# KENTISBEARE PARISH COUNCIL IT POLICY

**1. Introduction**

Kentisbeare Parish Council (henceforth known as KPC) 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.

**2. Scope**

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts. KPC will provide digital devices to staff and acknowledges that members will be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

**3. Training and awareness**

KPC will provide necessary training and resources to educate users about IT security best practices, privacy concerns, and technology updates. Employees and councillors will receive reminders on email security and best practices.

**4. Acceptable use of council provided IT resources and email**

When using IT resources for the council's purposes, you must adhere to ethical standards, and respect copyright and intellectual property rights.

**5. Device and software usage**

Where possible, authorised devices, software, and applications will be provided by KPC for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

You must not install unauthorised software without checking with the clerk, and you must not use equipment or email to access or forward inappropriate or offensive content.

KPC IT resources and email accounts are to be used for official council-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

**5. What you must do if you use your own personal devices**

KPC will provide staff with devices to use for council business. Where members are using their own device, they must ensure that they are:

- using strong passwords for all of your accounts (preferably using a password manager)
- downloading the latest operating system security updates
- using anti-virus software

**6. Network and internet usage**

Care must be exercised when joining Wi-Fi networks - public Wi-Fi networks such as those in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted internet connection, which is password protected when carrying out official business.

**7. Password and account security**

KPC 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.

**8. Email communication**

KPC will provide you with an official email account as soon as practically possible for organisation-related communication only. If you are currently using a personal email account, you will be provided with an official email account as soon as possible after which the council will no longer accept personal emails.

You must make sure that emails are professional and respectful in tone. You must always check you are sending any confidential or sensitive information to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

**9. Email access**

KPC reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails so that they can respond to FOI or subject-access requests. If you are using a personal email account for council business, this is still subject to data protections laws and FOI requests.

**10. Data management, data retention and security**

All sensitive and confidential data should be stored and transmitted securely. You must regularly backup any important data to prevent data loss and follow your organisation's data retention policies.

You should retain and archive emails in compliance with your data retention policies. Regularly review and delete unnecessary emails to maintain an organised inbox.

If you resign from your position as a Parish Councillor any emails on your personal email account relating to KPC should be deleted as soon as practically possible – KPC will ask for confirmation that this has been completed in writing.

**11. Reporting security incidents**

All suspected security breaches, including email breaches or incidents should be reported immediately to the Clerk.

**12. Compliance and consequences**

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

**13. Policy review**

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

**14. Contacts**

For IT-related enquiries or assistance, users can contact The Clerk.

All staff and councillors are responsible for the safety and security of IT and email systems.

**Date of adoption: 10-03-2026**

**Date for next review:  March 2027**