WELSH NEWTON AND LLANROTHAL GROUP PARISH COUNCIL
IT and Email Policy

Version: 1.0
Adopted: 12th March 2026
Next review: March 2027
Approved by: Full council

1. Introduction

Welsh Newton and Llanrothal Group Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its governance, operations, and communications.

This policy sets out the responsibilities for the appropriate use of IT resources and email by councillors, the Clerk/RFO, volunteers, and any contractors acting on behalf of the council.

2. Scope

This policy applies to all individuals who use Welsh Newton and Llanrothal Group Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

The council's primary IT resources are:

- The council website at welshnewtonllanrothalgroup-pc.gov.uk
- The Clerk's email account (clerk@welshnewtonllanrothalgroup-pc.gov.uk) and all councillor .gov.uk email accounts provided and managed by the council
- Any council-related documents stored in cloud or local storage
- Any devices used by the Clerk in connection with council business

3. Acceptable Use of IT Resources and Email

IT resources and council email accounts are to be used for official council-related activities. Limited personal use of council IT resources is permitted, provided it does not interfere with council duties or violate any part of this policy.

All users must:

- Adhere to ethical and legal standards in all IT use
- Respect copyright and intellectual property rights
- Use the council's .gov.uk email address for all official council communications. The council has provided .gov.uk addresses to all councillors and expects these to be used for council business in preference to personal email addresses

4. Device and Software Usage

The council owned one desktop PC, recorded on the asset register. At its meeting on 12th March 2026 the council authorised its secure disposal in accordance with NCSC guidance on secure data destruction; the item has been removed from the asset register accordingly. The council does not currently own any computing hardware. The Clerk uses their own device(s) for day-to-day council work. Where the Clerk uses personal devices for council business, those devices should be reasonably secured (see sections 8 and 9).

Should the council acquire devices in future, they must not be used for personal purposes, must be kept up to date with security patches, and any council data stored on them must be backed up. Unauthorised installation of software on any council-owned device is prohibited.

5. Data Management and Security

All sensitive and confidential council data must be stored and transmitted securely. This includes personal data held under the council's data protection obligations (see the council's Data Protection Policy).[1]

The Clerk should ensure:

- Regular backups of council documents and data are performed
- Secure methods are used for disposing of data when no longer required
- Documents containing personal data are not shared beyond those with a legitimate need for access

6. Network and Internet Usage

Internet connections used for council business should be used responsibly and for official purposes. Downloading or sharing copyrighted material without authorisation is prohibited.

7. Email Communication

All council .gov.uk email accounts are for official communications only. All emails sent on behalf of the council should be professional and respectful in tone.

Users should:

- Avoid sending confidential or sensitive information via unencrypted email where practicable
- Exercise caution with attachments and links to guard against phishing and malware
- Verify the source of any unexpected attachment or link before opening it
- Not use personal email addresses for official council business

[1] UK General Data Protection Regulation (UK GDPR); Data Protection Act 2018.

8. Password and Account Security

All users are responsible for maintaining the security of their accounts. The council follows the National Cyber Security Centre (NCSC) guidance on passwords: accounts should be protected with a strong, memorable passphrase using three random words (for example, PurpleCandleRiver). This approach provides good protection against brute-force attacks while being easier to remember than complex character substitutions. Passwords must be unique to each account and changed promptly if a breach is suspected. The use of a password manager is recommended.

The council's email accounts are hosted on Zoho Mail, which supports two-factor authentication (2FA) at the individual mailbox level. The council intends to implement 2FA across all council .gov.uk email accounts during 2026/27 once current changes to the councillor complement have stabilised. The Clerk, as account administrator, is responsible for enabling and maintaining 2FA across all accounts once implemented. Where a councillor does not actively use their .gov.uk account, the Clerk may suspend the account as a precautionary security measure.

9. Mobile Devices and Remote Working

The council does not currently provide mobile devices. The Clerk uses a personally-owned mobile phone for council business, including email access. Any personal device used for council business should be secured with a passcode and/or biometric authentication and kept up to date with software updates. Council data accessed or stored on a personal device remains subject to this policy. If the council were to provide mobile connectivity in future, an eSIM on a personal device would be a practical and cost-effective option. Public or unsecured Wi-Fi networks should be avoided when accessing council accounts or sensitive data.

10. Email Monitoring

Council .gov.uk email accounts are council resources. Account holders should have no reasonable expectation of privacy in their use of these accounts; by accepting a council email account, an account holder acknowledges that it may be accessed by the council for legitimate governance purposes.[2]

The council reserves the right to access any council .gov.uk email account where necessary, relying on its legitimate interests as the lawful basis under UK GDPR.[3] This right would only be exercised in exceptional and documented circumstances — such as a formal complaint, safeguarding concern, or investigation into potential misconduct — and only by the Clerk as account administrator acting on the written authority of the Chairman or Full Council. Any such access will be proportionate, limited to what is necessary, and recorded.

[2]Human Rights Act 1998, Article 8 (right to respect for private life); Investigatory Powers Act 2016; Investigatory Powers (Interception by Businesses etc.) Regulations 2018.

[3]UK GDPR Article 6(1)(f) — legitimate interests of the controller, balanced against the rights of the data subject.

11. Retention and Archiving

Emails and documents relating to council business should be retained in accordance with the council's records retention schedule and relevant legal requirements. The Clerk should periodically review and archive or delete emails that are no longer required, whilst retaining those needed for audit or governance purposes.

12. Reporting Security Incidents

Any suspected security breach, loss of data, or IT incident relating to council business must be assessed immediately by the Clerk, who acts as the council's IT Security Administrator and data protection lead. The Clerk will notify the Chairman promptly. As account administrator, the Clerk may suspend or disable any council .gov.uk account as an immediate remediation measure. Where personal data may have been compromised, the Clerk must assess whether the breach requires reporting to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it, and take appropriate action.[4]

13. Training and Awareness

The Clerk will maintain appropriate training in IT security and data protection best practice. The council will support this as part of its training and development policy. Councillors are encouraged to engage with guidance on email security and data handling as it is issued.

14. Compliance and Consequences

Breach of this policy by any councillor, the Clerk, or any contractor acting for the council may result in suspension of IT access and further action as appropriate under the council's standing orders, code of conduct, or employment/contract arrangements.

15. Policy Review

This policy will be reviewed annually, or sooner if required by changes in legislation, technology, or guidance. The Clerk is responsible for recommending updates to the council for adoption.

16. Contacts

For IT-related enquiries or to report a security incident: clerk@welshnewtonllanrothalgroup-pc.gov.uk

[4]UK GDPR Article 33 — notification of a personal data breach to the supervisory authority (ICO) within 72 hours.

Data Protection Lead and IT Security Administrator: The Clerk (clerk@welshnewtonllanrothalgroup-pc.gov.uk)

Website: welshnewtonllanrothalgroup-pc.gov.uk

Adopted by Welsh Newton and Llanrothal Group Parish Council at its meeting on 12th March 2026 (minute 13.1).