1. Purpose Mynnas

This policy sets out how the Parish Council manages and uses Information Technology (IT) systems to ensure:

- security of data;
- efficient working practices; and
- compliance with legal requirements.

2. Scope Skop

This policy applies to:

- Councillors;
- Clerk and employees; and
- all Parish Council IT systems and devices used to connect to those systems.

3. Acceptable use Devnydh kemeradow

Parish Council IT systems must be used:

- for official Parish Council business only;
- in a lawful and responsible manner; and
- without bringing the Parish Council into disrepute.

Limited personal use is permitted where it does not interfere with duties.

4. Security Sekerder

Users must:

- use strong passwords, and should consider using a password manager;
- use two-factor authentication or biometric security features where available or required;
- ensure that devices are locked when unattended, including automatic locking;
- restrict the use of biometric security features to the authorised user only;
- not share login credentials; and
- report all security concerns immediately.

5. Equipment Daffar

Parish Council-owned devices must:

- remain Parish Council property; and
- not have any software installed without approval from the Clerk or authorised officer.

Personal devices used to connect to Parish Council systems must:

- meet minimum security requirements set out in this Policy;
- be registered on a list of devices authorised to access Parish Council systems; and
- be used in a manner that ensures Parish Council data remains secure and is not accessible to unauthorised persons.

The Parish Council reserves the right to restrict or withdraw access to its systems from any device which does not meet these requirements or is considered to present a security or data protection risk.

6. Software and applications Medhelweyth ha gweythresow

Parish Council-owned devices:

- must only use software approved by the Clerk or authorised officer; and
- will be configured with appropriate security, antivirus, and update controls.

Personal devices:

- may use software of the user's choosing; however, only software that meets the Parish Council's security and data protection requirements may be used to access Parish Council systems; and
- must not use software that stores Parish Council data outside approved systems or bypasses established security controls.

6.1. Open standards and open source Savon opyn ha devedhyans opyn

The Parish Council will:

- adopt open standards wherever practicable;
- give preference to open source software where it meets operational requirements; and
- seek to reduce reliance on proprietary systems and avoid vendor lock-in.

Guidance from the Government Digital Service and the Technology Code of Practice will inform decision making.

6.2. General software requirements Edhommow medhelweyth ollgemmyn

The Parish Council will:

- maintain and publish a list of preferred software to support secure and consistent working practices; and
- identify and prohibit specific applications or services where they present an unacceptable risk.

All users must ensure that:

- software used to access Parish Council systems is kept up to date and supported;
- Parish Council data is only stored within approved systems, including the Council's Document Management System; and
- appropriate care is taken to avoid introducing security vulnerabilities through the use of third-party applications.

The Parish Council does not approve or manage all software installed on personal devices but sets conditions for access to its systems. Failure to comply may result in access being restricted or withdrawn.

7. Data storage Gwithva manylyon

All users must:

- store all personal Parish Council data, including draft documents, in the personal Documents folder on the DMS;
- use synchronisation tools where appropriate; and
- only synchronise files and folders required for Council business.

8. Digital security Sekerder beysel

The Parish Council will:

- provide antivirus and malware protection on Parish Council devices;
- ensure regular backups of all data; and
- provide awareness and training on risks.

All users must:

- maintain appropriate protection on devices used; and
- ensure backups do not create unnecessary exposure of Parish Council data.

9. Breaches Torrvaow

Any IT or data breach must be:

- reported immediately to the Clerk;
- investigated and recorded; and
- reported where required under law.

10. Review Daswel

This Policy will be reviewed:

- annually; or
- following changes in legislation or guidance.

Appendix A - Minimum security requirements for devices
Ystynnans A – Edhommow sekerder lyha rag devisyow

This appendix sets out the minimum security requirements for any device used to access Parish Council systems.

A.1. Device security Sekerder devis

Devices must:

- be protected by a secure lock method (PIN, password, or biometric);
- automatically lock after inactivity (recommended 5–10 minutes);
- not be shared while logged into Parish Council systems; and
- be kept physically secure.

A.2. Operating system and updates Kevreyth gweythresans ha nowedhyansow

Devices must:

- run a supported operating system (Windows, macOS, Linux, iOS, Android, etc.);
- have updates enabled and applied; and
- not be used if unsupported.

A.3. Antivirus and malware protection Antivirus ha difresyans malware

Devices must:

- have appropriate protection where applicable; and
- use built-in security features.

A.4. Access to systems Hedhas dhe kevreythyow

Users must:

- use strong, unique passwords;
- use 2FA where available;
- use trusted applications or browsers; and
- log out when appropriate.

A.5. Data storage and handling Gwithva data ha handlans

Users must:

- store data only in approved systems (Nextcloud);
- avoid permanent local storage unless synchronised;
- remove temporary files when no longer needed; and
- not use unapproved cloud services.

A.6. Backup and synchronisation

Users must ensure:

- appropriate synchronisation with the DMS; and
- that backups do not create uncontrolled copies.

A.7. Prohibited use Devnydh difennys

Devices must not:

- be jailbroken or rooted;
- use untrusted software; or
- expose Parish Council data to risk.

A.8. Loss or breach Fall po torrva

Users must:

- report incidents immediately; and
- take steps to secure the device (e.g. remote wipe).

A.9. Compliance and access Gostytter ha hedhes

Compliance is a condition of access.
Access may be withdrawn if requirements are not met.

A.10. User declaration Diskleryans devnydher

Users will be required to confirm compliance with this Appendix.