Treverbyn Parish Council

Information Technology (IT) Policy

1. Introduction

This Information Technology (IT) Policy sets out the principles, standards and procedures governing the use of information technology systems, devices, software, networks and electronic communications by Treverbyn Parish Council ("the Council").

The policy aims to:

- Ensure the secure and effective use of IT systems
- Protect Council information and data
- Support compliance with legal and regulatory requirements
- Reduce risks associated with cyber security and data loss
- Promote responsible and professional use of technology

This policy applies to:

- Councillors
- Employees
- Volunteers representing Treverbyn Parish Council
- Co-opted members
- Any person authorised to use Council IT systems or data

2. Scope

This policy covers:

- Computers and laptops
- Mobile phones and tablets
- Email systems
- Internet usage
- Cloud-based systems and storage
- Software and applications

- Social media where Council-managed
- Electronic records and data
- Cyber security arrangements
- Remote and home working arrangements (where applicable)

3. General Principles

All users of Council IT systems must:

- Use Council IT equipment responsibly and professionally
- Protect Council information from unauthorised access
- Comply with data protection legislation
- Follow cyber security guidance and good practice
- Use Council systems only for authorised purposes
- Report security incidents promptly

Users must not:

- Use Council systems for unlawful or inappropriate purposes
- Install unauthorised software
- Share passwords
- Access or distribute offensive, discriminatory, or inappropriate material
- Circumvent security controls

4. IT Equipment

4.1 Council-Owned Equipment

Treverbyn Parish Council maintains Council-owned IT equipment for authorised staff use within the Council offices.

Council-owned equipment may include:

- Desktop computers
- Laptops
- Printers
- Office networking equipment
- Mobile devices where applicable

At the time of adoption of this policy, Council-owned IT equipment is primarily used by office-based staff.

Authorised staff users are responsible for:

- Taking reasonable care of equipment
- Maintaining device security
- Preventing loss, theft, or damage
- Reporting faults or security concerns promptly

All Council-owned equipment remains the property of Treverbyn Parish Council.

4.2 Personal Devices (Bring Your Own Device – BYOD)

Some councillors use personal devices during meetings and when conducting Council business.

Where personal devices are used for Council purposes:

- Devices must be password or biometric protected
- Operating systems and software should be kept up to date
- Reasonable steps must be taken to prevent unauthorised access
- Council information must not be shared with unauthorised persons
- Public or unsecured Wi-Fi networks should be avoided where possible
- Council information should be deleted when no longer required

Councillors must ensure that personal devices used for Council business are managed responsibly and in accordance with this policy.

The Council reserves the right to require official Council business to be conducted through approved systems and email accounts.

5. Passwords and Access Security

Users must:

- Use strong passwords
- Keep passwords confidential
- Avoid reusing passwords across systems
- Change passwords if compromise is suspected
- Use multi-factor authentication where available

Passwords must not:

- Be shared with others
- Be written in insecure locations
- Be stored openly or transmitted insecurely

Access to systems shall be restricted according to role and operational need.

6. Email and Electronic Communications

Council email accounts shall be used for official Council business wherever possible.

Users must:

- Communicate professionally and respectfully
- Be aware that emails may be subject to Freedom of Information requests
- Avoid sending confidential or sensitive data insecurely
- Take care when opening attachments or links

Users must not:

- Send offensive or inappropriate content

- Use Council email for political campaigning
- Subscribe Council accounts to unnecessary services

The Clerk shall maintain appropriate control over official Council email accounts.

6.1 Council Email Accounts

Treverbyn Parish Council uses official '.gov.uk' email accounts for Council business.

Councillors and staff issued with Council email accounts shall use them for official Council correspondence wherever practicable.

Use of Council email accounts supports:

- Cyber security
- Professional standards
- Data protection compliance
- Freedom of Information compliance
- Business continuity

Council email accounts remain the property of the Council.

Access credentials must not be shared.

7. Internet Usage

Internet access is provided for legitimate Council business purposes.

Limited personal use may be permitted provided it:

- Does not interfere with Council duties
- Does not incur unreasonable cost
- Is lawful and appropriate

Users must not access:

- Illegal material
- Offensive or discriminatory content
- Gambling or inappropriate websites
- Content likely to damage the Council's reputation

The Council reserves the right to monitor usage where necessary and lawful.

8. Cyber Security

The Council recognises the importance of cyber security and shall take reasonable steps to protect systems and information.

Measures may include:

- Anti-virus software
- Firewalls

- Software updates
- Secure backups
- Multi-factor authentication
- Access controls
- Staff awareness training

Users must:

- Report suspicious emails or cyber incidents immediately
- Not click suspicious links or attachments
- Keep software updated where responsible for devices
- Follow guidance issued by the Clerk or IT provider

Councillors using personal devices for Council business are expected to take reasonable steps to maintain device security, including use of passwords, software updates, and anti-virus protection where appropriate.

9. Data Protection and Confidentiality

All users must comply with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000

Users must:

- Protect personal and confidential information
- Access data only where authorised
- Avoid unnecessary sharing of information
- Dispose of electronic records securely

Personal data breaches must be reported immediately to the Clerk.

10. Software and Licensing

Only authorised software may be installed on Council equipment.

Users must not:

- Install unauthorised applications
- Use illegal or unlicensed software
- Alter security settings without permission

Software licensing requirements must be observed at all times.

11. Remote and Home Working (Staff)

Users working remotely must ensure:

- Council information remains secure
- Devices are not left unattended in public places
- Screens are locked when unattended
- Secure internet connections are used where possible

Confidential discussions and documents should not be exposed to unauthorised persons.

12. Backups and Storage

Important Council records shall be backed up regularly.

Electronic records should be stored in approved locations only.

Users must avoid storing Council information solely on:

- Personal devices
- USB drives
- Unapproved cloud services

Retention and deletion of records shall comply with the Council's Retention Policy.

13. Social Media and Online Presence

Only authorised persons may post on behalf of the Council.

Council social media and online communications must:

- Be professional and respectful
- Avoid political bias
- Protect confidential information
- Comply with Council policies

Users must not represent personal opinions as those of the Council.

14. Monitoring

The Council reserves the right, where lawful and proportionate, to monitor:

- Use of Council IT systems
- Email usage
- Internet activity
- Security logs

Monitoring shall be conducted in accordance with relevant legislation.

15. Reporting Incidents

Users must report immediately:

- Lost or stolen devices
- Suspected data breaches
- Cyber security incidents
- Unauthorised access attempts
- Malware or suspicious activity

Reports should be made to the Clerk as soon as practicable.

16. Breaches of Policy

Failure to comply with this policy may result in:

- Withdrawal of IT access
- Internal disciplinary procedures
- Referral to external authorities where appropriate

Serious breaches may constitute misconduct or criminal offences.

17. Review

This policy shall be reviewed annually or sooner if required by changes in legislation, technology, or operational requirements.

18. Adoption

Adopted by Treverbyn Parish Council on: