# SAXMUNDHAM TOWN COUNCIL

# INFORMATION TECHNOLOGY POLICY

Review Body: Resources Committee
Policy Approved: Town Council
Approval Date: November 2025
Minute Item: 90/25TC
Review Period: Annual
Next Review: November 2026

## 1. Introduction

Saxmundham Town Council ('Council') recognises the importance of effective and secure information technology ('IT') and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by Council members and staff.

## 2. Scope

This policy applies to all individuals who access or use the Council's information technology resources, including computers, networks, software, mobile devices, data, and email accounts.

In line with paragraph 1.54 of the *Practitioners' Guide 2025*, it sets out how all users - including councillors, officers, and other authorised personnel - must conduct Council business securely, responsibly, and in compliance with legal and regulatory requirements, whether using Council-owned or personal equipment.

## 3. Acceptable use of IT resources and email

The Council's IT resources and email accounts are to be used for official Council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

## 4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by the Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

## 5. Data management and security

All sensitive and confidential Council data must be stored and shared only via Council-managed systems (e.g. the @saxmundham-tc.gov.uk Microsoft 365 and SharePoint/OneDrive), with encryption in transit and at rest. Use of personal devices or unapproved third-party cloud services is prohibited. Data must be disposed of using approved secure erasure/destruction methods, in accordance with the retention schedule.

## 6. Network and internet usage

The Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

## 7. Email communication

Email accounts provided by the Council are for official communication only. Emails should be professional, courteous, and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Particular care must be taken when using email distribution groups. Before sending or replying to a group email, Officers and Councillors should consider whether it is appropriate to use 'Reply All', both for internal and external correspondence, and whether all recipients genuinely need to receive the response.

When communicating externally with multiple recipients, blind carbon copy (BCC) should normally be used to protect individuals' personal data and comply with the UK GDPR by preventing disclosure of private email addresses. In such cases, the salutation should make clear the intended audience (e.g. 'To all market traders).

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

Council-issued email addresses (e.g. @saxmundham-tc.gov.uk) and any related data are the property of the Council.

The Council is the data controller for all personal data processed through these systems in accordance with Article 4(7) of UK GDPR).

Councillors act on behalf of the Council when using these accounts for official business and must comply with this Policy, the Data Protection Policy, and the Freedom of Information Act 2000.

All correspondence sent or received during Council business forms part of the Council's official record and may be disclosable under FOI or audit inspection.

When a Councillor leaves office:

- access to the Council email account will be withdrawn;
- the Council's IT provider will securely delete the mailbox and its contents; and
- the departing Councillor must not retain or continue to use personal data obtained through their role.

This procedure ensures compliance with the UK GDPR, the Data Protection Act 2018 and the Accounts and Audit Regulations 2015.

## 8. Password and account security

Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

## 9. Mobile devices and remote work

Mobile devices provided by the Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

## 10. Instant messaging, SMS and personal email

All Council business must be conducted using Council-controlled systems, primarily the @saxmundham-tc.gov.uk email domain and any other platforms explicitly approved by the Town Clerk. Personal email accounts and consumer messaging apps must not be used to conduct Council business.

Instant messaging apps (e.g. WhatsApp, Signal, iMessage, Facebook Messenger must not be used to make decisions, issue instructions, discuss casework, negotiate contracts or otherwise conduct Council business. Limited, non-substantive use for community signposting or social coordination is permitted in volunteer/community groups (e.g. Green Team, Blue Spaces), but any substantive matter must be moved to Council email.

Operational SMS from the Council mobile may be used for real-time logistics only. Where anything substantive is agreed verbally or by text, the recipient must confirm the outcome by Council email within one working day so there is an auditable record.

Staff and councillors must not process Council information on personal devices unless expressly authorised in writing by the Town Clerk. If a work-related message is received on a personal device, the recipient must direct the sender to their Council email, forward a brief record to the Council mailbox if needed, and delete the personal message after recording.

Communications relating to Council business are information assets and may be disclosable under FOI/EIR or subject access. They must be created and retained on Council systems in line with the retention schedule. Personal messaging apps are not an acceptable records repository; screenshots or exports from such apps are not a substitute for proper records on Council systems.

Users must ensure that personal data and confidential information are only shared through approved systems, with appropriate access controls. Suspected data breaches must be reported immediately to the Town Clerk in accordance with the Data Protection Policy.

## 11. Email monitoring

The Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

## 12. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

Routine retention of Councillor mailboxes after the end of a term of office is not required and may result in unnecessary processing of personal data. Accordingly, when a Councillor's term ends, the Council's IT provider will delete the mailbox securely in line with this Policy.

## 13. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Town Clerk and the Town Council's IT provider for investigation and resolution. Report any email-related security incidents or breaches to the IT provider immediately.

## 14. Training and awareness

The Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All staff and councillors will receive regular training on email security and best practices.

## 15. Compliance and consequences

Failure to comply with this policy may be dealt with under the Code of Conduct/Disciplinary Policy and could lead to withdrawal of IT access. Serious or repeated breaches may be reported to relevant authorities where required.

All users must acknowledge that Council-issued email accounts and related data remain under Council ownership and may be monitored or withdrawn as required to ensure legal compliance and good governance.

## 16. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

This policy will also be reviewed following any significant change in legislation or the Practitioners' Guide affecting digital or data compliance (e.g. Assertion 10 requirements).

## 17. Contacts

For IT-related enquiries or assistance, users can contact the Town Clerk or the Town Council's IT provider directly.

All staff and councillors are responsible for the safety and security of the Council's IT and email systems. By adhering to this policy, the Council aims to create a secure and efficient IT environment that supports its strategic objectives.