Twyford Parish Council

Information Technology and Electronic Communications Policy

Adopted September 2025, minute 85/25.

1. **Introduction**

   Twyford Parish 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, employees, volunteers, and contractors.
   The policy aims to:
   Reduce the risk of IT-related security incidents.
   Promote effective and professional communications internally and externally.
   Ensure the consistent and lawful application of the Parish Council's principles in all electronic communications and digital platforms.

2. **Scope**

   This policy has been adapted from the Smaller Authorities Paper Practice Panel's IT policy template, as issued under the new external audit Annual Governance Statement assertation 10: Digital and Data Compliance.
   This policy applies to all individuals using Twyford Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. This policy also applies to when using personal devices for Council related business.

3. **Acceptable use of IT resources and email**

   Council 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 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 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**

   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. **Responsibilities**

All Council staff and Councillors must comply with this policy at all times.
The Clerk is responsible for ensuring the policy remains up to date, complies with relevant legislation, and is reviewed regularly.

Breaches of this policy:

a. By staff – may result in disciplinary action or legal proceedings.
b. By Councillors – may be referred to the Winchester City Council Monitoring Officer and could result in further action under the LGA Model Members' Code of Conduct.

All Council staff and Councillors are responsible for the safety and security of the Council's IT and email systems.

8. **Email communication**

• All official communications from the Parish Council must come from a Parish Council owned email address.
• Email accounts provided by the Parish Council are for official communication only.
• Council staff and Councillors are provided with a dedicated Council email account for official Council business.
• These accounts are Council property and may be accessed (with proper authorisation) to ensure continuity of operations or for data protection or freedom of information request purposes.
• Council staff and Councillors must not share their Council email address and login credentials with others outside the organisation.
• Non Parish Council email accounts must not be used for official Council business except in exceptional circumstances and only with prior approval from the Clerk.
• Check email trails for confidential or sensitive information before forwarding, and delete any unnecessary information before sending.

9. **Legal considerations and monitoring**

• The Council is a Data Controller and Data Processor under the Data Protection Act 2018 (DPA).
• 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.
• Any Council-related business conducted via private email accounts is still subject to the Freedom of Information Act 2000 (FOIA) and the DPA.
• Concealing or deleting information after an FOIA request is received is a criminal offence under Section 77 of the FOIA.
• Users must not send derogatory, defamatory, indecent, sexist, racist, or discriminatory content. What may seem humorous to one person could be offensive to another and result in disciplinary and / or legal action.
• Emails must not contain confidential or commercially sensitive information unless essential and agreed with all relevant parties

10. **Password and account security**

All Council staff and Councillors 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.
Emails are a common method for malicious attacks. Users must:
• Avoid clicking on suspicious links or opening unexpected attachments. Verify the source before opening any attachments.
• Report suspicious emails to the Clerk immediately.

• Councillors are advised to change passwords at least every six months.

11. Other electronic & instant messaging platforms

• The same standards and rules that apply to email also apply to other platforms such as WhatsApp, Facebook Messenger, and similar services when used for Council business.
• Mobile devices provided to staff should be secured with passcodes and/or biometric authentication.
• Communications on these platforms are also subject to FOIA and the Data Protection Act.

12. Email monitoring

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.

13. Document access & storage

• Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox. Delete messages permanently from the deleted email folder regularly.
• Staff and Councillors will be given appropriate access to the Council's secure online storage systems.
• Access is controlled via unique user IDs and passwords. Users are personally responsible for all actions taken under their login.

Users must not:

• Leave devices unlocked while logged in.
• Share passwords, unless authorised to do so by a Manager.
• Access or attempt to access unauthorised data.
• Connect unauthorised devices to Council systems.
• Store Council data on personal or unauthorised devices.
• Distribute Council data or software without proper authorisation.
• Store personal files (music, videos, games, photos, etc.) on Council IT equipment or cloud systems.

14. Reporting security incidents

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.

15. Training and awareness

Training and resources can be provided to educate users about IT security best practices, privacy concerns, and technology updates. All staff and Councillors will receive updates on training opportunities, email security and best practices.

16. Compliance and consequences

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

17. Policy review

This policy will be reviewed by September 2028, to ensure its relevance and effectiveness, updates may be made to address emerging technology trends and security measures.