Kempsey Parish Council IT Policy

1. Introduction

Kempsey Parish Council herewithin "the Council" recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, its operations and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by Council members and Council employees, both permanent staff and staff on service agreement terms, collectively the "Users".

2. Scope

This policy applies to all individuals who use IT resources belonging to the Council, including computers, networks, software, devices, data and email accounts. The Council provides digital devices for Council permanent employees but acknowledges that some other service agreement staff and Council members may be using their own personal devices. All employees and staff must adhere to this policy to maintain digital security and all members of the Council should do so when engaged on Council business.

3. Training and awareness

The Council will, where appropriate, source regular training and resources to educate staff and members about IT security best practices, privacy concerns, and technology updates. This may include training on email security and best practices including but not limited to:

- the Parish Council Domain Helper Service's virtual cybersecurity workshops for councils

- The National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

4. Acceptable use of Council provided IT resources and email

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

Where appropriate, authorised devices, software and applications will be provided by the Council for work-related tasks.

Users must not install unauthorised software on Council owned devices without checking with the Clerk to the Council. Users must not use Council owned equipment or email to access or forward inappropriate or offensive content which might bring the Council into legal or reputational difficulty.

5. What you must consider if you use your own personal devices

The Council will endeavour to provide permanent employees with devices to use for Council business. Users employing their own devices should endeavour to:

- use strong passwords for all your accounts by following recognised guidelines (see below) and store passwords securely, preferably by using a recognised password manager application.
- download the latest operating system security updates
- use anti-virus software

6. Network and internet usage

Users are recommended to be careful about which Wi-Fi networks they join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Users should make sure that they are using a trusted internet connection, which is password protected, when carrying out official business.

7. Password and account security

Users are responsible for maintaining the security of their accounts and passwords. Users should consult the National Cyber Security Centre's advice for choosing a strong password. For business continuity, login details and passwords used by permanent employees must be stored securely so they can be accessed by trusted individuals in an emergency.

8. Email communication

The Council will provide permanent employees and members with an official email account for organisation-related communication only. The Council reserves the

right to block emails to the Council from personal accounts where an official email account has been provided. Users should make sure that emails are professional and respectful in tone and should always check that any confidential or sensitive information is being sent 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

The Council 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. The Clerk may need to access emails to respond to Freedom of Information (FOI) or subject-access requests. Correspondence from a personal email account being used for Council business 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. Users should regularly backup any important data to prevent data loss and follow the Council's data retention policy.

Users should retain and archive emails in compliance with the Council's data retention policy and regularly review and delete unnecessary emails to maintain an organised inbox and folders.

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 Policy may result in the suspension of IT privileges accorded by the Council.

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 at any time.

14. Contacts

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

All staff and members are responsible for the safety and security of both their own and the Council's IT and email systems.

Date of adoption: 31st March 2026 at the Extra Ordinary Meeting of the Council.

Date for next review: