Witham Town Council – IT and Email Policy

Witham Town Council depends on information technology, digital records and electronic communications to deliver services, support democratic decision-making and conduct its business efficiently. The Council is committed to protecting its information, systems, users and residents from accidental loss, unauthorised access, misuse, fraud, cyber attack and service disruption.

This policy establishes the rules for the secure, lawful and appropriate use of Council IT, information systems, devices, internet access, email and other electronic communications. It supports the Council's obligations under data-protection, records-management, freedom-of-information, employment and other applicable law.

The objectives of this policy are to:

- protect the confidentiality, integrity and availability of Council information and systems;
- ensure Council information is handled lawfully, securely and appropriately;
- enable staff and councillors to work effectively while reducing cyber-security and data-protection risks;
- ensure that Council records are retained, accessible and disposed of properly; and
- provide a clear process for reporting and responding to security incidents.

2. Scope

This policy applies to all persons who access, process, store, share or administer Council information or IT resources, including:

- councillors;
- employees, agency workers and apprentices;
- volunteers and interns;
- contractors, consultants and suppliers; and
- any other person authorised to use Council systems or information.

It applies whether work is carried out in Council premises, at home, at another location, or while travelling. It covers Council-owned, leased and managed devices, Council email accounts, networks, software, cloud services, files, records, data, internet access and collaboration tools.

This policy applies to Council business wherever it is conducted. Council information held on a personal device, personal email account or other non-Council system may still be subject to data-protection, records-management, Freedom of Information Act 2000 and Environmental Information Regulations 2004 obligations.

3. Definitions

For the purpose of this policy:

- **Council information** means any information created, received, collected, stored or processed for Council business, in any format.
- **Personal data** means information relating to an identified or identifiable living person.

- **Special category data** includes personal data about health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sex life or sexual orientation, genetic data or biometric data used to identify a person.
- **Confidential information** means information that is not intended for unrestricted public disclosure, including personal data, financial information, employment information, commercially sensitive information, security information and exempt or confidential meeting material.
- **IT resources** means Council devices, networks, software, applications, cloud services, email accounts, internet access, telephone systems, storage, security tools and related facilities.
- **Approved system** means a system, application, device, service or supplier that has been authorised by the Town Clerk or an appropriately delegated Council officer.
- **Security incident** means an event that may compromise the confidentiality, integrity or availability of Council information or systems. This includes suspected phishing, malware, unauthorised access, loss of a device, accidental disclosure and misdirected email.

4. Roles and responsibilities

4.1 All users

All users must:

- comply with this policy and related Council policies and procedures;
- use Council IT resources responsibly, professionally, securely and lawfully;
- protect Council information from loss, theft, unauthorised access, alteration or disclosure;
- complete required information-security and data-protection training;
- report suspected security incidents, data breaches and policy breaches immediately; and
- cooperate with reasonable investigations, audits and security measures.

4.2 Councillors

Councillors must use their Council-issued email account for Council business once one has been provided. Councillors must take reasonable steps to keep Council information separate from personal information and must comply with this policy when using Council information on any approved device.

4.3 Town Clerk

The Town Clerk is the policy owner and is responsible for ensuring that appropriate arrangements are in place to implement, communicate, review and enforce this policy. The Town Clerk may delegate operational responsibilities while retaining overall accountability.

5. Acceptable use

Council IT resources are provided primarily for Council business. Limited personal use may be permitted where it is lawful, reasonable, does not incur material cost, does not interfere with work or Council duties, does not affect system performance or security, and does not breach this or any other Council policy.

Users must not use Council IT resources to:

- carry out unlawful, fraudulent, discriminatory, harassing, bullying, threatening, defamatory or offensive activity;
- access, create, store, transmit or distribute illegal, obscene, discriminatory or otherwise inappropriate material;
- infringe copyright, licensing, intellectual-property or confidentiality obligations;
- run a private business, political campaign, commercial activity or fundraising activity without written authorisation;
- bypass security controls or access information, accounts, devices or systems without authorisation;
- introduce malware, unauthorised software, scripts, devices, services or network equipment;
- use Council systems for cryptocurrency mining, gambling or excessive non-business streaming, downloading or gaming; or
- deliberately conceal Council business from Council systems, recordkeeping arrangements or lawful information requests.

Users must act professionally in electronic communications and must not assume that email, messages or documents are private, permanent or incapable of disclosure.

6. Accounts, access and authentication

6.1 Individual accounts

Each user must have an individual account. Shared accounts must not be used unless they are necessary for a defined operational purpose, approved by the Town Clerk, appropriately secured and auditable.

Access to Council systems and information must be based on business need and the minimum access necessary to perform the user's role. Privileged or administrator access must be limited, approved and reviewed regularly.

6.2 Joiners, movers and leavers

User access must be authorised before it is provided. Managers must notify the Town Clerk promptly of a person joining, changing role, taking extended leave or leaving the Council. Access must be amended or removed promptly when it is no longer needed. Council devices, access tokens, keys, documents and other Council assets must be returned when a person leaves or when requested.

6.3 Passwords and multi-factor authentication

Users must protect their passwords, passphrases, security codes and authentication devices. They must not share them with anyone, including colleagues, managers, IT providers, family members or other third parties.

Passwords must be unique to the Council account or system, sufficiently long and not easy to guess. Users should use a Council-approved password manager where one is provided. Multi-factor authentication must be enabled and used for Council email, remote access, cloud services, finance systems, administrator accounts and other systems where it is available.

A user must change their password immediately and report the matter if they suspect that a password, account or authentication method has been compromised.

7. Devices, software and remote working

7.1 Council devices

Council devices must be protected by a screen lock, passcode, password or biometric authentication. Devices must be locked whenever left unattended and stored securely when not in use.

Users must take reasonable care of Council devices and must not leave them unattended in public places or visible in an unattended vehicle. Lost, stolen or damaged devices must be reported immediately.

Council devices must use supported operating systems and approved software. Security updates, anti-malware or endpoint protection, encryption and device-management controls must not be disabled, removed or bypassed.

7.2 Software and applications

Users must not install, download, subscribe to or use software, browser extensions, mobile applications, cloud services or other IT tools for Council business unless they are approved by the Town Clerk. This includes free or trial services.

The Council may remove unauthorised software or restrict access to protect its systems and information.

7.3 Staff Personal devices

Personal devices may only be used for Council business where permitted by the Town Clerk and where appropriate security controls are in place. At a minimum, an approved personal device must have a screen lock, current operating-system and application updates, and reasonable protection against unauthorised access.

Council information must not be stored unnecessarily on a personal device. Personal devices must not be used to store or process special category data, highly confidential information or restricted Council information unless specifically approved and appropriately secured.

Where technically possible and proportionate, the Council may require the removal of Council accounts or Council data from a personal device when access ends, the device is lost, or there is a security risk.

7.4 Remote and mobile working

When working remotely, users must protect information from being seen, overheard or accessed by unauthorised persons. Users must avoid discussing confidential matters in public places, use secure internet connections where possible, and avoid public Wi-Fi for sensitive work unless using an approved secure connection.

Paper records containing confidential information must be kept secure during transport and at the remote workplace, and returned or destroyed using approved arrangements when no longer needed.

8. Information handling and data protection

Users must handle Council information according to its sensitivity, purpose and legal requirements. Information must only be accessed, used, shared or retained where there is a legitimate Council business need.

Users must:

- collect and use the minimum personal data necessary for the task;
- check that recipients are correct before sharing information;
- use approved storage locations and approved methods of sharing information;
- restrict access to confidential information to authorised persons;
- use encryption or approved secure-transfer methods where required by the sensitivity of the information;
- keep paper records secure and dispose of them using confidential-waste arrangements where appropriate; and
- report any suspected loss, accidental disclosure, unauthorised access or other personal-data breach immediately.

Special category data and other highly confidential information must receive additional safeguards. It must not be sent to personal email accounts, uploaded to unapproved services or shared with people who do not have a clear need to know.

Users must not copy Council information to personal cloud storage, personal USB devices, personal email accounts or consumer file-sharing services unless expressly approved and appropriately secured.

9. Email, messaging and internet use

9.1 Council email

Council email accounts are for Council business and must be used professionally. Users must use their Council-issued email account when corresponding on Council business, unless an exception is authorised in writing by the Town Clerk.

Officers should normally send Council business to a councillor's Council-issued email address rather than a personal email address. Any exceptional use of a personal address must be documented, time-limited and managed so that Council recordkeeping, data-protection and information-rights obligations can be met.

Users must:

- check the recipient, address, attachments and content before sending an email;
- use Bcc where appropriate to avoid disclosing recipients' email addresses to one another;
- use approved encryption or secure-sharing arrangements for sensitive information;
- be cautious of unexpected links, attachments, QR codes, requests for payment or changes to bank details;
- report suspicious emails using the approved reporting method or to the IT provider/delegated IT lead; and
- avoid automatic forwarding of Council email to a personal email account.

Users must not set up automatic forwarding from a Council email account to a personal account unless expressly approved for a defined business purpose and with appropriate security controls.

9.2 Misdirected email

If an email or attachment is sent to the wrong recipient, or received in error, the user must report it immediately. The user must not attempt to conceal the error, delete evidence or contact the recipient in a manner that could increase risk without following the Council's incident procedure.

9.3 Messaging and collaboration tools

Council business may only be conducted through approved messaging, video-conferencing, document-sharing and collaboration tools. Where an approved tool is used for Council business, material decisions, commitments and records must be captured in the appropriate Council recordkeeping system.

9.4 Internet use

Internet access must be used responsibly and primarily for Council purposes. Users must not visit websites or use services that create a security, legal, reputational or productivity risk for the Council.

The Council may block or restrict access to websites, services, file types or categories of content where necessary to protect systems, users or information.

10. Artificial intelligence and external online services

Users must not enter confidential Council information into a public generative-AI tool, online transcription service, online translation service, external survey tool, web form, chatbot or other online service unless it has been approved for the intended use by the Town Clerk.

In particular, users must not upload personal data, confidential information, confidential meeting papers, draft decisions, financial information, contracts, security information or other non-public Council material to an unapproved AI or online service.

Where an AI or automated tool has been approved, users remain responsible for checking the accuracy, appropriateness, bias, copyright position, confidentiality and lawful use of any output before relying on it or sharing it externally. AI-generated content must not replace appropriate professional, legal, financial or human judgement.

11. Records management, retention and information rights

Email is not a records-management system. Where an email, message, document or attachment forms part of a Council decision, transaction, commitment, case, complaint, project, consultation, procurement exercise or other business record, the user must save it promptly in the approved Council recordkeeping location.

Council records must be retained and disposed of in accordance with the Council's retention schedule and records-management arrangements. Users must not retain records indefinitely in personal inboxes, personal folders or unapproved systems.

No Council record may be deleted, altered, destroyed or concealed if it is relevant, or may reasonably become relevant, to:

- a Freedom of Information request;
- an Environmental Information Regulations request;
- a subject access request or other data-rights request;
- an audit, complaint, investigation, insurance matter or legal proceedings; or
- a formal retention hold issued by the Council.

Users must cooperate with the Town Clerk, and relevant officers in locating, preserving and providing Council information in response to lawful requests.

12. Monitoring and privacy

The Council may carry out proportionate monitoring of its IT resources, systems, networks, accounts and logs where necessary to:

- protect Council information and systems;
- detect, prevent or investigate cyber-security threats, fraud, misuse or unlawful activity;
- maintain service continuity and system performance;
- investigate suspected breaches of policy or other Council procedures; and
- comply with legal, regulatory, audit or safeguarding obligations.

Monitoring will be conducted transparently, only where necessary and proportionate, and in accordance with data-protection law, the Council's privacy information and any required data-protection impact assessment.

Access to an individual's email content or files will be restricted to authorised persons and will only occur where there is a legitimate, documented reason. The Council will take account of the privacy of users and third parties, including where limited personal use is permitted.

13. Security incidents and data breaches

All users must report actual or suspected security incidents immediately to the Town Clerk. Examples of reportable incidents include:

- phishing emails, suspected scams or suspicious links, attachments or QR codes;
- suspected compromise of an account, password or multi-factor authentication method;
- malware, ransomware, unusual pop-ups, unexpected software or unusual system behaviour;
- lost, stolen or damaged Council devices, paper records, access tokens or storage media;
- unauthorised access to Council information or systems;
- sending confidential information to the wrong person, disclosing too much information or receiving confidential information in error;
- unauthorised software, cloud services or external sharing of Council information; and
- interruption to a critical Council system, service or data store.

Users must not attempt to conceal an incident, delete relevant emails or files, or take actions that could worsen the situation. Where safe and appropriate, the user should stop using the affected account or device and follow instructions from the Town Clerk.

The Council will assess, contain, investigate, document and learn from reported incidents. The Town Clerk will determine whether notification to the Information Commissioner's Office, affected individuals, insurers, police or other bodies is required.

14. Training, assurance and review

All users must complete information-security and data-protection training at induction and at intervals determined by the Council. Additional role-based training may be required for

users with responsibility for finance, personal data, system administration, records management or procurement.
The Council may carry out proportionate audits, access reviews, security testing, phishing-awareness exercises and compliance checks to assure itself that this policy is being followed and that its controls remain effective.
This policy will be reviewed at least annually and sooner where necessary following a significant incident, change in technology, change in working arrangements, change in law or regulatory guidance, or identified weakness in controls.

15. Non-compliance and exceptions

Failure to comply with this policy may result in access being restricted or withdrawn, disciplinary action for employees, action under the Council's code of conduct or other applicable arrangements for councillors, termination of a contract, and/or referral to relevant authorities where appropriate.
Any exception to this policy must be requested in advance wherever possible, authorised in writing by the Town Clerk , documented with the reason and risk controls, and reviewed regularly. Exceptions must be time-limited and must not override legal obligations.

Adopted on 16.09.2025
Reviewed 21.09.2026
For review September 2028