INFORMATION TECHNOLOGY POLICY

ADOPTED: 15th December 2025

Version Control

Version	Description of Change	Officer	Reviewing Committee	Frequency of Review	Version Approval Date	Next Review Date
1.	Creation	Parish Clerk	Council	Annual	December 2025	December 2026

1. Purpose

1.1 This policy defines how Manea Parish Council manages its uses of Information Technology (IT), in line with the Transparency Code 2015 and the 2025 edition of the Practitioners' Guide. It ensures the Parish Council's digital operations are transparent, secure and compliant with data protection laws.

2. Scope

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

- Desktop and laptop computers, tablets and smartphones.
- Email and cloud-based systems.
- Town Council website, social media and digital publication tools.
- Video conferencing and messaging platforms.

- Personal devices used under Bring Your Own Device (BYOD) provision.

3. Governance and Oversight

3.1 The Parish Clerk and Chairman are the IT Systems Administrators with support from the Parish Council's IT Contractor.

3.2 The Clerk/RFO is the Parish Council's Data Protection Officer.

3.3 The Council oversees implementation, security and compliance.

4. Data Protection and Security

4.1 All processing of personal data shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

4.2 **Privacy Policy**: All data collection, processing and subject rights are governed by the Parish Council's Privacy Policy, available on the Parish Council website. All users must familiarise themselves with it.

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

4.4 **Retention**: Personal data will be retained in accordance with the Parish Council's Management of Council Records Policy and securely deleted when no longer required.

4.5 **Security Controls**:

- Password protection and multi-factor authentication where applicable.
- Regular updates and anti-malware software.
- Backups of essential data in secure locations.

5. Use of Personal Devices (BYOD)

5.1 **Authorised Use Only:** Councillors and staff may use personal devices for council business only if explicitly authorised and subject to compliance with this policy.

5.2 **Security Requirements:** Devices must be protected by strong passwords, encryption (where possible) and up-to-date antivirus software.

5.3 Access to Parish Council data on personal devices must be controlled and subject to regular review.

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

6. Use of Personal Email Addresses

6.1 **Prohibited Practice:** The use of personal email accounts for Parish Council business is strictly prohibited. All Parish Council correspondence must be conducted through official council-provided email addresses. Emails from council-owned domains must not be forwarded to personal email addresses.

6.2 **Monitoring and Compliance:** Any breaches will be investigated and appropriate measures taken in line with the Parish Council's disciplinary or governance procedures.

6.3 **Email Retention:** All Parish Council emails will be stored in compliance with the UK GDPR and Freedom of Information requirements.

7. IT Infrastructure and Support

7.1 **Asset Register**: Maintained for all Parish Council owned hardware, and where relevant software.

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

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

8. Monitoring and Review

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

8.2 **Audits**: Periodic internal audits will check for compliance with security and transparency requirements.

9. Data Breach Process and Protocols

9.1 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

10.1 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 of theft of devices containing personal data.
- Unauthorised access to Parish Council email accounts or files.
- Sending personal data to the wrong recipient.
- Malware or ransomware attacks comprising council systems.

10.2 Reporting a Breach

10.2.1 **Immediate Notification:** Any councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Parish Clerk who will liaise with the Data Protection Officer.

10.2.2 Initial Response: The Data Protection Officer will assess the severity and scope of the breach and determine if mitigation steps are required i.e. changing passwords, disabling access, enabling 2FA, etc.

10.3 Investigation

10.4.1 A full investigation will be conducted by the Parish Clerk or designated member within 72 hours of the breach being discovered. The breach will be logged, including:

- Data and time of breach
- Type and volume of data affected
- Cause and extent of the breach
- Actions taken to address the breach

10.4 Notification Requirements

10.4.1 If the breach is likely to result in a risk to the rights and freedoms of individuals, the Parish Council must notify the Information Commissioner's Office (ICO) within 72 hours.

10.4.2 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

10.5 Remediation and Review

10.5.1 The Parish Clerk and Council will ensure lessons are learned and policies, procedures or training are updated as necessary.

10.5.2 Technical fixes or security upgrades will be prioritised to prevent recurrence.

10.5.3 Breach logs will be reviewed periodically to identify systematic issues.

Alan Melton

Clerk to the Council

December 2025