IT Acceptable Use Policy

Adopted by:	Watton Town Council
Date:	April 2026 v2 June 2026
Review date:	April 2029

1. Purpose and Scope

1.1 This policy explains the standards that apply when using Watton Town Council IT systems and digital services. Its purpose is to protect Council information, support effective working, and reduce the risk of security incidents, data breaches and misuse.

1.2 The Council relies on IT systems for communication, administration, records management and service delivery. All users are expected to use those systems responsibly, lawfully and in a way that protects the Council's information, reputation and operational resilience.

1.3 The Council uses the NJC Green Book (2024) and the NALC Model Contract of Employment (2023) as guidance when determining employment terms and conditions. Not all provisions apply automatically. Where this policy, an employee's contract, or another adopted Council policy sets out a local arrangement, that local arrangement will apply.

1.4 This policy applies to employees of Watton Town Council. It also applies to councillors, contractors, volunteers and other authorised users where they are given access to Council IT systems or Council information. Where councillors are using Council systems in connection with Council business, they are expected to comply with the relevant parts of this policy. Any employment-related sanctions under this policy apply to employees only.

1.5 This policy should be read alongside the Data Protection Policy, Employee Privacy Notice, Social Media Policy, CCTV Policy, Vehicle Tracking Policy, Disciplinary Procedure and any Council guidance on records retention, cyber security or remote working.

1.6 This policy is non-contractual and may be amended by the Council from time to time.

2. Council Systems Covered by this Policy

2.1 This policy applies to Council-owned or Council-managed computers, laptops, tablets, mobile phones, email accounts, cloud services, software, internet access, storage systems, remote access arrangements and any other digital tools provided or authorised by the Council.

2.2 It also applies to Council information accessed through personal devices where the Council has expressly authorised that arrangement.

3. General Principles of Use

3.1 Council IT systems are provided mainly for work-related purposes and Council business. Limited personal use may be allowed where it is reasonable, infrequent, lawful and does not interfere with duties, service delivery or security.

3.2 Users must act professionally and with common sense when using Council systems. This includes thinking carefully before sending emails, opening links, downloading files or sharing information.

4. Acceptable Use

4.1 Users must use Council IT systems in accordance with Council policies, their role requirements and applicable law.

4.2 Users must keep passwords, login details and other access credentials secure and must not share them with others unless a properly authorised arrangement is in place.

4.3 Devices must be locked when left unattended, and users should log out or close systems when they are no longer in use.

4.4 Emails and other electronic communications must be professional, respectful and appropriate. Users should assume that messages sent through Council systems may later need to be disclosed for governance, legal or data protection reasons.

4.5 Suspected cyber incidents, phishing attempts, loss of equipment, accidental disclosure or any other IT security concern must be reported to the Clerk as soon as reasonably practicable.

5. Unacceptable Use

5.1 Users must not access, create, store or share material that is offensive, obscene, discriminatory, harassing, defamatory or unlawful.

5.2 Users must not deliberately access systems, files or data that they are not authorised to use.

5.3 Users must not download or install unauthorised software, apps, browser extensions or tools onto Council equipment or systems.

5.4 Council systems must not be used for private commercial activity, personal business or any purpose that conflicts with the interests of the Council.

5.5 Council information must not be stored on personal devices, memory sticks, messaging apps or personal cloud accounts unless the Council has expressly authorised this and appropriate safeguards are in place.

5.6 Users must not bypass security settings or other technical controls put in place by the Council or its IT support.

6. Information Security and Data Protection

6.1 All use of Council systems must comply with data protection law and the Council's data protection arrangements. Personal data must be accessed only where there is a legitimate business need, handled carefully, and shared only with authorised recipients.

6.2 Users should take reasonable care to prevent loss, unauthorised access, accidental disclosure or damage to Council information. This includes checking recipients before sending emails, using secure storage, and avoiding informal or insecure sharing methods.

6.3 Paper and digital records must be managed in accordance with Council retention and confidentiality requirements.

7. Passwords, Phishing and Cyber Security

7.1 Passwords must be strong and unique to Council systems. Where systems allow, passwords should normally be at least 12 characters long.

7.2 If a user thinks a password or account may have been compromised, they must change it promptly where possible and report the concern without delay.

7.3 Users must be alert to phishing emails, suspicious links, unexpected attachments and unusual requests for information or payment. If in doubt, the user should stop and check before taking action.

7.4 Where multi-factor authentication is available for Council systems, users are expected to use it.

7.5 All suspected security breaches, including email breaches or incidents should be reported immediately to the Clerk.

7.6 For IT-related enquiries or assistance, users can contact the Clerk. All staff and councillors are responsible for the safety and security of IT and email systems.

8. Remote Working and Personal Devices

8.1 When working remotely, users must take reasonable steps to protect confidentiality and security. This includes using password-protected devices, avoiding unsecured public Wi-Fi where possible, and preventing screens or documents from being seen by unauthorised people.

8.2 Where the Council has authorised access through a personal device, the user must still comply with this policy and any additional security requirements set by the Council.

9. Monitoring

9.1 The Council may monitor use of its IT systems where this is necessary and proportionate. Monitoring may take place to maintain system security, investigate suspected misuse, protect Council information or meet legal and governance obligations.

9.2 The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Clerks may need to access emails so that they respond to FOI or subject-access requests. If you are using a personal email account for council business, this is still subject to data protections laws and FOI requests.

9.3 Any monitoring will be carried out in accordance with data protection law and the Council's Employee Privacy Notice or other relevant privacy information.

10. Breaches of this Policy

10.1 Failure to comply with this policy may result in action being taken. In the case of an employee, this may include action under the Disciplinary Procedure.

10.2 Serious breaches, including deliberate misuse, unauthorised access, serious data breaches or conduct that creates significant risk for the Council, may be treated as gross misconduct in the case of an employee.

10.3 Where the person involved is a councillor, contractor, volunteer or other authorised user, the Council may take other appropriate action, including removing access to systems or referring the matter through the appropriate governance route.

11. Monitoring and Review

11.1 The Council will keep this policy under review and may amend it where required by changes in law, ICO guidance, cyber security good practice, operational need or Council decision.

11.2 This policy will be applied in a way that is proportionate to the size, resources and practical needs of Watton Town Council while maintaining appropriate standards of security and professionalism.