Gwennap Parish Council

Information Technology (IT) & Cyber Security Policy

Adopted: 09 March 2026
Review Date: Annually
Version: 1.0

---

1. Purpose

This policy sets out the requirements for the secure use of information technology systems by Gwennap Parish Council ("the Council").

It aims to:

- Protect Council information and assets
- Ensure compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Reduce cyber security risk
- Safeguard residents' personal data
- Clarify acceptable use expectations for Members and Officers

---

2. Scope

This policy applies to:

- The Parish Clerk (as Proper Officer and Responsible Financial Officer)
- All serving Councillors
- Any Council employees
- Contractors, volunteers or working groups given access to Council systems
- All devices used to access Council data (including personal devices where applicable)

---

3. Council IT Systems

Council systems include:

- Council email accounts (e.g. gov.uk domain accounts where issued)
- Cloud storage platforms used by the Council
- Council website
- Council social media accounts
- Council laptops, tablets or mobile phones

- External storage devices used for Council business
- Financial software and online banking access

---

4. Roles & Responsibilities

4.1 The Council

The Council will:

- Provide secure systems for conducting Council business
- Maintain appropriate cyber security protections
- Ensure regular data backups are in place
- Maintain domain and website security
- Comply with data protection legislation

4.2 The Parish Clerk

The Clerk is responsible for:

- Administration of Council IT systems
- User access control
- Ensuring secure storage of Council records
- Maintaining password and access procedures
- Reporting data breaches to the Information Commissioner's Office where required
- Arranging secure disposal of redundant IT equipment

4.3 Councillors

Councillors must:

- Use Council email (where provided) for official business
- Not use Council systems for party-political activity
- Protect personal data they receive in their role
- Follow this policy at all times
- Immediately report suspected cyber incidents to the Clerk

---

5. Acceptable Use

Council IT systems must only be used for legitimate Council business.

The following are prohibited:

- Accessing or distributing offensive, unlawful or inappropriate material
- Downloading unauthorised software
- Sharing login credentials
- Using Council email for private commercial purposes
- Forwarding chain mail or unsolicited bulk messages

Limited incidental personal use is permitted where it:

- Does not interfere with Council duties
- Does not incur cost
- Does not breach this policy

---

6. Email & Communication

- All formal Council correspondence should be conducted via official Council email accounts where issued.
- Councillors using personal email accounts must ensure relevant Council correspondence is copied to the Clerk for record retention.
- Care must be taken before opening attachments or clicking links.
- Sensitive personal data should be password-protected when transmitted electronically.

---

7. Passwords & Access Control

All users must:

- Use strong passwords (minimum 12 characters)
- Use Multi-Factor Authentication (MFA) where available
- Keep passwords confidential
- Lock devices when unattended
- Not reuse Council passwords elsewhere

Access will be removed promptly when a councillor leaves office.

---

8. Personal Devices (BYOD)

Councillors may use personal devices to access Council information provided:

- The device is password or biometric protected
- The device operating system is kept updated
- Antivirus software is installed where appropriate

- Council data is not permanently stored locally where avoidable
- Lost or stolen devices are reported immediately

---

9. Data Protection & GDPR

Gwennap Parish Council is a Data Controller under UK GDPR.

Users must:

- Only access data necessary for their role
- Not retain personal data longer than required
- Not share personal data without lawful basis
- Store electronic files in Council-approved systems
- Shred paper documents containing personal data

Data breaches must be reported immediately to the Clerk.

Where required, breaches will be reported to the Information Commissioner's Office within 72 hours.

---

10. Remote Working

When working away from home or office:

- Avoid public Wi-Fi for accessing sensitive systems
- Ensure screens are not visible to others
- Keep devices secure when travelling
- Do not leave devices unattended in vehicles overnight

---

11. Website & Social Media

Only authorised persons may post on the Council’s official website or social media accounts.

Content must:

- Be factual and accurate
- Reflect Council decisions
- Not disclose confidential information
- Not contain personal data without consent

Councillors must clearly distinguish personal views from Council decisions.

---

12. Financial Systems & Online Banking

- Online banking access must be secured with MFA.
- Banking credentials must never be shared.
- Financial files must only be stored in approved secure systems.

---

13. Backup & Business Continuity

The Council will:

- Maintain regular automated backups
- Store backups securely (cloud or offsite)
- Periodically test restoration procedures

---

14. Cyber Security Incidents

Examples include:

- Phishing attempts
- Suspicious login activity
- Ransomware
- Accidental data disclosure
- Loss or theft of devices

All incidents must be reported immediately to the Clerk.

---

15. Monitoring

The Council reserves the right to monitor use of its IT systems where lawful, proportionate, and necessary to protect Council interests.

---

16. Breach of Policy

Failure to comply may result in:

- Removal of access
- Referral under the Council's Code of Conduct

- Disciplinary action (where applicable)

---

17. Review

This policy will be reviewed annually by the Council.

Gwennap Parish Council

Member IT Acceptable Use Agreement (Annual Declaration)

To be signed annually by all Councillors

I confirm that:

1. I have read and understood the Gwennap Parish Council IT & Cyber Security Policy.
2. I will use Council IT systems only for legitimate Council business.
3. I will use my Council email account (where provided) for Council correspondence.
4. I will not share passwords or login credentials.
5. I will use strong passwords and enable Multi-Factor Authentication where available.
6. I will protect personal data in accordance with UK GDPR.
7. I will not store Council personal data insecurely on personal devices.
8. I will immediately report any suspected cyber incident or data breach to the Clerk.
9. I understand that failure to comply may result in removal of system access or referral under the Code of Conduct.

Councillor Name: _____

Signature: _____

Date: _____