

Torver Parish Council IT & Acceptable Use Policy

1. Purpose

This policy sets out how the Parish Council uses and protects its information technology systems, devices, email accounts, data, and internet services.

The aims are to:

- Protect council information and personal data
 - Reduce the risk of cyber incidents
 - Ensure lawful and professional use of IT systems
 - Support councillors and staff in safe working practices
-

2. Scope

This policy applies to:

- Parish councillors
- Employees and contractors
- Volunteers using council IT systems or accessing council information

It covers:

- Council-owned laptops, phones, and storage devices
 - Personal devices used for council business
 - Email systems
 - Cloud storage and collaboration systems
 - Internet and social media use
-

3. Acceptable Use

Users must:

- Use council IT primarily for council business
- Behave professionally and lawfully online
- Keep passwords secure
- Lock devices when unattended
- Report suspicious emails or security concerns promptly

Users must not:

- Share passwords

- Install unauthorised software
- Access unlawful or inappropriate material
- Use council systems for political campaigning
- Store unnecessary personal data

Limited personal use is acceptable where it does not interfere with council business or create security risks.

4. Passwords and Account Security

- Passwords must be strong and unique
- Multi-factor authentication (MFA) should be enabled wherever available
- Passwords must never be written down in accessible places or shared
- Accounts must be disabled promptly when a councillor or employee leaves office

Recommended minimum password standard:

- At least 12 characters
 - Combination of words, numbers, and symbols
-

5. Email Security

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

Users must:

- Be cautious of phishing emails and unexpected attachments
- Verify bank detail changes or payment requests independently
- Avoid sending sensitive personal data unless necessary
- Use blind copy (BCC) for group emails where appropriate

Personal email accounts should not normally be used for council business.

6. Data Protection and GDPR

All users must comply with UK GDPR and the Data Protection Act 2018.

Personal data must:

- Be collected only where necessary
- Be kept accurate and secure
- Not be retained longer than required

- Only be shared where lawful and appropriate

Sensitive or confidential information must not be stored on unsecured personal devices.

7. Remote and Home Working

Where council business is conducted remotely:

- Devices should be kept physically secure
 - Public Wi-Fi should be avoided unless using secure connections
 - Screens should not be visible to unauthorised persons
 - Paper records containing personal data should be stored securely and shredded when no longer needed
-

8. Software and Updates

Council devices should:

- Use supported operating systems
- Have antivirus protection enabled
- Receive regular software updates
- Use licensed software only

Automatic updates should be enabled where practical.

9. Backup and Storage

Important council records should be backed up regularly using approved cloud or secure storage systems.

The council should maintain:

- At least one secure backup copy
 - Access controls for shared folders
 - A process for recovering important files
-

10. Social Media and Website Use

Only authorised persons may publish official council communications online.

Posts must:

- Be respectful and factual
- Avoid disclosing confidential information

- Comply with council policies and legal obligations
-

11. Cyber Security Incidents

Any suspected breach, malware infection, phishing attempt, or data loss must be reported immediately to the Clerk or designated officer.

Examples include:

- Lost or stolen devices
- Emails sent to the wrong recipient
- Suspicious login activity
- Ransomware or virus alerts

The council may temporarily suspend access to systems where necessary to protect data.

12. Monitoring

The council reserves the right to monitor use of council systems where necessary for:

- Security
- Legal compliance
- Investigating misuse

Monitoring will be proportionate and lawful.

13. Training

Councillors and staff should receive periodic awareness training covering:

- Password security
 - Phishing awareness
 - GDPR responsibilities
 - Safe handling of council information
-

14. Review

This policy should be reviewed annually or following any significant IT or security incident.