



Internet and Email Use Policy

Introduction

1. This policy has been developed in response to the acknowledged need for guidelines describing the acceptable use of the council e-mail and related services and facilities. It describes the standards that are expected to be observed when using council facilities for e-mail. It establishes a framework within which staff are expected to apply self-regulation to their use of the council e-mail facilities. Usage of e-mail and Internet facilities in breach of the policy may lead to appropriate disciplinary action being taken against members of staff which could lead to dismissal.

Scope of the policy

2. This policy applies to the use, for the purpose of sending or receiving messages and attachments, of any IT facilities, including hardware, software networks, provided by Kingsbury Parish Council (KPC). The policy is applicable to all employees and other authorised users.

Appropriate and proper use

3. KPC supports the appropriate and proper use of the Internet, e-mail, and related services and facilities that the council provides for its employees and other authorised users. Associated with the provision of these services and facilities the council endeavors to provide an appropriate regulatory framework including specific standards and guidance for the appropriate use of these services and facilities.
4. This policy constitutes a component part of this regulatory framework.

Use of e-mail

5. The council provides appropriate staff with an e-mail account as a vital tool to fulfill the council's objectives and to enable them to communicate effectively with other personnel, both within the council and externally. Staff must not abuse the council e-mail account in any way. A non-exclusive list of abusive conduct is deemed to include:
 - Sending unsolicited e-mails to other companies or individuals (spamming)
 - Using council e-mail for purposes unrelated to the job
 - Personal use of any electronic Council devices is strictly forbidden
 - Circulating unsuitable or illegal material
 - E-mailing personal information entrusted to the council without obtaining permission from councillors
 - Defaming any individual or the council regardless of whether the subject is, or could be, aware of the content
 - Use of the council e-mail address in any on-line forum, discussion group or message board without obtaining permission from councillors
 - Spoofing other people's e-mail accounts (pretending to send, or attempting to receive e-mail on behalf of others without their permission)

- Setting up the equipment so that it could act as an “Open Mail Relay” for third party spammers
- Using the council’s IT facilities for swapping of games, music, videos, or DVDs
- Opening or reading e-mail, which has an unacceptable risk as set out below in “Preventing the spread of malicious software”
- Operating the e-mail without operating a suitable e-mail-aware anti-virus system as provided by council

Personal use

6. Staff may not use the council-provided internet facilities for personal use.

Email Retention Policy (ERP)

7. The objective of the Email Retention Policy (ERP) is to help employees and members determine what information sent or received by email, should be retained and for how long. Emails will be automatically deleted in line with the council’s retention schedule. However there are some emails that should be retained and stored in the relevant case management system or the relevant business folder for your service these emails include:
 - decisions, directives, policies, or disciplinary actions communicated to employees by management via email.
 - emails to residents and service users for the purpose of conducting business.
 - emails communicating financial information to third parties, suppliers, partners, or others who may make decisions based on this information.
 - communications that comply with government or industry regulations.
 - communications relating to audit evidence/artifacts.
8. The information covered in this policy includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies. All employees and members should familiarise themselves with this policy and acknowledge the reasons why the policy is important, such as:
 - data protection - emails can contain sensitive business information, and therefore this policy ensures that the council’s data is protected.
 - cyber threats - protecting the data held by the council against various cyber threats.
 - regulations - to ensure the council complies with current laws and regulations.
 - legal and contractual concerns - retained emails can be a factor in any litigation or contract the council may be involved in. Having this policy in place - as well as the ability to retrieve emails - will help to protect against future litigation or contractual issues or fines.
9. This policy is designed to provide direction, support, and help council employees and members carry out their day-to-day business for the council in a secure manner. By complying with this policy, the risks facing the council are minimised. This document supports the council’s cyber security policy and the employee code of conduct.
10. Emails held by the council are to be legally discoverable following a request under the General Data Protection Regulation (GDPR), the Freedom of Information Act (FOI), Subject Access Request and may be required as evidence in legal proceedings. The Data Protection Act 2018 and Freedom of Information Act 2000 have highlighted that it is important to adopt a more formal policy for email retention, that ensures the council is

compliant with legal and regulatory requirements, lowers our infrastructure costs, and improves our operational efficiency and effectiveness.

Email Retention

11. You should not use Outlook or any other email client managing KPC messages for storing business critical information. Such information should be stored in the relevant business folders on your shared drive:
- Emails content must be assessed and stored with great care and users must consider the impact any misuse may have on KPC.
 - Emails that have to be kept should be kept electronically as a separate file or added to an appropriate file.
 - Emails are the property of KPC and must not be deleted without consent from the DPO.

Devices used to store emails must meet the Digital Services requirements associated with the device type. These devices must not be shared in a manner that allows unauthorised access to the council's emails.

12. Mailbox owners are responsible for managing their own mailbox and the data held within it. Emails shall be retained for the following periods:
- Current employees' emails will be automatically archived after 2 years and then deleted after 7 years from date received unless required for business-critical needs or an ongoing investigation.
 - Former employees no longer working for the council will have all email communication deleted after 2 years.
 - Employees on long term sick leave or maternity leave, must ensure that out of office is applied, and incoming emails are redirected to a shared mailbox or another appropriate mailbox. Please speak to the DPO or Chair to help you set redirects up.
 - Current members emails will be automatically archived after 2 years and then deleted after 7 years.
 - Members that have left the council will have their emails deleted after 2 years from the last date of their service.

Disciplinary action

13. If staff ignore the rules and guidance set out above and/or misuse and/or abuse the system, its facilities or any property belonging to KPC, they will be liable to disciplinary action. Depending on the circumstances, the misuse and/or abuse could lead to summary dismissal. KPC will take any breach of these rules very seriously. At the same time, the conduct and/or action(s) may be unlawful or illegal and the staff member may be personally liable.

Pornography

14. The uploading, downloading, storing, and/or printing out of computer data of indecent images by any employee or unauthorised person is conduct which will normally lead to summary dismissal of the employee or authorised person.

Preventing the spread of malicious software (viruses)

15. Staff must take all reasonable steps to prevent the receipt and transmission by e-mail of malicious software e.g. computer viruses and worms. In particular, staff must not:

- Transmit by e-mail any file attachments which are known to be infected with malicious software
- Open e-mail file attachments received from unsolicited or untrusted sources
- Use removable media that has not been scanned by the council's antivirus software immediately prior to its use
- Download or install software without express approval by the councillors

Removable Media Policy

15. The following shall apply to the use of removable media:

- KPC will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.
- Removable media devices include, but not limited to memory stick/USB keys, writeable CD/DVD, laptops, smartphones, cameras, memory cards. It is KPC policy to limit the use of removable media devices.
- The use of removable media devices will only be approved if it is required for Council business.
- All data stored on removable media devices must be accessible by the Data Protection Officer (DPO) if needed and encrypted when required.
- Damaged or faulty removable media devices must not be used.
- If a CD or memory stick is received from a third party it must be virus checked using antivirus software updated to current version prior to insertion into Council equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft, or damage.
- Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage.
- When not in use a Council owned storage device must be kept in a locked drawer / cabinet where there is no public access (e.g. at the Clerk's / Councillors' home).
- Information Security Incident Management: KPC will ensure that it reacts promptly and appropriately to any actual or suspected breach.

16. **Reviews**

This policy will be reviewed every 3 years, from the date of adoption by KPC.

Adopted at the Parish Council Meeting on 22nd April (Minute 660)

Revision Control

Revision	Details of Change
April 2026	New
June 2026	Policy reviewed and adopted. Min. 697