

# IT POLICY

## 1. Introduction

All authorities must have an IT policy. The 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, volunteers, and contractors.

## 2. Scope

This policy applies to all individuals who use the Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts, whether owned by the authority or if personal devices are used.

## 3. Acceptable use of IT resources and email

Only our Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. We require the use of an official, generic council email (eg [councillor@parishcouncilname.gov.uk](mailto:councillor@parishcouncilname.gov.uk)) for all correspondence on the council's own domain. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

## 4. Device and software usage

Where possible, authorised devices, software, and applications will be provided by the parish council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

## 5. Data management and security

All Parish Council sensitive and confidential 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. The role as Data Controller under GDPR will be reinforced, referring to the Data Protection Policy and providing clear steps for managing FOI (Freedom of Information) and SARs (Subject Access Requests).

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

The Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

## **7. Email communication**

Email accounts provided by the Parish Council 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 cautious with attachments and links to avoid phishing and malware. Councillors and Staff must verify the source before opening any attachments or clicking on links.

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

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.

## **9. Mobile devices and remote Work**

Mobile devices provided by the parish council 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.

## **10. Email monitoring**

The 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.

## **11. 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.

## **12. Reporting security incidents**

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

## **13 Training and awareness**

The parish council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

## **14. Compliance and consequences**

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

## **15. 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.

## **16. Contacts**

For IT-related enquiries or assistance, users can contact Katrina Baker MBE CiLCA, Clerk to Council.

All staff and councillors are responsible for the safety and security of their Parish Council's IT and email systems. By adhering to this IT and Email Policy, our parish council aims to create a secure and efficient IT environment that supports its mission and goals.