



Elton Parish Council

DRAFT Information Technology Policy

This policy is supplemental to, and does not in any way override, the Parish Council Standing Orders and/or Financial Regulations.

This policy was adopted by the full parish council at its meeting on 9 February 2026 (minute 25.131.1)

This policy will be reviewed every three years.

1. Introduction

1.1 Elton Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

1.2 A separate Communications Policy and Press and Media Policy has been adopted by the parish council.

2. Scope

2.1 This policy applies to all individuals who use Elton Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Legislation

3.1 Many pieces of legislation apply including:

3.1.1 Freedom of Information Act 2000 – right to request information from a public body.

3.1.2 Data Protection Act 2018 and Regulations – right for individuals to access information held about them by a public body.

3.1.3 The Equality Act 2010, which includes the Public Sector Equality Duty – providing protection for individuals, including those with protected characteristics and ensuring services are accessible to all.

3.1.4 The Practitioners Guide 2025 requires councils to comply with the requirements of Assertion 10, which covers council-owned domain names; website accessibility; availability of public domain information; security of personal data and the adoption of an IT Policy.

3.1.5 Web Content Accessibility Guidelines 2.2 AA and the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018– set out the requirements to have a website that is accessible to all or to notify users through an Accessibility Statement of those areas which are not accessible, why they are not accessible and when they will become accessible or how to request the information in an accessible format.

4. Dissemination and Training

4.1 The council will issue this policy to all employees as part of their induction, to councillors and the policy will be available on the Parish Council website.

5. Monitoring and review

5.1 A review of the policy shall be undertaken every three years; necessary amendments will be advised by the Parish Clerk and reported to the council for approval.

5.2 Changes in the law will be monitored and, if necessary, amendments/reviews made to the policy.

6. General Statement of Policy

6.1 Elton Parish Council aims to be open and transparent at all times.

6.2 Information Technology is part of normal working life and often used without a second thought. However, with increased security threats the Parish Council must adopt a mindful approach to Information Technology usage and establish a robust protocol for use and for ensuring the security of its data.

7. Specifics

Elton Parish Council will apply the guidance below in order to fulfil the aims of the policy:

7.1 Acceptable use of IT resources and email

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.

7.2 Device and software usage

The parish council provides a laptop computer, mobile phone, appropriate software and applications to the Clerk for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited.

Personal devices which are used for council business must adopt the security measures detailed in this policy.

7.3 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.

7.4 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.

7.5 Data management and security

All sensitive and confidential parish council 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.

7.6 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. Caution should be exercised with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

7.7 Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regular review and deletion of unnecessary emails should take place to maintain an organised inbox.

7.8 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.

7.9 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.

7.10 Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk/Chair of the parish council for investigation and resolution. Report any email-related security incidents or breaches to the Clerk or the Chair immediately.

7.11 Compliance and consequences

Breach of this Policy may result in the suspension of IT privileges and possible further consequences or measures as outlined in the Disciplinary Policy/Complaints Policy.

Author	Review Date	Date of Adoption	Minute reference
Lara Jacob		9 Feb 2026	25.131.1
	Feb 2029		