Wem Town Council

IT and Cyber Security Policy

October 2025

1. Introduction

The Council recognises the increasing threat posed by cybercrime, including phishing, malware, and data theft. This IT and Cyber Security Policy outlines the responsibilities and best practices for protecting Wem Town Council's data, systems, and digital communications.

2. Scope

This policy applies to all Councillors, employees, and volunteers using council-issued devices or accounts.

3. Background

Wem Town Council has three office-based employees using laptops, tablets and mobile phones, one groundskeeper using a mobile phone, and 14 councillors using council-issued tablets. All have gov.uk email addresses.

According to the Department for Communities and Local Government and Cabinet Office guidance, local councils are frequent targets of attack. Even small organisations must act to mitigate risks and protect services.

Threats may come from criminals, hacktivists, insiders, or state actors, with motivations ranging from financial fraud to reputational damage. While no system can be completely secure, practical measures can significantly reduce risk.

The National Cyber Security Centre (NCSC) recommends implementing five technical control themes to improve cyber security[1]: These themes (firewalls, secure configuration, security update management, user access controls and malware protection are covered separately in Appendix A.

4. Device and System Security

<u>Council-owned Devices</u>

- Must be password protected with strong, unique credentials.
- Must be securely configured before use, with unnecessary apps, services, and accounts removed.
- Automatic updates must be enabled for operating systems and critical software.

[1] Cyber Essentials: Requirements for IT Infrastructure v3.2

- Reputable anti-malware software must be installed and kept up to date.
- Default passwords must be changed before use. Auto-run and guest access must be disabled.
- USB devices and unapproved software must not be used without authorisation.
- Firewalls must be enabled and configured to block unauthorised connections. Settings should be reviewed regularly by IT support.

5. User Access and Authentication

- Each user must have a unique login with access limited to what they need for their role.
- Shared accounts are not permitted. Access must be revoked when a user leaves or changes roles.
- Passwords must be strong, regularly updated, and kept confidential.
- Multi-Factor Authentication must be used where available.

6. Email and Internet Use

- All Council correspondence must be conducted using official gov.uk email addresses.
- Emails must be professional and respectful. Attachments or links from unknown sources must not be opened.
- Sensitive information should only be shared using encrypted methods.
- Council IT and email should mainly be used for Council work. Limited personal use is allowed if it doesn't interfere with duties.
- Inappropriate or illegal content must not be accessed or shared.
- The Council may monitor email use in line with legal requirements.
- Emails must be retained according to the Council's data retention policy. Irrelevant emails should be deleted regularly.

7. Malware and Threat Protection

- Anti-malware tools must run real-time scans and update automatically.
- Files and external media must be scanned before use.
- Staff and councillors must report suspicious activity to the Clerk or IT support immediately.

8. Data Backup and Recovery

- Important data must be backed up regularly using secure cloud or off-site systems.
- Backups should be tested periodically to ensure they can be restored.

9. Training and Awareness

- All users must complete cyber security training if made available.
- The Clerk will circulate guidance and alerts from national agencies such as Action Fraud.
- Breaches of this policy may result in restricted access or other actions.

10. Incident Management and Continuity

- Any suspected breach must be reported to the Clerk immediately.
- An incident log will be maintained. Serious breaches may be reported to the ICO or GovCertUK.
- Business continuity plans and disaster recovery procedures must be reviewed and tested regularly.

11. Recommendations

- Include cyber risk on the Council's risk register.
- Assign a councillor lead for cyber oversight and data security.
- Join the Cyber Security Information Sharing Partnership (CiSP).
- Follow NCSC recommendations for small organisations and public bodies.
- Review recovery plans regularly.
- Review this policy annually or after a major incident.

Appendix A Technical Controls Aligned with NCSC Guidance

Firewalls

- All council-issued devices must have a software firewall enabled. Office-based systems must also be protected by a network firewall.
- Firewalls must be properly configured to block unauthorised inbound and outbound connections.
- Firewall settings must be reviewed regularly by IT support to ensure continued protection.

Secure Configuration

- Devices must be securely configured before use. This includes removing unnecessary apps, services, or default accounts.
- Default passwords must be changed before use, and features such as auto-run and guest access must be disabled.
- Security settings should include screen-locks, USB device restrictions, and disabling installation of unauthorised software.

Security Update Management

- Automatic updates must be enabled on all operating systems and critical software applications.
- Security patches must be applied within 14 days of release or sooner if they address a critical vulnerability.
- The Clerk or IT support will review update logs monthly to ensure devices are compliant.

User Access Controls

- Every councillor and staff member must have their own unique login credentials.
- Access permissions must be based on the user's role and limited to what is necessary.
- Shared accounts are not permitted. When a user leaves or changes role, their access must be revoked promptly.
- Strong passwords must be enforced, and Multi-Factor Authentication should be used wherever available.

Malware Protection

- All council-owned devices must have reputable anti-malware software installed, set to update and scan automatically.

- Real-time scanning must be enabled to detect threats from downloads, websites, and emails.
- Devices must block installation of unapproved or unsigned software.
- Staff and councillors should report any suspicious behaviour or malware alerts to the Clerk or IT support immediately.

Appendix B **Cyber Attack Response Plan**

If Wem Town Council experiences a cyber-attack, the following actions must be taken:

Immediately (first 24 hours)

- ☐ Disconnect affected devices from the internet and council network.
- ☐ Inform all staff and IT support provider immediately.
- ☐ Preserve evidence by not wiping devices or deleting files.
- ☐ Notify relevant authorities if necessary (e.g. Action Fraud, NCSC, and ICO if personal data is involved).
- ☐ Alert councillors and staff to be cautious of phishing or suspicious communications.
- ☐ Mayor and Councillor with responsibility for Cyber Security to be informed as soon as practicable.

Within 1 Week

- ☐ Conduct an initial investigation with IT support to identify what was accessed, stolen, or damaged.
- ☐ Reset passwords for all accounts (email, devices, systems).
- ☐ Apply urgent software and security updates to prevent repeat attacks.
- ☐ Communicate transparently with councillors, staff, and (if relevant) residents about any impact.
- ☐ Review and update backups to restore essential data if needed.

Within 1 Month

- ☐ Complete a full technical investigation with IT support.
- ☐ Assess and document the financial, operational, and reputational impact.
- ☐ Submit reports to Full Council, the ICO (if required), and insurers.
- ☐ Update risk assessments and refine access controls.
- ☐ Provide refresher training for councillors and staff on spotting cyber threats.

Longer Term (Ongoing)

- ☐ Regularly test and improve incident response and recovery plans.
- ☐ Invest in stronger cyber protections (firewalls, MFA, endpoint protection).
- ☐ Carry out annual independent security reviews.
- ☐ Ensure cyber risk remains on the Council's risk register.
- ☐ Continue councillor/staff awareness training at least annually.
- ☐ Ensure all staff are aware of and understand this response plan.

Appendix C

COUNCILLOR EMAIL, INTERNET AND DEVICE ACCEPTABLE USE POLICY

Approved May 2025

Use of devices and dedicated email accounts enables Councillors to access information on the move, take advantage of Wi-Fi and reduce paper and printing costs.

1. Introduction

Under the Data Protection Act 2018 it is important that Wem Town Council (the 'Council') ensures that its data is kept secure. Councillors are required to comply with this policy. Please note additional instructions and advice may be issued from time to time regarding the use of devices or systems.

This policy sets out general rules for acceptable use of digital systems including;

- How use of the facilities made available reflects the Council;
- Responsibilities for handling personal and sensitive information properly, including email addresses;
- Considerations required before sending confidential or sensitive information by email;
- How and when personal use of email and the internet is permissible;
- Removal of personal email from the Council's systems;
- Prohibition of the use of Council's email addresses on public websites for non-Council purposes; and
- Circumstances under which the Council may monitor communications.

2. IT Devices

The devices referred to in this policy include tablets and other portable devices which the Council may choose to provide to Councillors.

You must take care of any allocated devices and ensure that they are safe and secure at all times. Any loss of or compromise to equipment must be reported immediately so the device or account can be disabled.

Equipment and system passwords are important confidential information. Do not share them with others and make sure that they are not written down where an unauthorised person can access them.

You must not delete any of the Council installed software and must not install any software to a Council device without the permission of the Town Clerk.

If you have problems accessing the systems, raise this with council staff as soon as possible so that investigation can take place and advice can be given.

3. Use of Personal Devices

The Council has resolved that no individual councillor may access Council emails on a personal device.

4. Email

All email correspondence should be dealt with professional and carefully. Emails are subject to the Data Protection Act 2018 and may be included in Freedom of Information requests. Only Council email accounts should be used to conduct Council business. Under no circumstances should emails be forwarded either individually or in bulk by means of an auto-forward to other email accounts (personal, business or other authorities).

When using your Council email account, you should be mindful of the fact that any email you send will be identied as coming from the Council. You should therefore take care not to send anything by email that may reflect badly on the Council. Using a Council email address to send inappropriate material, including content of a sexual or racist nature, is strictly prohibited.

Should you receive any offensive or inappropriate content by email you should delete it. Councillors should inform the Town Clerk of this as soon as possible so that it can be fully removed from the system.

Attachments in email messages are commonly used to introduce computer viruses and malware to systems. An email containing such an attachment may appear to come from someone you know. If you feel the email is not genuine, do not attempt to open the attachment. Delete the email immediately and advise the Town Clerk of the presumed sender and outline content so that action can be taken.

You should also take care that emails will be seen only by the person intended. Care should be taken when sending confidential information that the email has been correctly addressed, marked ‘private’ and not copied in to those not authorised to see the information. Sending confidential information by email without proper authorisation or without ensuring it is properly protected will be treated as misconduct.

In cases where you are sending an email to more than one personal account you must blind copy all recipients to avoid a data breach.

While a limited amount of personal use of email is perfectly acceptable, your email remains the property of the Council and you should not use your Council email to send or receive any information that you regard as private.

The Council may, during its operation, read emails that you have sent or received – although in the absence of evidence of wrongdoing the Council will try to avoid reading personal emails.

5. Internet Use

Councillors with access to the internet on Council-owned devices should use that access responsibly. In particular the following is deemed unacceptable use or behaviours:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using to the computer to perpetrate any form of fraud, or for software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about the Council, the Councillors, staff or the public on social networking sites, blogs, wikis and any other online publishing format
- revealing confidential information about the Council in a personal online posting, upload or transmission
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of malicious software into the Council's network

6. Social Media

This section should be read in conjunction with the Council's Social Media Guidelines 2022.

When using social media, councillors must be mindful of the information they post, in both a personal and Council capacity, and keep the tone of the comments respectful and informative. Online content should be accurate, objective, balanced and informative.

Councillors' behaviour on any social networking or other internet site must be consistent with the behaviour required of being a representation of the Council.

Councillors must not:
- present their own opinions as those of the Council;
- express any views which may have a party-political bias;
- present themselves in a way that might cause embarrassment to the Council;
- post content that is contrary to the democratic decisions of the Council;
- post controversial or potentially inflammatory remarks;
- engage in personal attacks, and hostile communications;

- publish photographs or videos of minors without parental permission;
- post any information that infringes copyright of others;
- post any information that may be deemed libel;
- post online activity that constitutes bullying or harassment;
- bring the Council into disrepute, including through content posted in a personal capacity;
- post offensive language relating to race, sexuality, disability, gender, age, religion or belief; and conduct any online activity that violates laws, regulations or that constitutes a criminal offence.

Councillors should not operate a social media account or profile that purports to be operated on or behalf of the Council without the express permission of the Town Clerk.

Any Councillor receiving unwelcomed comments, threats, or harassment online should report it to the police. If you feel your account is being attacked by someone acting as a 'Troll' it is best practice to ignore this person or persons and report the issue to the social media site on which the problem is occurring. There are also several options in relation to 'blocking' a person if the behaviour is particularly upsetting or abusive.

7. Personal/Business Use

The Council's communication facilities are provided for the purposes of the Council's business. Limited and responsible personal use by users is also permitted.

Although the Council's email facilities are provided for the purposes of Council business, you may occasionally want to use them for your own personal purposes. This is permitted on the condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of Council facilities for personal correspondence, you can expect very little privacy because the Council may need to monitor communications.

Under no circumstance may the Council's facilities be used in connection with the operation or management of any business or for commercial activity. The facilities should not be used by councillors for general party-political activity, and must not be used for campaigning or election activities. They may, however, be used for correspondence within the political group, general political research, casework as a councillor and similar activities. If you have any doubts, please ask the Town Clerk.

You must also ensure that your personal email use:

- is minimal;
- is lawful and complies with this policy;
- does not take priority over your responsibilities as a councillor;

- does not cause unwarranted expense or liability to be incurred by the Council; and
- does not have a negative impact on the Council in any way.

After being read, personal email should be deleted or forwarded to a personal email account and then deleted. You should note that email is backed up regularly and deleting it from the live system may not necessarily result in it being permanently deleted. for good.

If you make personal use of the Council's facilities for sending and receiving email, you will be treated as having agreed to abide by the conditions imposed for their use and consented to the Council monitoring your personal email in accordance with this policy. If you do not agree or consent to this, then you must not use the system to send or receive personal email.

8. What happens if this policy is breached

If the rules and procedures are not followed, then use of the Council's facilities may be curtailed or withdrawn. Serious breaches of this policy may amount to breach of the Code of Conduct and the withdrawal of permission to use the Council's equipment for personal purposes. Some aspects of this policy also deal with matters which amount to criminal offences under the Computer Misuse Act 2020.

If there is anything in this policy that you do not understand, please ask the Town Clerk for clarification.

Please sign and return this form

I confirm that I have read, understand and will comply with the Wem Town Council Acceptable Use Policy for Councillors.

Signed ……

Name ……..

Date …….

Appendix D **Associated Staffing Policies**

Wem Town Council staff should refer to the following policies in the most recent version of the WTC Staffing Handbook:

- Use of Computer Equipment Policy
- Email and Internet Policy