1. Purpose

This policy defines how Chevington 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**, **employees**, **volunteers**, and **contractors** who use 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: The Clerk is the designated Data Protection Lead (DPL) and IT Systems Administrator.

IT Support provided by Community Action Suffolk : Oversees implementation, security, and compliance

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.

Privacy Policy: All data collection, processing, and subject rights are governed by the council's Privacy Policy, available on the council website.

Access and Storage: Data is stored securely, with access granted only to authorised personnel based on necessity.

Retention: Personal data will be retained in accordance with the council's Data Retention Schedule and securely deleted when no longer needed. See Data Retention Policy.

Security Controls:

- Strong password protection with multi-factor authentication where possible is required for all systems.
- Passwords used on council systems are to be unique to this environment and no user in scope must use logins associated with non-council systems.

- Regular security updates and anti-malware software are required on all council-owned and personal devices.
- Backups of essential data must be stored in a secure location.

4.1 Access Control

The Clerk will revoke all access credentials immediately upon a councillor leaving office. This includes changing the password and freezing the email account(s), access to council systems (accounting software, cloud storage, website admin).

5. Use of Personal Devices (BYOD)

Authorised Use Only: Councillors and staff may use personal devices for council business and subject to compliance with this policy. This includes the use of council-owned domain-based email and access to the council's accounting system and website administration. 2-factor or multi-factor authentication is required where supported.

Security Requirements: Devices must 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.

N.B Any loss, theft, or compromise of a device used for council business must be reported to the Clerk immediately.

6. Use of Personal Email Addresses

Prohibited Practice: The use of personal email accounts for council business is strictly prohibited. All council correspondence must be conducted through official council-provided email addresses. Council emails must not be shared or forwarded outside of approved data areas, such as forwarding to a non-council owned domain or personal email.

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, DPA and Freedom of Information requirements.

6.1 Correspondence protocol – all councillors using council-owned email systems will ensure the clerk is copied into all correspondence, including replies.

- Applies only to *council business*
- Excludes confidential HR matters
- Excludes correspondence where the Clerk is the subject of a complaint

7. IT Infrastructure Support

Asset Register: Maintained for all council-owned hardware and software.

Maintenance: All devices must be regularly updated and checked for compliance with this policy along with recommended software updates and both strong password with multi-factor authentication enabled where possible.

Training: Users can be given training on IT systems, cybersecurity, data handling, and transparency responsibilities if appropriate

8. Monitoring and Review

Annual Review: This policy will be reviewed annually, or sooner if legislation changes.

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 and DPA 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, employee, or contractor who becomes aware of a data breach must report it immediately to the Clerk (Data Protection Officer/Lead).

Initial Response: The Clerk in consultation with Council will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling 2FA [Two-factor authentication]).

10.2 Investigation

A full investigation will be conducted by the Clerk 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
- 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

- Chevington 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 Chevington Parish Council 19 March 2026 and will be reviewed annually or following a significant incident or legislative change.