Kersey Parish Council IT and Email Policy

1. Introduction

Kersey Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its work and communications. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources, including computers, software, devices, data, and email accounts, by Councillors, employees and volunteers. The Parish Council is a data controller and processor.

2. Acceptable use of IT resources and email

Kersey Parish 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.

3. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Kersey Parish Council for the Clerk for work related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns. Councillors will use their own devices. All users will comply with all relevant policies, procedures and UK legislation with respect to the use of IT software.

4. Use of own devices 'bring your own device' (BYOD)

Kersey Parish Council supports the use of personal devices, such as mobile phones, tablets and laptops, to enable efficient access to Council Information. Using a personal device in this manner is known as 'Bring your own Device' (BYOD). The Parish Council does not take responsibility for supporting devices it does not provide. Councillors must take responsibility for their own devices and how they use them. They must:

- Familiarise themselves with their device and its security features so that they can ensure the safety of Council information (as well as their own information)
- Ensure software is regularly updated and safety features are activated
- Ensure that the device is only used in line with the values in the Code of Conduct and the Nolan Principles

Councillors using BYOD must take all reasonable steps to:

- Maintain the security of information to prevent theft and loss of data
- Keep information confidential where appropriate
- Be aware of any data protection issues and ensure personal data is handled appropriately
- Take responsibility for any software they download onto their device
- Set up passwords, PIN's or biometric equivalents
- Where it is essential that information belonging to the Council is held on a personal device, it should be deleted as soon as possible once it is no longer required. This includes information contained within emails
- Report the loss of any device containing Council data (including email) to the Clerk
- Report any security breach immediately to the Clerk
- Ensure that no Council information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party. To do this, remove any information manually and then reset to factory settings
- Ensure they immediately delete all Council data from their personal devices once they have left the Council.

Kersey Parish Council IT and Email Policy

The Council, in line with guidance from the Information Commissioner's Office on BYOD, recognises that there are inherent risks in using personal devices to hold personal data. Therefore, Councillors must follow the guidance in this document when considering using BYOD to process personal data. A breach of the Data Protection Act 2018 or the UK GDPR can lead to the Council being fined. Any Councillor found to have deliberately breached the Act or the Regulations may be subject to disciplinary measures or even a criminal prosecution.

5. Data management, security, privacy and data protection

The Clerk and Councillors will all adhere to the Data Protection and Information Security Policy and the Data Retention Policy. All sensitive and confidential Kersey Parish Council data will 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. Email communication

Email accounts provided by Kersey Parish Council to the Clerk and all Councillors are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be aware of cyber security and be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links. You should carefully check the email address of the sender to verify the email address and sender name are the same.

6. Password and account security

Kersey 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.

7. Email monitoring

Kersey 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 UK GDPR.

8. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements and the Parish Council Data Retention Policy. Regularly review and delete unnecessary emails to maintain an organised inbox.

9. Parish Council website www.kerseyparish.gov.uk

The Kersey website meets the WCAG 2.2 AA standards and the Parish Council publishes all the required documents, such as Councillor information, minutes and financial documents on the Parish Council pages of the Kersey website. The Clerk is responsible for ensuring the Parish Council pages are regularly updated. The website is checked annually for accessibility and broken links and this is reported to the Council.

10. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk or Chair for investigation and resolution. Report any email-related security incidents or breaches immediately to the Clerk who will contact Suffolk.Cloud, our mailbox host for support.

11. Training and awareness

Kersey Parish Council will provide training and resources to educate Councillors and staff about data protection principles and practices, IT and email security best practices and privacy concerns. As part of their initial training, all new Councillors will attend training delivered by SALC, which covers data protection. The Council will provide regular refresher training on IT, Email and data security principles and practices.

12. 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.

All staff and councillors are responsible for the safety and security of Kersey Parish Council's IT and email systems. By adhering to this IT and Email Policy, Kersey Parish Council aims to create a secure and efficient IT environment that supports the work of the Council.