EMAIL, INTERNET, SOCIAL MEDIA AND COMPUTER USE POLICY AND BEST PRACTICE

Adopted at the XXXXXXX meeting of Eastleigh Town Council

Subsequent amendments agreed as follows:

Version	Owner	Date Approved	Minute Ref	Action?	Website updated	Next review
V1-2025	Town Council	23/07/2025	30 / 25 / 2			

Introduction

Eastleigh Town Council provides internet access and Wi-Fi within some council facilities, along with email accounts and applications for use by councillors, employees and volunteers who have access to a desktop PC, laptop, smartphone, tablet or other computing device. This document sets out the council's policy for the use of these facilities and services, and for general computer use.

Objectives

The objectives of the policy are to ensure that the services made available to users are used:

- In accordance with the values, principles, and standards of the council
- Appropriately, in terms of council time and resources consumed
- Lawfully
- So as not to threaten the integrity of the council's IT services

Security

Access to the council's computers and cloud services is restricted to individual users who have been given access rights by the Town Clerk.

Access for each user is controlled by means of a password and two factor authentication. Passwords must be:

- sufficiently complex to mitigate the risk of brute force attacks
- not contain personal details or information that may be easily guessed or obtained through phishing attacks
- not reused across different user accounts or services

Passwords must never be disclosed to others, including council officers, staff, and service providers. Disclosure could result in internet or email misuse being attributed to the owner of the password.

Care should be taken not to leave any computer device connected to council services unattended and unlocked.

Employees and councillors should be aware that any device used for council-related work whether council-issued or personal and all data stored on it, including emails, documents, messages, and notes, may be subject to a Freedom of Information request under the Freedom of Information Act 2000, or a Subject Access Request under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Under no circumstances should anyone outside of the council be given access to the council's computer-based services without first obtaining permission from the Town Clerk. Breaches of security of the computer systems e.g. disclosure of personal passwords, thus giving unauthorised access to the system, may result in disciplinary action which could result in dismissal for employees and a referral to the monitoring officer for breach of the councillor's code of conduct or direct action by the Information Commissioners Office

Personal devices can access council provided WIFI using the 'Guest' network only. Under no circumstances should contractors, visitors or customers be given access to private council networks unless permission has been given by the Town Clerk.

Best Practice

This section of the document provides best practice on the acceptable use of the council's email and internet services and electronic databases.

Training

All employees at the start of their employment, and councillors at the start of their term, will be provided basic training on how to use council provided email and office applications, along with how to save and share documents.

Email Usage

The council's email system enables users to email other employees, councillors and external individuals and organisations. Users should be aware that once an email is sent outside the council, it is beyond the council's control and is not guaranteed to be confidential.

Prohibited Activities and Internet Use

The following activities are prohibited:

- Examining, changing, or using another person's files, output or username without explicit authorisation.

- Sending or forwarding any material that is obscene, defamatory, or hateful, or intended to annoy, harass or intimidate others.
- Sending or forwarding emails which are likely to damage the reputation of the council or risk security of the council's data or cloud services.
- Sending or forwarding electronic chain letters
- Soliciting emails that are unrelated to council activities or soliciting non-council business for personal gain or profit
- Intentionally interfering with the normal operation of the council's network, including spreading computer viruses and generating sustained high-volume network traffic
- Linking your council email address to any personal social media profile or billing/account services (e.g., iTunes, PayPal).
- Intentionally sending or forwarding attachments of such size as to cause disruption to the councils' network
- Sending inappropriate or unlawful material, including content of a sexual, racist, discriminatory, or harassing nature
- Visiting internet sites that contain pornographic, obscene, or otherwise objectionable material.
- Using the internet for gambling or illegal activities
- Accessing social networking sites for non-council related activities during working hours or when it interferes with work duties
- Making or posting indecent, offensive, or discriminatory remarks, proposals, or materials.
- Uploading, downloading, or transmitting commercial software or copyright material in violation of copyright
- Revealing or publicising confidential information, including financial details, personal information, council confidential files, and network access information
- Other inappropriate uses as identified and publicised by the council's IT Administrator

Acceptable Personal Use of Council IT Services and Internet

The limited use of council IT services for personal purposes is permitted, subject to the following conditions: Employees and councillors who use the council's facilities for personal use expressly consent to the conditions detailed in this document. Employees and councillors who do not accept the conditions under which the councils email facilities can be used for personal purposes must not use the facility

- Personal use must occur outside of normal working hours or during break times and must not interfere with the performance of work duties or reduce resources available to others.
- Personal use must not cause damage to council computers or networks, nor cause difficulty or distress to others.
- Personal use must not breach any prohibited activities or internet use as detailed elsewhere in council policies.

- Users should be aware that council IT services and internet use may be monitored and searched to meet legal obligations and legitimate council interests.

Email Awareness

- Email is not a secure method of transmission – it should not be assumed that any email communication is secure or private while in transit between our cloud server and the recipient's server. Users should take this into account particularly when emailing confidential or sensitive information.

Email Best Practice

Users should:

- Ensure that each email has a specific target audience
- Be selective, especially when deciding who should be copied in on an email. This ensures that only those who really require the information, receive it and avoids wasteful emails and wasted time/resources
- Information for the attention of several users should be saved to SharePoint and an email containing the link sent to notify readers of its location
- Users should minimise use of attachments but instead locate the file in SharePoint and share the link to that file. The options of who can view, edit and download should be verified by the sender prior to copying the link to the email message body
- OneDrive is a secure alternative for sending batch files. To prevent duplication, files should be saved to a folder, and that folder shared as per the above instructions.
- For assistance with checking the size of emails and attachments, please contact the council's IT Administrator
- When sending emails outside of the Town Council where recipients do not know each other, the recipient addresses must be entered into the BCC (blind copy) field. This is limited to a maximum of 10 recipients; for larger distributions, an appropriate bulk mailing list system must be used. Users should contact the IT Administrator if assistance is required
- Employees and councillors should be reminded that folders in Outlook also hold the one-year retention. Any emails or attachments should be moved to SharePoint. Employees should consider their ROPA (Record of Processing Activities) and retention period before moving emails over
- Time should be set aside on a regular basis for "housekeeping", to delete old or unwanted items from mailboxes. This is essential to ensure the efficient operation of the email system and helps to keep mailboxes organised. The 'Inbox', 'Sent Items' and 'Deleted Items' folders should be examined as part of a housekeeping routine, performed at a minimum frequency of once a month

- The council's email system should not be used to circulate non-council related information such as party-political activities, items for sale, personal social events and news items
- Unless necessary, it is strongly recommended that only generic email addresses are promoted online, booking forms, application forms or printed materials. This supports good security measures by limiting phishing emails and allows other officers to continue with tasks if there is an absence

Email Etiquette

Email is about communication with other people, and as such some basic courtesy should be observed.

- Always include a subject line in your message - it should briefly summarise what your email is about. This helps the recipient understand the purpose of the message and makes it easier to find later.
- When replying to an email, include enough of the original message to provide a context
- An email signature is an effective way of providing detail of who is sending the email and the details of how to respond is set by a global policy automatically. Any additional details for that signature should be requested from the Town Clerk
- Consider the tone and language used, and the use of plain English. When sent externally emails represent and reflect upon the council
- Avoid using capitals throughout as this may be interpreted as shouting
- Email communication is not the best method of communication for urgent action but can be used to follow up urgent conversations over the phone or in person
- Use "Reply All" only when your response is relevant to everyone included in the original message
- Emails may be sent at any time; however, there is no expectation of an immediate response, and replies will be given as availability permits

Internet Usage

Use of the internet by council employees and councillors is permitted and encouraged where such use is relevant to, and in pursuit of, the work of the council. Internet use is regarded as an aid to the normal responsibilities of the employee and councillors; it should be used in a manner that is consistent with the council's standard of proper conduct, courtesy and customer care. Basic training will be provided for all internet users as well as internet etiquette. More advanced training will be provided where necessary.

Social media

The council respects an employee's and councillors right to a private life. However, the council must also ensure that confidentiality and its reputation are protected. It therefore requires employees and councillors using social networking websites to:

- Ensure that they do not conduct themselves in a way that is detrimental to the council
- Take care not to allow their interaction on these websites to damage working relationships between members of staff, councillors, customers, and members of the public.

You must avoid making any social media communications that could damage our business interest or reputation, even indirectly. You must not use social media to:

- Defame or disparage or make any other inappropriate comments about the council, elected members, our staff or any client or other third party, including the work, staff and elected members of any other local or regional authority or government.
- Harass (including sexually harass), bully or unlawfully discriminate against staff, clients or other third parties.
- Make false or misleading statements; or
- Impersonate colleagues or third parties

Because social media interactions can be copied and widely disseminated in a way that you may not be able to control, the council will take a particularly serious view of any misconduct that occurs using social media.

You should make it clear in social media postings, or on your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address. 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.

You must not operate a social media account or profile or express an opinion that purports to be operated/made on behalf of the council without express permission to do so from the Town Clerk. You must not comment on social media about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on social media.

You are not permitted to add business contacts made during your employment to personal social networking accounts.

Any misuse of social media that you see should be reported to your manager. Breach of this policy may result in disciplinary action up to and including dismissal for employees and a referral to the monitoring officer for breach of the councillor's code of conduct or direct action by the Information Commissioners office. You may be required to remove any social media content that we consider constitutes a breach of this policy.

Security and Identity theft

Employees and councillors should be aware that social networking websites are a public forum, particularly if the employee or councillor is part of a "network." Employees and councillors should not assume that their entries on any website will remain private. Employees and councillors should never

send abusive or defamatory messages. Employees and councillors must also be security conscious and should take steps to protect themselves from identity theft, for example, by restricting the amount of personal information they give out. Social networking websites allow people to post personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees should:

- Ensure that no information is made available that could provide a person with unauthorised access to the council and/or any confidential information
- Refrain from recording any confidential information

Database Usage

In accordance with the UK General Data Protection Regulations (UK GDPR) and The Data Protection Act 2018, no personal data from any council databases should be given out to external parties under any circumstance.

Council-related personal data or databases may only be stored on laptops, or personal home-based computers where this is specifically authorised and appropriate safeguards are in place. Unauthorised storage or sharing of personal data may result in legal action by affected third parties.

It is important to note, that if an employee has downloaded the TEAMS or outlook app on their personal device, they must not sync contacts from work to personal or vice versa.