Wilton Town Council

Information Technology (IT) and Email Policy

Document history

Status	Date	Adopted Date	Minute Ref	Summary of Changes
Original	02/09/2025	02/09/2025		New policy to incorporate existing Email Policy in readiness for Assertion 10 – AGAR 2025/2026
Revision 1				
Revision 2				
Revision 3				

Next review date September 2028

1. Introduction

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

1.2 This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

1.3 All staff and councillors are responsible for the safety and security of the council's IT and email systems. By adhering to this IT and Email Policy, the council aims to create a secure and efficient IT environment that supports its mission and goals.

2. Scope

2.1 This policy applies to all individuals who use the council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Purpose

3.1 The purpose of this policy is to ensure the proper use of Wilton Town Council's internet, email and telephone systems and make users aware of what the Town Council deems as acceptable and unacceptable use of its communication systems. 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

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

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

5. Data management and security

5.1 All sensitive and confidential data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

6. Network and internet usage

6.1 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

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

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

7.3 The following rules MUST be adhered to by all users within the Town Council. It is prohibited to:

- Send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks. If you receive an email of this sort, you must notify your line manager.
- Forward a sensitive or controversial message without acquiring permission from the sender first.
- Forge or attempt to forge email messages.
- Disguise or attempt to disguise your identity when sending mail.
- Access another employee's email unless:- (a) the employee has given their consent, (b) their email needs to be accessed by their line manager for specific work purposes whilst they are absent or (c) an appropriately authorised investigation is being undertaken.
- Send email messages using other person's email address without permission. It should be stated in the message that you are the author of the message
- Copy a confidential message or attachment belonging to another user without permission of the originator.

7.4 The following disclaimer will be added to each outgoing email:

All Wilton Town Council emails and attachments are private and intended solely for the use of the individual or entity to whom they are addressed.

Some emails may contain information that is legally privileged, or copyright protected. Any views or opinions expressed in emails are solely those of the author and do not necessarily represent those of Wilton Town Council.

Unauthorised use (disclosure, storage or copying) of emails is not permitted. If you are not the intended recipient, please destroy all copies and inform the sender by return email. Please note, however, that unencrypted emails sent to the council can be intercepted by an unauthorised third party; as the information contained within is not protected.

Wilton Town Council reserves the right to monitor, record and retain any incoming and outgoing emails for security reasons and for monitoring internal compliance with the Council's policy on staff use. Although software may be used to check, monitor and/or block the contents of emails and attachments to identify the presence of malware; you are advised that you open any attachments at your own risk.

As a public body, the Council may be required to disclose this email (or any response to it) under the Freedom of Information Act 2000 unless the information in it is covered by an exemption in the Act.

8. Password and account security

8.1 The 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

9.1 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. System Monitoring

10.1 Whilst respecting the privacy of authorised users, under the Data Protection Code of Practice, Wilton Town Council maintains its legal right to monitor and audit the use of email by authorised users under the Lawful Business Practice Regulations 2000.

10.2 Users expressly waive any right of privacy in anything they create, store, send or receive on the Town Council's computer system. The Town Council can, but is not obliged to, monitor emails without prior notification.

If there is evidence that you are not adhering to the guidelines set out in this policy, the Town Council reserves the right to take appropriate disciplinary/legal action, which could result in termination of employment.

10.3 Users expressly waive any right of privacy in relation to any incoming or outgoing telephone calls made on the Town Hall telephone landline system. The Town Council can, but is not obliged to, monitor all incoming or outgoing telephone calls in accordance with the Telephone Monitoring Policy.

11. Retention and archiving

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

12. Personal use of Internet and email/Social media

12.1 Subject to this policy, personal use could include but is not solely restricted to areas such as online banking, shopping, entertainment, leisure activities or bookings, personal research and web-based email services e.g. MSN and Hotmail. All such use is carried out at users' own risk and the Council does not accept responsibility or liability for loss caused as a result of use of the Internet.

12.2 The Town Council permits employees to use their council issued PC's free of charge to access the Internet and send/receive email for personal/ developmental use. Employees wishing to use internet/email access for personal purposes are deemed to have agreed to the following terms and conditions:

12.3 This permission only applies to times OUTSIDE recorded working hours.

- does not interfere with the performance of your official duties;
- does not take a priority over your work responsibilities;
- does not incur expense on the Council
- does not have a negative impact on the Council in any way, nor damage its reputation.
- Unless you have specific prior permission from your line manager, you should not give your work email address as one of your contact details for regular extra-curricular/social/voluntary commitments outside work.

- Any private research using the Internet must be restricted to the employee's lunch time, rest period or break period, as agreed by your line manager.
- Employees are not allowed to access social media websites for personal use from the council's computers or devices during working time and they must not be left running 'in the background', whilst at work. These provisions also apply to personal computers and mobile devices.
- Leaving Social Media sites 'running' constantly in work time is considered to be a breach of the acceptable use of the internet policy.
- Where it is essential to send an email (in your own time) from work in relation to extra-curricular commitments, it must be prefaced with a disclaimer, making clear that the Town Council is in no way connected to the content of your email. The Personal Disclaimer must appear in CAPS and read "This is a personal message from the sender, and no links with Wilton Town Council are intended, nor should they be inferred".
- If you have one-off social or non-work requirement to send an email from work (in your own time) i.e. chasing up a planning application, giving a reference for a friend, booking a venue etc, it must be prefaced with the Personal Disclaimer above, making it clear that the Council is in no way connected to the content of your email.
- Do NOT use your work email address for any non-work communication if there is any possibility that the recipient will be influenced (either positively or negatively) by receiving a communication from an officer of the Town Council.
- To avoid cluttering the system with unwanted adverts or other material, please do not sign up for personal direct mail using your work email address. For example, if you have used the internet (in your own time) to buy goods or services, and are invited to subscribe to 'news of other products' please click 'no' or provide your home email address as the point of contact.
- Many people receive jokes or humorous articles from outside the organisation. Users must consider whether anyone is likely to take offence if you pass material on. Passing on offensive material via the work system is a disciplinary matter and may result in legal action or termination of employment.
- Users are responsible for their individual accounts and as such they should take all reasonable precautions to prevent others from being able to use their account.
- Do not send system account information by email, this includes user accounts, passwords, internal network configurations, addresses or system names. This information is confidential.
- Users must not manually or automatically forward Council work-related emails that contain personal or sensitive (including commercially sensitive) information, to their own personal/home email account, e.g. Google mail, Yahoo, Hotmail etc. This is strictly prohibited.
- Should users have a legitimate business need to access work related emails and/or Council systems from home, remote access may be arranged formally subject to approval of the relevant business case by the user's line manager.
- Before sending emails that contain personal information users must consider whether email is the most appropriate method of communication and ensure that the potential risks associated with emailing personal data, e.g. email being sent to the wrong recipient or wrong attachment being sent is minimised.

- Users access to, and the use of non endorsed "cloud storage & facilities" e.g. Dropbox & Google Docs, must be approved by the Town Clerk. For those facilities where approval has been granted, any use of such cloud facility must not be used for the purpose of storing or sharing confidential, personal or sensitive information.
- If you are informed of the presence of a virus, do not make colleagues aware by any electronic means, as by doing so you may inadvertently spread the virus. Contact the Town Clerk by telephone immediately in such circumstances.
- If users mistakenly access inappropriate information, they must immediately advise their Line Manager. This will protect them against any claim that they have intentionally violated this policy. Users must promptly disclose to their line manager any messages or images they receive that are inappropriate or make them feel uncomfortable.
- Use the “Out of Office Assistant” if you know you will not be able to access your Email system for a period of time. Good practice is to explain when you will be returning to work and whom the person can contact in your absence to deal with queries. Remember the Out of Office Assistant can be read by external organisations, so ensure your message is professional in its content.
- Using the council’s computers or devices for playing games whether via the Internet or already on the system hard drive must be restricted to the employee’s lunch time, rest period or break period as agreed by your line manager and they must not be left running ‘in the background’, whilst at work.
- Personal use of Council internet or phone systems must not incur any costs to the council. The Council reserves the right to reclaim any charges incurred.

13. Listening to Music

13.1 Listening to music at work can only take place with the prior permision of the line manager regardless of the particular medium (radio, iPod, website, etc.) and regardless of whether the employee is using personal headphones. Remember that the most important consideration is health and safety as the Council must comply with its duty to take reasonable care of all employees’ health and safety in terms of providing a safe working environment and safe working practices. Distraction to other employees and perception of a lack of professionalism by visitors is also a consideration.

13.2 NOTE: PRS and PPL - If music is played openly in a public place (which also includes a workplace, even if the general public don’t have access), whether this is on a radio, TV, CD or through the internet, any organisation first needs to have obtained a licence from both the Performing Rights Society (PRS) and Phonographic Performance Ltd (PPL). Employees who want to listen to music on radios, the internet, etc. can therefore only do so on an individual basis via headphones, or to listen to their own personal music players.

14. Abuse of Internet/email access

14.1 Any breach of this and related policies may warrant further investigation that may lead to the Council’s disciplinary procedures being invoked and in certain circumstances, may necessitate the involvement of the Police.

14.2 The Council will co-operate fully with any Audit or Police investigation. If the investigation

demonstrates that material that is accessed is offensive, e.g. pornographic, advocate's illegal acts, violence or discrimination to other people, this will be considered gross misconduct and appropriate disciplinary procedures will be followed, possibly resulting in dismissal.

14.3 Abuse of Internet/email access could include but is not exclusively:

- Accessing or distributing material that is profane or obscene (pornography), that incites illegal acts, violence or discrimination towards other people (hate literature).
- Accessing web sites, blogs or chat rooms that are offensive, unsuitable or inappropriate to the workplace
- Using language or behaviour likely to bring the Town Council into disrepute
- Using the Town Council's official role/status for personal gain
- Using the Town Council official role/status to support a specific political or issue-based campaign
- Online gambling.
- Using the equipment to contribute to fraud
- Using or passing on privileged or confidential information
- Making deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Harassing another person. Harassment occurs when a person engages in unwanted conduct which has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that person. If users are told by another person to stop sending them messages, they must stop. Further guidance on harassment is available through the Council's Dignity at Work Policy.
- Knowingly or recklessly posting false or defamatory information about a person or organisation.
- Posting, forwarding or replying to chain letters or engaging in "spamming". (Spamming is the word used to describe the sending of annoying or unnecessary messages to a large number of people).
- Officers will not 'speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council), unless authorised to do so.
- The personal use of email or Internet access must be completely in accordance with this and any other Wilton Town Council policy.

15. Legal risks

15.1 Email is a business communication tool, and users are obliged to use this tool in a responsible, effective and lawful manner. While email seems to be less formal than other written communication, the same laws and guidelines apply.

15.2 Users should note that an Email has the same significance and legal implications as a signed letter. Furthermore, users should never send 'off the record' Emails – nothing is 'off the record' where the law requires disclosure of information.

15.3 Users should be aware of the legal risks of email:

- If you send or forward emails with any libellous, defamatory, offensive, racist or obscene remarks, both you and the Town Council can be held liable. In addition, it may be considered to have been an infringement of the disciplinary procedure.

- If you unlawfully forward confidential information, you and the Town Council can be held liable.
- If you unlawfully forward or copy messages without permission, you and the Town Council can be held liable for copyright infringement.
- If you knowingly send an attachment that contains a virus, you and the Town Council can be held liable.

15.4 Whilst it can sometimes be helpful to maintain a chain of e-mails on a particular subject, long chains of emails are best avoided. Information from e-mails may be required to answer Data Protection/FOI requests and difficulties can arise if a chain of e-mails refers to data which should not be disclosed. Users should consider this when responding to or creating an e-mail chain and, where appropriate, create a fresh message.

15.5 Read and delete emails regularly. Unless notification has been made by an "out of office" message emails should be responded to within three working days. Keep your 'Inbox', and 'Sent' folder contents to a minimum. Regularly delete 'Deleted items' and associated sub-folders.

15.6 Please follow the guidelines in this policy to minimise the legal risks to yourself and the Town Council. If any user disregards the rules set out in this policy, the user will be fully liable, and the Town Council will disassociate itself from the user as far as legally possible.

15.7 Users should be aware of UK and international laws that govern the use of emails. These include any statutory modifications or amendments but are not limited to:

• Copyright
• Libel and Defamation
• Public Records Acts 1958 and 1967
• Data Protection Act 1998
• Human Rights Act 1998
• Freedom of Information Act 2000
• Regulation of Investigatory Powers Act 2000
• Electronic Commerce (EC Directive) Regulations 2002

15.8 The preferred method when emailing councillors is the use of the 'cc' function.

16. Access to Systems (General)

16.1 Should any employee attempt to gain access to a system for which they do not have authority, they will be acting in breach of the Computer Misuse Act 1990. This will be regarded as gross misconduct and the disciplinary procedure will be invoked.

16.2 Employees are reminded that the Computer Misuse Act 1990 specifies the following as criminal offences: -

- unauthorised amendment or damage to data.
- unauthorised access, or contact with other systems, with criminal intent.

16.3 Any employee found to be attempting to gain unauthorised access to any internal mailbox without authority will also be subject to disciplinary procedure.

16.4 All PCs are virus protected, and virus shields updated regularly.

16.5 All PCs are provided with a spam filter which can be updated regularly.

16.6 Only DVD/CDs/Portable Device provided by the Town Council are to be used in any workstation, without specific authority.

16.7 Employees must gain written authorisation from the Town Clerk before installing any software onto the Town Council system.

16.8 Any software provided by the Town Council can only be removed with specific authority.

17. Unsolicited Communications

17.1 No employee can be held responsible by the Town Council for the contents of any unsolicited communication, regardless of its contents, when received through any systems operated and maintained by the Town Council.

18. Telephone System

18.1 Council employees must not use WTC's telephone system for personal use, except in emergencies.

18.2 This includes any mobile telephone or similar device provided by WTC.

18.3 All user need to be aware of the Council's Telephone Monitoring Policy

19. Personal Telephones / Hand Held devices

19.1 Use of personal telephones / hand held devices in working hours is discouraged, other than in an emergency. Excessive use could be subject to disciplinary action.

20. Social Media

20.1 This The policy does not include guidance on the acceptable use of Social Media such as blogs, message boards, social networking (Facebook, Twitter, LinkedIn, My Space) and content sharing websites (Flickr, YouTube). This can be found separately under the Council's Appropriate use of

21. Reporting security incidents

21.1 All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

22. Training and awareness

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

23. Compliance and consequences

23.1 Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate