Chenies Parish Council
IT and Cybersecurity Policy

1. Purpose
This policy ensures council data stays secure, confidential, and compliant with data protection laws.

2. Scope
This policy applies to all councillors, employees, and contractors using council IT systems.

3. Device Security
- **Passwords**: Use strong passwords with numbers, symbols, and capital letters.
- **Locking**: Lock screens immediately when leaving a device unattended.
- **Updates**: Install software and security updates as soon as prompted.
- **Storage**: Store all council files on approved cloud storage, never on personal hard drives.
- **Loss**: Report lost or stolen devices to the Clerk immediately.

4. Email and Communication
- **Accounts**: Use official @cheniesparishcouncil.gov.uk emails for all council business.
- **Personal Email**: Never use personal email accounts for council correspondence.
- **Phishing**: Do not click links or open attachments from unknown senders.
- **FOI**: Remember that all emails are subject to Freedom of Information requests.

5. Data Protection (GDPR)
- **Privacy**: Only collect and hold personal data required for specific council duties.
- **Sharing**: Never share personal details of residents without explicit consent.
- **Disposal**: Shred sensitive paper documents and permanently delete digital files when no longer needed.

6. Acceptable Use
- **Legality**: Do not use council IT systems to access illegal or inappropriate material.
- **Software**: Do not download or install unauthorised software on council devices.