Ickleton PC: Information Technology Policy

Document name / title	IT Policy
Version number	v2.0
Status (draft, published or superseded)	Published
Distribution	Internal
Author / owner	Clerk
Date of publication	July 2026
Document type (policy, standard, procedure, guide)	Policy
Security classification (confidential, internal, public)	Public
Review Frequency	Annual

1. Introduction

Ickleton Parish Council recognises the importance of secure and effective use of information technology in supporting council operations, communications, record keeping, and service delivery.

This policy establishes the requirements for the secure and appropriate use of council information, technology systems, devices, networks, software, email services, and cloud-based services. It aims to protect council information, comply with legal obligations, and reduce cyber security risks.

2. Scope

This policy applies to all:

- Councillors
- Employees
- Contractors
- Volunteers
- Temporary workers
- Third parties who have access to council information or systems

The policy applies to all council-owned and personal devices used for council business.

3. Roles and Responsibilities

Clerk

The Clerk is responsible for:

- Maintaining this policy
- Coordinating security incident reporting
- Ensuring appropriate security measures are implemented
- Providing or arranging staff and councillor training
- Ensuring compliance with relevant legislation

Councillors, Employees, Contractors and Volunteers

Users are responsible for:

- Following this policy and related procedures
- Protecting council information and equipment
- Using council systems responsibly
- Reporting security incidents promptly
- Completing required cyber security training

4. Acceptable Use

Council IT resources must primarily be used for legitimate council business.

Limited personal use is permitted provided it:

- Does not interfere with council duties
- Does not incur significant cost
- Does not create security risks
- Does not breach any law or council policy

Users must not:

- Access, create, store or distribute offensive, discriminatory or illegal material
- Conduct personal commercial activities
- Circumvent security controls
- Share confidential information without authorisation
- Download or distribute copyrighted material unlawfully
- Use council systems in a manner that may damage the council's reputation

5. Device and Software Management

Where possible, council-approved devices and software will be provided for council business.

Users must:

- Use only authorised software and applications
- Not install software without approval
- Keep operating systems and applications updated
- Enable automatic security updates where possible
- Ensure anti-malware protection is active and updated

Unsupported or obsolete software must not be used for council business.

6. Use of Personal Devices (BYOD)

Where personal devices are used for council business, users must ensure:

- Devices are protected by a password, PIN or biometric authentication
- Devices are configured to lock automatically when unattended
- Operating systems and applications are kept updated
- Anti-malware protection is installed where appropriate
- Council information is stored securely
- Lost or stolen devices are reported immediately to the Clerk

The council reserves the right to require the removal of council information from personal devices where necessary to protect council data.

7. Data Management and Information Security

Council information must be managed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and related council policies.

Information should be classified as:

- **Public** – information approved for public release
- **Internal** – routine council business information
- **Confidential** – sensitive operational information
- **Personal Data** – information relating to identifiable individuals

Users must:

- Access only information required for their role
- Store information securely
- Share information only where authorised
- Dispose of information securely when no longer required

8. Password and Account Security

Users are responsible for maintaining the security of their accounts.

Users must:

- Use strong and unique passwords
- Not share passwords with others
- Use a password manager where appropriate
- Change passwords immediately if compromise is suspected

Multi-Factor Authentication (MFA) must be enabled for council email accounts, cloud services and other systems where available.

9. Email Security and Communication

Council email accounts must be used for official council communications.

Users must:

- Maintain professional and respectful communications
- Verify email senders before opening attachments or links
- Exercise caution regarding phishing attempts
- Report suspicious emails immediately
- Avoid forwarding confidential information unless authorised

Confidential or sensitive information must only be transmitted using approved secure methods.

10. Cloud Services and File Sharing

Only council-approved cloud services may be used for storing or sharing council information.

Users must:

- Use approved sharing permissions
- Restrict access to authorised individuals
- Avoid sharing confidential information through unapproved services
- Review sharing permissions regularly

11. Network and Internet Usage

Council networks and internet connections must be used responsibly.

Users must:

- Access only legitimate business-related services
- Use secure Wi-Fi connections
- Avoid conducting council business over unsecured public Wi-Fi unless suitable security measures are in place
- Follow all applicable copyright and licensing requirements

12. Mobile Working and Remote Access

When working remotely, users must:

- Prevent unauthorised viewing of council information
- Secure devices when unattended
- Ensure confidential discussions cannot be overheard where practical

13. Monitoring and Privacy

The council reserves the right to monitor the use of its IT systems where necessary to:

- Protect council information
- Investigate suspected misconduct
- Ensure compliance with legal obligations
- Maintain system security

Any monitoring will be proportionate, lawful and conducted in accordance with UK GDPR, the Data Protection Act 2018 and other applicable legislation.

14. Records Retention and Archiving

Council records, including emails and electronic documents, must be retained and disposed of in accordance with the council's Records Retention Policy and legal requirements.

Users must not deliberately delete records that are required for operational, legal, audit or regulatory purposes.

15. Reporting Security Incidents

All suspected or actual security incidents must be reported to the Clerk as soon as possible and no later than 24 hours after discovery.

Examples include:

- Phishing emails
- Malware infections
- Unauthorised access
- Loss or theft of devices
- Data breaches
- Accidental disclosure of information

The Clerk will coordinate investigation, containment and any required reporting actions.

16. Training and Awareness

The council will provide appropriate training and guidance on:

- Cyber security awareness
- Data protection responsibilities
- Phishing and social engineering risks
- Secure use of council systems

All councillors, employees and relevant contractors are expected to participate in required training.

17. Compliance and Breaches

Failure to comply with this policy may result in:

- Removal of system access
- Investigation of the incident
- Disciplinary action where applicable
- Referral to law enforcement or regulatory authorities where appropriate

18. Related Policies

This policy should be read alongside:

- Data Protection Policy
- Privacy Notice
- Records Retention Policy
- Code of Conduct

19. Policy Review

This policy will be reviewed annually or sooner where required by changes in legislation, technology, security threats or council operations.

20. Contact

For IT, cyber security or information governance enquiries, contact the Clerk.

All councillors, employees and authorised users share responsibility for maintaining the security of Ickleton Parish Council's information and technology systems. Compliance with this policy helps protect council information, maintain public trust and support effective council operations.

Version History

The version history panel provides a history of the changes made to the document from the initial draft to the current version.

Version	Changes made	Date	Made by
0.1	Draft policy created	7 July 2025	B Benn
1.0	Approved for adoption at July 2025 meeting with minor change to wording.	17 July 2025	B Benn
2.0	Policy updated to reflect current guidance.	25 June 2026	B Benn
2.00	Approved for publication at July 2026 meeting.	22 July 2026	B Benn