KING'S SUTTON PARISH COUNCIL
IT POLICY

1. Introduction

King's Sutton 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, Clerk, volunteers, and contractors. King's Sutton Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

2. Scope

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

3. Acceptable use of IT resources and email

King's Sutton Parish Council's 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.

4. Data management and security

All sensitive and confidential King's Sutton Parish 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.

5. Network and internet usage

King's Sutton Parish Council's network and internet connections should be used responsibly and efficiently for official purposes Parish Council purposes. The CCTV system also uses the Parish Council's network. Downloading and sharing copyrighted material without proper authorisation is prohibited.

6. Email communication

The Parish Clerk and all Parish Councillors have an email designated for use for Council use only. The Parish Clerk controls the access to these accounts, adding new ones and deleting those made redundant (by resignation etc). Wardens may choose to have a designated generic email for their role which allows easy transfer if a new Warden is appointed. All members of the King's Sutton Times editorial team have also been assigned a Parish Council email address.

Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless 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.

When communicating with third parties, users should ensure that they are doing so on behalf of the council and represent its views. If the e-mail represents personal views, the e-mail should be sent from a personal email account. This ensures clarity and transparency at all times.

7. **Password and account security**

King's Sutton Parish 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.

8. **Mobile devices and remote work**

Any mobile devices used for King's Sutton Parish Council business 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.

9**. Email monitoring**

King's Sutton Parish 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.

10**. Retention and archiving**

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

11. **Reporting security incidents**

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

12. **Training and awareness**

KING'S SUTTON PARISH COUNCIL
IT POLICY

King's Sutton Parish Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates if requests to do so.

13. **Compliance and consequences**

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

14. **Policy review**

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

Reviewed: 22nd July 2025 **Minute No. FGP: 22.25/26 B**
Approved: 4th September 2025 **Minute No 95.25/26 B.1**