

# Kingston Parish Council - IT Policy

## 1. Introduction

Kingston 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 and voluntary post holders.

## 2. Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors use technology in the course of their duties. The policy helps to:

- Set expectations for appropriate use of parish council systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data
- Clarifies what constitutes acceptable and unacceptable use;

This Policy applies to all individuals who use Kingston Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

## 3. Acceptable use of IT resources and monitoring

IT resources and email accounts provided by Kingston Parish Council are intended solely for official Council business and tasks. All users must adhere to ethical standards, respect copyright, and intellectual property rights, and avoid accessing inappropriate or offensive content.

The council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors and employees are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

## 4. Device and software usage

The Council recognises that some councillors and employees may need to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's Dropbox site or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

Councillors and employees that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. If required, authorised devices, software, and applications may be provided by Kingston Parish Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is prohibited due to security concerns.

## **5. Data management and security**

All confidential and sensitive information from the Kingston Parish Council should be stored and sent only through approved, secure methods. To avoid losing information, it is important to back up data regularly and use secure methods to destroy it when needed.

All councillors or employees using their own equipment should:-

- use a strong password to protect their device(s) from being accessed.
- configure their device(s) to automatically prompt for a password after a period of inactivity.
- Inform the parish clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources.

## **6. Network and internet usage**

The Kingston Parish Council's network and internet must be used efficiently and exclusively for official purposes. It is not allowed to download or share copyrighted material without proper permission.

## **7. Email communication**

Email accounts provided by Kingston Parish Council are for official communication only. Emails should be professional and respectful in tone. Sensitive or confidential information should only be emailed if it is encrypted.

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

## **8. Password and account security**

Kingston Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

### **Access to Passwords**

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- Passwords must not be stored in plain text or written down in insecure locations
- Users are responsible for creating and maintaining secure passwords for their accounts.

## **9. Email monitoring**

Kingston Parish Council reserves the right to monitor email communications to ensure compliance with this Policy and relevant laws. All monitoring will follow the requirements of the Data Protection Act and GDPR.

## **10. Retention and archiving**

Emails should be deleted or archived in accordance with Legal and Regulatory requirements.

## **11. Reporting security incidents**

Any potential security breach or incident should be reported immediately to the designated IT contact to ensure timely investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

## **12. Training and awareness**

Kingston Parish Council will facilitate education of users if required. The Parish Council will endeavour to ensure that users are aware of IT security best practices, privacy concerns, and technology updates.

## **13. Compliance and consequences**

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

## **14. Use of the Internet**

Copyright - Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited.

Trademarks, links and data protection - the council does not permit the registration of any new domain names or trademarks relating to the parish council's name.

Accuracy of Information - One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

Use of Social Media - Care should be taken when using social media at any time. The parish council recognises the importance of social media. However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors or employee's posts therefore, even if the council is not named, care should be taken with any views expressed. Comments posted by councillors or employees on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.

The council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or normally through the grievance procedure.

## **15. Policy Review**

The policy will undergo a periodic review to confirm it remains effective and applicable. Adjustments may be implemented to address new technological trends and enhance security measures.

Date Adopted:- 10 March 2026

Planned Review:- 10 March 2028