ELMSWELL PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

Introduction
Elmswell 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; it applies to all councillors, employees, volunteers, and contractors.

Purpose and Scope
The policy covers all forms of information and communication technologies including council-owned devices, email systems, websites, cloud storage, third-party platforms, and personal devices used for council business.

It ensures we meet the requirements of the 2025 Practitioners' Guide – Assertion 10: Digital and Data Compliance, and follow laws such as:

- Data Protection Act 2018 and UK GDPR
- Freedom of Information Act 2000
- Transparency Code for Smaller Authorities
- Website Accessibility Regulations 2018

Roles and Responsibilities
(a) The Clerk is responsible for managing and enforcing this policy, ensuring IT resources are used appropriately and securely.
(b) Councillors and staff are responsible for complying with the policy and reporting any breaches or incidents immediately.
(c) External IT support providers and contractor must adhere to the standards set out in the policy when handing council information.

Acceptable Use
Elmswell 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.

Data Management and Security
All 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.

Staff and councillors must not disclose confidential council information to any unauthorised person, either during or after their term of office or employment.

Device and Software Usage
Where possible, authorised devices, software, and applications will be provided by Sileby parish council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Network and Internet Usage
Elmswell 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.

Email Communication
Email accounts provided by Elmswell 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. Verify the source before opening any attachments or clicking on links.

Password and Account Security
Elmswell 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.

Remote Working and Devices
Staff and councillors who work remotely must ensure they use a secure internet connection and do not leave devices unattended in public or shared spaces. Devices must be locked when not in use and must not be shared with unauthorised personnel. Council documents must not be downloaded onto personal devices unless approved by the Clerk.

Incident and Reporting and Cyber Security
Any data breach, loss of equipment or suspected cyber incident must be reported immediately to the Clerk, who will investigate and determine whether the breach needs to be reported to the Information Commissioner's Office (ICO). The Council will follow procedures outlined in its Data Protection Policy. All councillors and staff must remain vigilant against phishing attempts and other online threats.

Training and Awareness
Elmswell 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. Staff and councillors are encouraged to familiarise themselves with National Cyber Security Centre (NCSC) guidance on staying safe online.

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

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.

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

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

ELMSWELL PARISH COUNCIL
Blackbourne, Blackbourne Road, Elmswell IP30 9UH
clerk@elmswellpc.co.uk
01359 244134
elmswell-pc.gov.uk