



INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS POLICY

INCORPORATING THE SOCIAL MEDIA POLICY

1. PURPOSE

This policy sets the standards for the safe, lawful and professional use of Sudbury Town Council's (STC) information technology systems, communications systems, data, devices, cloud services and social media channels.

The Town Clerk has overall responsibility for this policy, including keeping it under review.

This policy does not form part of any employee's contract of employment and may be updated at any time.

2. SCOPE

The policy applies to:

- Employees
- Agency workers
- Contractors
- Consultants
- Volunteers
- Councillors and Officers where council systems are used
- Any third party granted access to council systems or data

The purpose of this policy is to:

- Protect council information and systems
- Ensure compliance with UK data protection law and public sector obligations
- Reduce cyber security risk
- Ensure lawful and proportionate monitoring
- Protect the reputation of STC
- Ensure digital communications are managed as public records where required

Users must:

- Use council systems primarily for legitimate council business
- Protect confidential, personal and sensitive information
- Follow all IT security controls and guidance issued by authorised support providers
- Report incidents, mistakes, suspicious activity and losses immediately
- Cooperate with investigations, audits, Freedom of Information (FOI) searches and Subject Access Requests (SAR)

Failure to comply may result in disciplinary action and may amount to gross misconduct.

3. LEGAL AND REGULATORY FRAMEWORK

STC will manage this policy in accordance with:

- Data Protection Policy
- Data Retention Policy and Information Security Procedures
- Employee Privacy Notice

- Loan of Council Property Policy
- Risk Management Strategy
- Disciplinary Policy and Procedure
- Health and Safety Policy
- Local Authority Publicity Code
- Model Councillor Code of Conduct

4. EQUIPMENT SECURITY, PASSWORDS AND ACCESS CONTROL

You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You must use passwords on all IT equipment and be particularly careful with items that you take out of the office.

All users must use unique passwords or passphrases for STC systems. They should ideally include a random string of capital and lowercase letters, symbols and numbers.

You must keep your passwords confidential and change them every three months in line with the STC Risk Management Strategy.

Passwords must never be:

- Shared with colleagues
- Written down insecurely

Where documents are password protected, ensure the password is never sent with the protected document, send in a separate email or when appropriate via an alternative method, such as a text message.

Where a device requires a Personal Identification Number (PIN), password or passkey to access council records, systems or devices a physical record of the credentials must be sealed in a dated, tamper evident envelope and securely retained by the Town Clerk. This envelope may only be opened in the presence of at least two councillors. If opened in any circumstance, the Clerk or IT lead must change the credentials immediately. The opening must be reported to all members without delay and minuted formally at the next Full Council meeting.

You must only log on to Sudbury Town Council systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

If you are away from your desk, you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

5. DEVICES, EQUIPMENT AND PHYSICAL SECURITY

Users are responsible for the physical security of all council issued devices in line with the STC Loan of Council Property Policy.

This includes, but is not limited to:

- Laptops
- Tablets
- Mobile Phones
- Removable media

Users must:

- Take reasonable care of the property
- Keep it secure at all times
- Not allow use by any third party
- Report faults immediately to your line manager
- Report loss, theft or damage immediately to your line manager
 - The police must be informed and a crime number obtained for lost or stolen electronic devices
- Return the item on request or at the end of the loan period
- Comply with all IT, Data Protection, Data Retention and cyber security policies, including password protection, software updates, secure storage, and immediate reporting of any suspected personal data breach.

If you are issued with portable IT equipment by STC, then you must make sure that it is stored safely and securely when being transported. If you are using STC IT equipment whilst in a public place, then others may be able to view your screen. Please make sure that you do not display any confidential information when using IT equipment in public.

If you are issued with any IT equipment (such as computers, monitors, keyboards, or printers) then you must agree to return it to STC on demand and in any event, on termination of your employment. You are responsible for maintaining any IT equipment issued in good condition. You are responsible for damage to any issued IT equipment, other than that caused by reasonable wear and tear.

6. SYSTEMS, SOFTWARE, CLOUD SERVICES AND DATA SECURITY

Only authorised council systems, applications and cloud services may be used for STC business. Unauthorised software must not be downloaded, installed or used without authorisation from the Deputy Town Clerk or Town Clerk. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

You must not remove or tamper with any software systems installed on the computers. If you have an issue in relation to any software installed on your work computer, then you should contact your line manager or IT Support.

Devices must not delay critical security patches and updates beyond the deadlines set by IT support.

You must not attach any device or equipment including mobile phones, tablets or USB storage devices to our systems without authorisation from the Deputy Town Clerk or the Town Clerk.

All data will be stored centrally on the STC Master Drive which will be backed up nightly by our IT contractors.

Council information must not be stored on:

- Personal devices
- Personal email accounts

Sudbury Town Council data must only be downloaded and processed on equipment owned and controlled by STC. If you foresee a business need to use any other equipment such as portable devices you must have the prior written permission of the Deputy Town Clerk or Town Clerk and a full data risk assessment in place.

USB Storage is prohibited unless specifically authorised by the Deputy Town Clerk or Town Clerk. Where removable media is approved it must be:

- Encrypted
- Asset logged
- Used only for specific business need
- Securely wiped after use

Data should be handled according to its sensitivity and in line with Data Protection and Data Retention Policies. Sensitive data requires additional access controls and sharing restrictions.

We monitor all e-mails passing through our system for viruses. You should exercise caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

You must inform the Deputy Town Clerk or the Town Clerk immediately if you suspect your computer may have a virus.

7. ARTIFICIAL INTELLIGENCE (AI) AND AUTOMATED TOOLS

No STC information may be entered into public AI systems unless formally approved.

The following must never be entered into unapproved AI tools:

- Personal data
- Payroll information
- Legal advice
- Confidential minutes
- Procurement information
- Staffing matters
- Complaint records
- Safeguarding information
- Restricted committee papers

Any AI generated content must be:

- Fact checked
- Reviewed by a human

- Checked for bias and hallucination risk
- Checked for copyright risk
- Accessibility checked before publication

8. EMAIL, MESSAGING AND DIGITAL COMMUNICATIONS

You must use the STC standard e-mail signature and disclaimer for all emails. Adopt a professional tone and observe appropriate etiquette when communicating with third parties by email.

Remember that emails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved.

It is possible to enter into a legally binding contract via email. If your job role involves the negotiation of terms which could form a contract, then you should ensure that all correspondence is headed 'Subject to Contract'.

You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails.

You should avoid the use of slang, emojis and 'text speak' when sending work emails.

You must not:

- Auto-forward STC email to personal accounts
- Use personal email for council business
- Send or forward private (non-council business) emails
- Use another user's mailbox without authority
- Send messages under an assumed name
- Send offensive, discriminatory, harassing or defamatory material
- Send or forward chain mail, junk mail, cartoons, jokes or gossip
- Send or forward private emails at work which you would not want a third party to read
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to others who do not have a real need to receive them

STC does not permit access to web-based personal e-mail such as Gmail or Hotmail on our computer systems at any time due to additional security risks.

Where personal or confidential data is sent externally, approved encryption or secure sharing methods must be used. This could include password protection or encryption tools built directly into Outlook and Microsoft 365.

Bulk emails must use BCC or approved mailing tools.

Any email sent to the wrong recipient containing council information must be reported immediately to the Person Responsible for Data Protection or the Town Clerk.

STC business must not be conducted through personal WhatsApp, Signal, messenger or similar services unless:

- Expressly authorised
- Records can be retained
- Messages are searchable
- Content can be disclosed under FOI and complaints processes

Disappearing messages must not be used for STC business.

9. USING THE INTERNET, INCLUDING PERSONAL USE

Internet access is provided primarily for business purposes. Occasional personal use, including sending emails, web browsing and making telephone calls is permitted where it:

- Is minimal
- Takes place mainly during breaks
- Does not interfere with work
- Does not create cost or cyber risk
- Personal emails should be labelled 'Personal' in the subject header
- Complies with all STC policies and procedures

You must not access:

- Illegal material
- Extremist content
- Pornography
- Gambling sites
- Malicious downloads
- Pirated media
- Offensive or discriminatory content

Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

STC may block or restrict access to some websites and categories of content.

You must not use STC systems to post on chat rooms or social media sites unless you are doing so as part of your job. For more guidance in this area please refer to the Social Media section of this policy.

Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Inappropriate use or excessive personal use will be dealt with under the STC Disciplinary Procedure.

Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature)
- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients
- A false and defamatory statement about any person or organisation
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy)
- Confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties)
- Unauthorised software
- Any other statement which is likely to create any criminal or civil liability (for you or us)
- Music or video files or other material in breach of copyright.

10. DISPLAY SCREEN EQUIPMENT AND SAFETY

Users who regularly use display screen equipment must:

- Complete workstation self-assessments
- Take regular screen breaks
- Report discomfort or injury promptly to your line manager
- Ensure chairs, screens and desks are safely arranged
- Ensure cables and charging equipment do not create trip hazards

Users are entitled to request:

- Workstation assessment support
- Ergonomic equipment where justified
- Eye test arrangements in accordance with STC policy

11. INCIDENT REPORTING, CYBER EVENTS AND DATA BREACHES

The following must be reported immediately:

- Phishing emails
- Suspicious links clicked
- Ransomware messages
- Unexpected Multi-factor Authentication (MFA) prompts
- Lost or stolen devices
- Suspected malware
- Accidental disclosure
- Wrong-recipient emails
- Unauthorised access
- Unusual system behaviour

Potential personal data breaches must be escalated immediately to the Person Responsible for Data Protection to assess statutory reporting obligations.

Failure to report a potential data breach promptly may itself be treated as misconduct.

12. MONITORING

Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications.

For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise. We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business.

STC may monitor the use of its systems for:

- Cyber security
- Service continuity
- Legal compliance
- Safeguarding information
- Detecting misconduct
- FOI searches and SAR compliance
- Records retention
- Business continuity

All monitoring will be:

- Lawful
- Proportionate
- Transparent
- Risk-based
- Undertaken in line with the employee privacy notice

13. USE OF PERSONAL DEVICES FOR WORK PURPOSES

STC's general rule is that personal devices are not allowed to be used for business purposes. However, there may be circumstances where you need to use certain personal devices (such as smartphones, laptops and tablets) for work. Any use must be in accordance with the following rules:

- Any personal device (such as smartphones, laptops and tablets) must be approved by the Town Clerk and/or IT Support before it can be connected to STC systems and be used for work purposes. STC may require you to implement additional security measures prior to approving your device for work use.
- When accessing work systems (e.g. intranet, CRM, cloud storage) from a personal device, you must only use approved applications for file sharing, communication and any remote work.
- When accessing work systems from a personal device, you must always connect through a secure Virtual Private Network (VPN).
- You must not use personal email, storage or messaging apps for work related communication or data transfer.

- Any software systems installed on your device by STC to allow your device to be used for work must not be tampered with or removed by you.
- STC reserves the right to monitor, intercept and remove any content on your device which has been created by STC on our behalf to the extent permitted by law or for our legitimate business purposes. Please see the Data Protection and Privacy Notice for more detail. As your device is a personal one, we are aware that inadvertent monitoring, interception, review and removal of personal data may occur. You should have no expectation of privacy in relation to any data on the device if you are using it for work purposes.
- You must delete any data relating to STC business which is stored locally on your device as soon as it is no longer required.
- You must pay all costs associated with your device and its use, including technical support.
- You must cooperate with STC and allow your device to be inspected at any time on request. You will provide any necessary passwords or login details to enable us to have full access.
- You must report any loss of the device immediately to the Town Clerk.
- If you leave STC's employment or propose to sell or transfer your device to someone else, then you agree to present your device to STC prior to transfer / termination to allow STC to remove all business software and data from it.

Any breach of these rules may result in us revoking your permission to use your device for work purposes. It may also result in disciplinary action up to and including dismissal or, in the case of a contractor or agency worker, the termination of your engagement.

14. BREACHES OF THIS POLICY

Any breaches of this policy will be handled under our Disciplinary Policy. In the case of agency workers, contractors, casual workers and temporary staff, we reserve the right to terminate your engagement in the event of a breach or an alleged breach of this Policy.

Certain behaviours in breach of this Policy may give rise to a criminal offence or other public concern. We may pass any evidence collated to the police or other relevant authority.

If you become aware of conduct of others which may be in breach of this policy, you should report your concern immediately to your line manager. Our Whistleblowing Policy provides further guidance.

15. MONITORING AND REVIEW

The Town Clerk is responsible for monitoring the implementation and effectiveness of this policy, supported by the Deputy Town Clerk, the Person Responsible for Data Protection, managers and the Council's appointed IT support provider where appropriate. Compliance with this policy will be monitored through security incident reports, data breach investigations, audits, system monitoring, user feedback and changes in legislation, technology or cyber security risks.

The policy will be reviewed at least every five years, or sooner where there are significant changes in legislation, regulatory guidance, National Cyber Security Centre (NCSC) recommendations, organisational requirements, or following a significant cyber security incident, data breach or identified weakness in the Council's information governance arrangements.

SOCIAL MEDIA POLICY

1. PURPOSE

This policy is in the place to minimise the risks to our organisation through the use, both business related and personal use, of social media.

This policy does not form part of any employee's contract of employment and may be updated at any time.

2. SCOPE

This section applies to:

- Official STC social media accounts
- Officer use of social media for council business
- Councillor use where STC branding, council business or civic roles are referenced
- Personal use that may affect STC
- Professional networking sites
- Video and community platforms
- Messaging channels used for public engagement

3. WHAT IS SOCIAL MEDIA ?

'Social media' includes online communications and applications through which communications, media and messages can be shared. The 'social' aspect refers to the fact that you are interacting and sharing with other people.

There are different types of social media, examples include:

- Social networks: the most well-known form of social media, such as Facebook, LinkedIn and X.
- Media sharing networks: these are used for sharing photographs, videos and other forms of media, such as Instagram and Snapchat.
- Discussion forums: these are forums where topics of interest can be discussed, such as Reddit and Mumsnet.
- Consumer review networks: these are sites which allow you to leave reviews in relation to products, services and brands such as TripAdvisor.
- Blogs: these are used for publishing and commenting on articles on different topics. Many businesses have their own blogs on their corporate web platforms, and many individuals have blogs chronicling things they wish to share.

4. OFFICIAL ACCOUNTS

Only authorised officers may create, manage or post on official STC accounts.

Post must be:

- Accurate
- Politically neutral unless lawfully required

- Respectful
- Accessible
- Retained where they form public records
- Approved in line with delegated communications procedures

Official STC channels must clearly state expected response times and must make clear they are not to be used for emergencies, safeguarding matters, crimes in progress or urgent service failures.

5. PRE-ELECTION PERIOD AND PUBLICITY CONTROLS

During the pre-election period, all STC operated social media channels must comply with the Local Authority Publicity Code and current LGA guidance.

Content must remain strictly politically neutral and must not:

- Promote or oppose any political party
- Promote any candidate or campaign
- Amplify councillor campaign messaging
- Comment on politically controversial issues unless legally necessary for service delivery
- Publish content that could reasonably be perceived as influencing voters

Additional approval controls may be imposed by the Town Clerk during pre-election periods.

6. ACCESIBILITY AND INCLUSIVE COMMUNICATIONS

All official social media communications must meet applicable public sector accessibility standards. This includes, where relevant:

- Captions or subtitles for video
- Alternative text (Alt text) for images
- Readable colour contrast
- Plain English drafting
- Accessible document links
- Avoiding text heavy image posters where possible

7. COUNCILLOR, OFFICER AND CIVIL ROLE SEPARATION

STC managed accounts must not be used for party political purposes or personal campaigning. Councillors must keep separate:

- Council civic role communications
- Personal political views
- Election campaigning messaging
- Party political activity

Where mayoral, chair or civic accounts are used, content must remain non-party political unless clearly separate from STC managed channels.

8. PERSONAL USE OF SOCIAL MEDIA

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

There may be occasions when your actions on social media in a personal capacity impact your employment with STC. Even if you do not name STC as your employer, people who know you and where you work may still make an association with STC, or people might use 'jigsaw' identification (putting information together from more than one source) to discover you work for STC. We have a right to protect our legitimate business interests.

Users must not post anything that:

- Damages STC reputation
- Discloses confidential information
- Undermines public trust
- Harasses or discriminates
- Prejudices investigations or staffing matters
- Compromises political neutrality requirements
- Interferes with live complaints, licensing, planning or standards matters
- Uses STC logos

Users must not act inappropriately in your interactions on social media. This includes acting in a discriminatory manner, harassing others or being rude online. Users must not make any derogatory statements about any other person or business.

If in a social media profile, you disclose your association with STC, then you should make sure that all postings maintain an appropriate professional style and content.

You must make clear that any opinions given are your personal ones.

You must not publish anything which may bring STC, or others associated with STC into disrepute.

You must not publish anything that would be in breach of copyright or the rights of others.

You must not post to social media other than in your own name, and you must not pretend to be another person, real or non-existent.

Any misuse of social media, including content that disparages or reflects poorly on STC should be reported to the Town Clerk.

The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment, you must provide STC with a

copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.

9. BUSINESS USE OF SOCIAL MEDIA

It is important that if you are posting or commenting on social media as a representative of the Council, you behave appropriately and in a way which upholds our values.

If your duties require you to speak on behalf of Sudbury Town Council on social media, you must seek approval for that communication from the Town Clerk. If you are contacted for comments about the business for publication you should contact the Town Clerk for support. Do not respond without written approval.

Any circumstance where you are posting as a proxy for the Council (so that the post reads as if it came directly from STC) or as our representative, and any post or comment on a platform where your association with STC is visible is regarded by us as 'business use' of social media and the following rules apply:

- You should avoid slang.
- You should avoid inappropriate or rude language.
- You should only comment on matters which fall within your expertise or knowledge.
- You should not make any false or misleading statements.
- You should check spelling and grammar before posting any comments online.
- You should only post on topics which are relevant to our business
- You should never provide references for other individuals on social or professional networking sites. These references, positive or negative, can create legal liability for STC and for you.
- You should not post any confidential or otherwise sensitive information.
- If your post is posting as our representative, you should make sure that any post is approved in advance by the Town Clerk.

10. PUBLIC RECORDS, MODERATION AND EVIDENCE RETENTION

Official posts, direct messages, screenshots, moderation actions and complaint related exchanges may form public records and must be retained in line with the STC Data Retention Policy.

Before removing abusive, threatening, defamatory or safeguarding related content, authorised officers must preserve evidential screenshots where they may be:

- Legal relevance
- Safeguarding relevance
- Standards compliance relevance
- Police relevance
- Insurance relevance

11.AI-GENERATED MEDIA, IMPERSONATION AND MISINFORMATION

AI-generated text, audio, video or images must not be published from STC official accounts without:

- Human approval
- Factual verification
- Copyright review
- Accessibility review
- Misinformation risk assessment

Suspected fake accounts, impersonation, scam posts, manipulated media, cloned council pages or misinformation affecting public safety or trust in council services must be escalated immediately to the Business Manager or the Town Clerk.

12.MONITORING

STC may monitor, intercept and review any social media activity carried out using our IT and communications systems as permitted under our Data Protection Policy to monitor compliance with this policy.

STC may monitor, intercept and review social media accounts and posts if they are public. STC may also review any content or post in a private or 'member only' forum or any deleted post in either a public or private forum which is brought to our attention (for example by the provision of screen shots).

13.BREACH OF THIS POLICY

Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Policy Name	Information Technology & Communication Systems Policy, incorporating Social Media Policy
Current Status	Adopted
Approved	September 2026
Next Review Date	July 2031
Policy Owner	Deputy Town Clerk