

# **Old Catton Parish Council**

## **IT and Email Policy**

### **1. Introduction**

Old Catton 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 Old Catton Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. It covers Councillors, employees, contractors, and authorised third parties.

### **3. Acceptable use of IT resources and email**

Old Catton 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.

### **4. Device and software usage**

Where possible, authorised devices, software, and applications will be provided by Old Catton Parish Council for work-related tasks. Personal devices may be used for Council business only where explicitly approved, and must be secured with passwords, up-to-date antivirus, and encryption where available. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited.

### **5. Data management, backups and security**

All sensitive and confidential Council data should be stored and transmitted securely using approved methods. Regular encrypted backups must be performed to prevent data loss, and secure data destruction methods used when necessary. The Clerk is responsible for ensuring appropriate backup and disaster recovery protocols are in place.

### **6. Network, remote access and cloud services**

Old Catton Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Remote access must be via secure methods such as VPNs. Only GDPR-compliant cloud services and approved third-party providers may be used.

## **7. Email communication**

Email accounts provided by Old Catton Parish Council are for official communication only. Personal email accounts must not be used for Council business. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent unless encrypted. Be cautious with attachments and links to avoid phishing and malware.

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

Users are responsible for maintaining the security of their accounts and passwords. Passwords must be strong (using upper and lower case, numbers, and special characters) and not shared with others. Multi-factor authentication should be used where available and appropriate.

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

Mobile devices used for Council business must be secured with passcodes or biometric authentication. When working remotely, users must follow the same security practices as if working in the office.

## **10. Monitoring and audits**

Old Catton Parish Council reserves the right to monitor IT systems and 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. Periodic audits will be carried out to review security and compliance.

## **11. Retention and archiving**

Emails and documents should be retained and archived in accordance with legal and regulatory requirements. Unnecessary files and emails should be deleted regularly to maintain an organised system.

## **12. Reporting security incidents**

All suspected security breaches or incidents must be reported immediately to the Clerk or designated IT contact. This includes any data breaches, suspected phishing attacks, or loss/theft of devices.

## **13. Training and awareness**

All Councillors, staff and volunteers will receive regular training on IT and data security, GDPR, and safe handling of information. Refresher training will be provided every three years, or sooner if required.

## **14. Compliance and consequences**

Failure to comply with this policy may result in withdrawal of IT access, disciplinary action for staff or Councillors, termination of contracts for third parties, or referral to regulatory authorities in serious cases.

### **15. Responsibilities**

The Clerk has overall responsibility for IT systems, compliance, and managing supplier contracts. IT providers are responsible for maintaining secure systems. All users are responsible for following this policy and safeguarding Council information.

### **16. Policy review**

This policy will be reviewed annually to ensure its relevance and effectiveness, or sooner if required by legislation, guidance, or security incidents.

### **17. Contacts**

For IT-related enquiries or assistance, users should contact the Clerk. All staff and Councillors are responsible for the safety and security of Old Catton Parish Council's IT and email systems.

**This policy was approved and adopted by the Parish Council on 13<sup>th</sup> January 2026.**