By using a personal device for Council duties, users agree to comply with this policy and acknowledge that the Council may withdraw this permission at any time for security or compliance reasons.

11. Email monitoring

Llanyblodwel 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.

12. 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. Please refer to the Council's Document Retention Policy for further clarification on the retention of data.

13. 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 IT administrator immediately. Please refer to the Security Incident Policy.

14. Training and awareness

Llanyblodwel parish council will provide access to regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors have access to regular training on email security and best practices.

15. Compliance and consequences

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

16. 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.

17. Contacts

For IT-related enquiries or assistance, users can contact The Parish Clerk.
All staff and councillors are responsible for the safety and security of Llanyblodwel parish council's IT and email systems. By adhering to this IT and Email Policy, Llanyblodwel parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Adopted: 20.11.25
Reviewed: 15.01.26
Next Review: January 2027