Wilton Town Council

Information Technology (IT) & Email Policy

Version 1.1 – March 2026

Contents

1. Document Control Information

Title: Information Technology & Email Policy

Date: March 2026

Version: 1.1

Authors: Wilton Town Council

Version Control & Approval:

Version No	Date	Description	Approval	
			Minute Reference	Date
1.0	8th December 2025	Policy Published incorporating existing Email policy in readiness for Assertion 10 – AGAR 2025/26	FC252	08/12/2025
1.1	March 2026	Reviewed and updated to accessible format. Appendix 1 added for Bring Your Own Device (BOYD)	FC 291	10th March 2026

Planned Review Date: March 2029

2. References

There are no sources in the current document.

3. Introduction

3.1 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.

3.2 This policy outlines the guidelines and responsibilities for the appropriate use of IT resources, by Council members, employees, volunteers and contractors i.e.: 'Users'.

3.3 All Users are responsible for the safety and security of the Council's IT resources 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.

4. Scope

4.1 This policy applies to all Users of the Council's IT resources, including: computers; networks; software; telephones; devices; data; email account, i.e. 'IT Systems'.

5. Purpose

5.1 The purpose of this policy is to inform all users of the proper use of the Council's IT systems.

6. Device & Storage Usage

6.1 Where appropriate, authorised devices and software will be provided by the Council for Wilton Town Council work.

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

6.3 See Appendix A for policy regarding using your own device

7. Data Management & Security

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

8. Network and internet usage

8.1 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.

9. Email communication

9.1 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.

9.2 Users must be cautious with attachments and links to avoid phishing and malware; verify the source before opening any attachments or clicking on links.

9.3 The following rules MUST be adhered to by all users. It is prohibited to:

- send or forward emails containing libellous, defamatory, offensive, racist or obscene remarks.
- 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 email.
- access another person's email unless: (a) they have given their consent (b) an appropriately authorised investigation is being undertaken or (c) access is required to maintain business continuity and minimise risk
- send email messages using another person's email address, unless in one of the scenarios above; 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.

9.4 The following disclaimer should 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, 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 IT and Email Policy . 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.

10. Password and account security

10.1 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.

11. Mobile devices and remote work

11.1 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.

12. System Monitoring

12.1 While 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.

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

12.3 If there is evidence a user is not adhering to the guidelines set out in this policy, the Council reserves the right to take appropriate disciplinary/legal action.

12.4 Users expressly waive any right of privacy when using the Council's telephone system. The Council can, but is not obliged to, monitor all incoming or outgoing telephone calls.

13. Retention and archiving

13.1 Emails should be retained, deleted or archived in accordance with legal and regulatory requirements. Users should regularly review and delete unnecessary emails, in order to maintain an organised inbox.

14. Personal use of the Council's IT systems

14.1 The Council's IT systems should only be used for Wilton Town Council related business and not for any other business or personal reason.

15. Abuse of Internet/email access

15.1 Any breach of this policy may warrant further investigation in certain circumstances, may necessitate the involvement of the Police.

15.2 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 further legal action will likely be taken.

16. Abuse of Internet/email access includes but is not limited to:

16.1 accessing or distributing material that is profane or obscene (pornography) that incites illegal acts, violence or discrimination towards other people (hate literature);

16.2 accessing web sites, blogs or chat rooms that are offensive, unsuitable or inappropriate to the workplace;

16.3 using language or behaviour likely to bring the Council into disrepute;

16.4 using the Council's official role/status for personal gain;

16.5 using the Council official role/status to support a specific political or issue-based campaign

16.6 online gambling;

16.7 using the equipment to contribute to fraud;

16.8 using or passing on privileged or confidential information;

16.9 making deliberate illegal attempts to disrupt the computer system or destroy data by spreading

16.10 computer viruses or by any other means;

16.11 harassing another person by engaging in unwanted conduct

16.12 which violates a person's dignity or creates an intimidating, hostile, degrading, humiliating or offensive environment for that person;

16.13 knowingly or recklessly posting false or defamatory information about a person or organisation;

16.14 posting, forwarding or replying to chain letters or sending annoying or unnecessary messages to a large number of people i.e. 'spamming';

16.15 Speaking on behalf of the Council, when not authorised to do so.

17. Legal risks

17.1 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.

17.2 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.

18. Users should be aware of the legal risks of email.

18.1 If you send or forward emails with any libellous, defamatory, offensive, racist or obscene remarks, both you and the Council can be held liable.

18.2 If you unlawfully forward confidential information, you and the Council can be held liable.

18.3 If you unlawfully forward or copy messages without permission, you and the Council can be held liable for copyright infringement.

18.4 If you knowingly send an attachment that contains a virus, you and the Council can be held liable.

18.5 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 emails may be required to answer Data Protection/FOI requests and difficulties can arise if a chain of emails refers to data

which should not be disclosed. Users should consider this when responding to or creating an email chain and, where appropriate, create a fresh message.

18.6 It is good practice to 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. 'Inbox', "Deleted Items" and 'Sent' folder contents should be kept to a minimum.

18.7 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

19. Access to Systems (General)

19.1 Should anyone 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.

19.2 Users are reminded that the Computer Misuse Act 1990 specifies the following as criminal offences:

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

19.3 Anyone found to be attempting to gain unauthorised access to any Council mailbox without authority will also be in breach of this policy. .

19.4 Virus shields, spam filters etc should be updated regularly.

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

20. Reporting security incidents

20.1 All suspected security breaches or incidents should be reported immediately to the Town Clerk.

21. Compliance and consequences

21.1 Breach of this IT and Email Policy may result in disciplinary proceedings (staff), the suspension of IT privileges and further consequences as deemed appropriate.

Appendix 1: Bring Your Own Device (BYOD) Policy

Introduction

This Appendix defines how Wilton Town Council permits councillors and staff to use personal devices (e.g., mobile phones, tablets, laptops) to access low-risk Council information. It aims to support effective working while safeguarding Council data. This policy applies in all working locations.

Councillors

a) Councillors may use personal devices for Council business once they have acknowledged this policy and signed the BYOD form. No further approval is required.
b) Policy breaches by councillors will be referred to the Monitoring Officer at Wiltshire Council.

Staff

c) Staff may use personal devices for Council business only with written authorisation from the Town Clerk or Assistant Town Clerk.
Policy breaches follow the staff disciplinary process.

Permitted Use (Low-Risk Data Only)

d) Personal devices may be used only for low-risk, non-sensitive Council information such as:
- Accessing Council email,
- Viewing non-sensitive Council documents,
- Accessing meeting papers,
- Preparing agenda items containing no sensitive information.

Prohibited Use

e) Personal devices must not be used to access or store:

- Resident personal data,
- financial records,
- Payroll information,
- Planning applications,
- Confidential or sensitive information.

Security Requirements

f) All personal devices used for Council business must:

- Have a screen-lock,
- Lock automatically,
- Be kept updated,
- Have antivirus where applicable,
- Be reported if lost or stolen immediately.

What These Security Rules Actually Mean

- Don't install software that bypasses the manufacturer's protections or lets you alter system files.
- "Keep your device updated"
- When your phone or laptop says an update is available, install it.
- "Use a lock screen"
- Your device must require a PIN, password, fingerprint or similar to unlock.
- "Automatic locking"
- If you put the device down, it should lock itself after a short time.
- "Report loss/theft"
- If the device goes missing, tell the Town Clerk straight away so we can protect Council information.

Authorisation and Documentation

g) Councillors sign BYOD form; staff require written approval. A register of authorised users will be maintained.

Loss, Theft or Incidents

h) Users must report incidents immediately. No remote wiping or routine monitoring will be performed.

Monitoring

i) Council does not routinely monitor devices; however, may request access only to Council-related information if legally required.

Compliance and Consequences

j) Councillor breaches: Referred to the Monitoring Officer at Wiltshire Council
k) Staff breaches: Follow the Disciplinary Policy.
l) BYOD access may be withdrawn at any time if security concerns arise or if the User breaches this or any other part of the Council's IT and Email Policy.

Data Protection and Privacy

m) Users are responsible for ensuring that Council information accessed via a personal device complies with the Data Protection Act, Freedom of Information Act and all other relevant legislation listed in Section 14 of the main policy.
n) Users must follow this Appendix and the main IT Policy.