Easton Parish Council Information Technology (IT) Policy

1. Purpose

This policy defines how Easton Parish Council manages its use of information technology, in line with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide. It ensures the council's digital operations are transparent, secure, and compliant with data protection laws.

2. Scope

This policy applies to all **councillors**, **volunteers**, and **contractors** who access or manage the council's IT resources, including but not limited to:

- Desktop and laptop computers, tablets, and smartphones
- Email and cloud-based systems
- Council website, social media, and digital publication tools
- Video conferencing and messaging platforms
- Personal devices used under Bring Your Own Device (BYOD) provisions

3. Governance and Oversight

IT Oversight is the responsibility of Steve Thomason who is the designated Data Protection Officer (DPO) and IT Systems Administrator.
There is no specific IT Sub-Committee: overseeing implementation, security, and compliance. This is managed by the parish council as a whole as agenda item/s twice per year at a minimum, via the usual monthly Parish Council Meetings.

4. Data Protection & Security

All processing of personal data shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
There is a separate parish council Privacy Policy document held on the parish council website which outlines the governance of data collection, processing, and subject rights.

Access and Storage: Data is stored securely, with access granted only to authorised personnel currently defined as all members of the parish council and the parish council clerk.

Retention: Personal data will be retained in accordance with the council's Data Retention Schedule outlined in the Data Retention Policy document. It is also securely deleted when no longer needed as outlined in the schedule.

Key Security Controls: For parish council owned hardware password protection and multi-factor authentication is in place where applicable.
For parish council owned hardware regular software updates and anti-malware software are in place.
For parish council owned hardware backups of essential data is managed to ensure integrity and security of data.

5. Use of Personal Devices (BYOD)

Authorised Use Only: as part of this policy councillors and staff may use personal devices including mobile phones, tablets and personal computers for council business without being individually documented within this policy.

Security Requirements: Devices are recommended to be protected by strong passwords, encryption (where possible), and up-to-date antivirus software. Access to council data on personal devices must be controlled and subject to regular review.

Data Separation: Council data must be kept separate from personal data using dedicated apps or storage areas.

6. Use of Personal Email Addresses

Prohibited Practice: The use of personal email accounts for formal council business is strictly prohibited. All council correspondence must be conducted through official council-provided email addresses.
Emails from council-owned domains must not be forwarded to personal email addresses.
Monitoring and Compliance: Any breaches will be investigated, and appropriate measures taken in line with the council's disciplinary or governance procedures.
Email Retention: All council emails will be stored in compliance with the GDPR, Freedom of Information requirements, and the council's data retention policy.

7. IT Infrastructure & Support

Asset Register: Maintained for all council-owned hardware and software.
Currently the asset register comprises the following

1. HP Laptop managed by the Easton Parish Clerk. Purchased in March 2016.
2. External hard drive, used for managing Parish backups for the Dell Laptop, managed by the Easton Parish Clerk.

Maintenance: All devices must be regularly updated and checked for compliance with this policy.

Training: Users will be given training on IT systems, cybersecurity, data handling, and transparency responsibilities.

8. Monitoring and Review

Annual Review: This policy will be reviewed annually, or sooner if legislation or any requirements change.
Audits: Periodic internal audits will check for compliance with security and transparency requirements.

9. Data Breach Process and Protocols

The Parish Council is committed to responding promptly and effectively to any data breaches to minimise risk and comply with UK GDPR requirements.

10. Definition of a Data Breach

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:
- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising council systems

10.1 Reporting a Breach

Immediate Notification: Any councillor or clerk who becomes aware of a data breach must report it immediately to the Clerk or Data Protection Officer.
Initial Response: The Clerk or Data Protection Officer will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling two factor authentication).

10.2 Investigation

A full investigation will be conducted by the Clerk or Data Protection Officer within 72 hours of the breach being discovered. The breach will be logged, including:
Date and time of breach
Type and volume of data affected
Cause and extent of the breach
Potential impact of the breach
Actions taken to address the breach

10.3 Notification Requirements

If the breach is likely to result in a risk to the rights and freedoms of individuals, the council must notify the Information Commissioner's Office (ICO) within 72 hours
If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay, outlining:

- The nature of the breach
- Likely consequences
- Measures taken to mitigate the risk
- Contact information for further support

10.4 Remediation and Review

The Clerk and Parish Council will ensure lessons are learned and policies, procedures, or training are updated as necessary.
Technical fixes or security upgrades will be prioritised to prevent recurrence.
Breach logs will be reviewed periodically to identify systemic issues.

11. Approval and Adoption

This policy was adopted by Easton Parish Council on 8th January 2026 and will be reviewed annually or following a significant incident or legislative change.
Signed:
Steve Thomason acting Chair of the Parish Council Date: 08/01/2026
Anthea Beer Clerk to the Parish Council Date: 08/01/2026

12. Review Timescales

This document was last reviewed in January 2026 and is due for review again January 2027.