Shipston on Stour Town Council

Information Technology (IT) Policy

Document Control

- **Policy Owner: Town Clerk / Responsible Financial Officer (RFO)**
- **Approved by: Full Council**
- **Approval Date: 09/03/2026**
- **Review Frequency: Annual**
- **Next Review Date: 09/03/2027**
- **Version: 1.0**

1. Purpose

This policy establishes the framework for the secure, effective, and lawful use of Information Technology (IT) systems within the Town Council.

It ensures:

- Protection of council information and assets
- Compliance with applicable legislation
- Secure and efficient delivery of council services
- Clear responsibilities for users of council IT resources

2. Scope

This policy applies to:

- All Town Councillors
- Employees (full-time, part-time, temporary)
- Contractors and consultants
- Volunteers with access to council systems
- Third parties granted access to council data

It covers all IT assets including:

- Computers, laptops, tablets, and mobile phones
- Servers and network infrastructure
- Cloud-based systems
- Email and communication platforms
- Council website and social media accounts
- Software and applications
- Data stored electronically or digitally transmitted

3. Legal and Regulatory Compliance

The Council shall comply with all relevant legislation including, but not limited to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

All users must ensure that their use of IT systems complies with these requirements.

4. Roles and Responsibilities

4.1 Full Council

- Approves the IT Policy
- Ensures adequate budget provision for IT security and maintenance

4.2 Town Clerk

- Acts as system owner
- Ensures policy implementation
- Oversees compliance and incident management

4.3 Responsible Financial Officer (RFO)

- Ensures financial controls for IT procurement
- Maintains asset register

4.4 Users

- Use systems responsibly and lawfully
- Protect passwords and confidential information
- Report incidents promptly

5. Acceptable Use

Council IT systems must be used primarily for official council business. Limited personal use is permitted where it:

- Does not interfere with duties
- Does not incur cost to the council
- Does not breach any legislation
- Does not compromise security

The following are strictly prohibited:

- Accessing unlawful or inappropriate content

- Installing unauthorised software
- Sharing confidential information without authority
- Circumventing security controls

6. Information Security

6.1 Access Control

- Unique user accounts must be used
- Passwords must be strong and confidential
- Multi-factor authentication should be enabled where available
- Access must be removed promptly when employment or service ends

6.2 Device Security

- All council devices must be password protected
- Devices must auto-lock after inactivity
- Encryption must be enabled where possible
- Anti-virus software must be installed and maintained

6.3 Remote Working

When working remotely:

- Secure Wi-Fi must be used
- Public networks should be avoided unless VPN-protected
- Devices must not be left unattended in public

7. Data Protection

The Council shall:

- Collect only necessary data
- Store data securely
- Retain data in accordance with the council's retention schedule
- Dispose of data securely

Personal data breaches must be reported immediately to the Town Clerk, who will assess whether notification to the Information Commissioner's Office is required.

8. Email and Communications

- Council email accounts must be used for official business
- Personal email accounts must not be used for council matters
- Suspicious emails must not be opened and should be reported

- Emails form part of the official record and may be subject to disclosure

9. Website and Social Media

- Only authorised personnel may publish content
- Content must be lawful, accurate, and respectful
- Accounts must use secure passwords and multi-factor authentication
- Administrative access must be documented and reviewed annually

10. Procurement and Asset Management

- All IT purchases must follow the Council's Financial Regulations
- Software must be properly licensed
- An IT asset register must be maintained
- Disposal of equipment must ensure complete data destruction

11. Business Continuity and Backups

- Critical systems must be regularly backed up
- Backups should be encrypted and stored securely
- Backup restoration must be tested periodically
- IT risks must form part of the Council's Risk Register

12. Incident Management

All IT security incidents, including suspected data breaches, must be reported immediately to the Town Clerk.

Incidents may include:

- Lost or stolen devices
- Malware infections
- Unauthorised access
- Accidental disclosure of confidential information

An incident log must be maintained.

13. Monitoring

The Council reserves the right to monitor the use of its IT systems to:

- Ensure compliance with policy

- Protect system integrity
- Investigate misconduct

Monitoring will be proportionate and lawful.

14. Training

All councillors and staff will receive:

- Data protection awareness training
- Cyber security awareness training
- Refresher training as required

15. Breach of Policy

Failure to comply with this policy may result in:

- Disciplinary action
- Withdrawal of system access
- Referral to appropriate authorities

16. Policy Review

This policy will be reviewed annually or sooner if:

- There are changes in legislation
- Significant IT changes occur
- An incident indicates policy revision is required

Declaration

This policy was adopted by Shipston Town Council at its meeting on 09/03/2026