Information Technology Policy 2025 for Barwick and Scholes Parish Council

1 Introduction and Scope

1.1 Policy Purpose

This Information Technology Policy establishes the framework for the secure, compliant, and appropriate use of all information technology resources within Barwick and Scholes Parish Council. This policy is designed to meet our legal obligations under relevant UK legislation while supporting the Council's operational needs and service delivery to our community. The policy embodies our commitment to maintaining the highest standards of data security, privacy, and responsible technology use in accordance with the **Yorkshire Local Councils Associations (YLCA)** guidelines for parish councils and the **SAPPP 2025 Practitioners' Guide** requirements for digital compliance . All council members, employees, contractors, and volunteers ("Users") are required to comply with this policy when accessing or handling council IT resources and data.

1.2 Scope and Application

This policy applies to all information technology systems owned, leased, or operated by Barwick and Scholes Parish Council, including but not limited to: computer hardware, software applications, network infrastructure, cloud services, email systems, internet access, mobile devices, telecommunication equipment, and all data stored processed or transmitted through these systems. The policy extends to **all users** including council members, employees, contractors, volunteers, and any third parties who access council systems or data, regardless of ownership of the device used to access these resources. This policy complements and should be read in conjunction with the Council's existing **Privacy Policy**, **Data Protection Policy**, and **Social Media Policy** .

1.3 Responsibilities and Governance

The Parish Council as a whole maintains ultimate responsibility for ensuring compliance with this policy and relevant legislation. The Council Clerk will serve as the designated

Data Protection Officer (DPO) and IT Lead, responsible for day-to-day implementation, monitoring, and maintenance of this policy. All users bear individual responsibility for understanding and adhering to this policy, completing required training, and reporting any suspected violations or security concerns immediately. The Council will provide appropriate resources and training to ensure all users can meet their obligations under this policy.

2 Legal Framework and Compliance

2.1 Data Protection Legislation

Barwick and Scholes Parish Council is committed to full compliance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and any subsequent data protection legislation. Our processing of personal data follows the data protection principles requiring that personal data be processed **lawfully, fairly, and transparently**; collected only for **specific, explicit purposes**; **adequate, relevant and limited** to what is necessary; **accurate and kept up to date**; kept in an identifiable form for **no longer than necessary**; and secured against **unauthorized access, loss or damage**. The Council recognizes its role as a **data controller** under these regulations and maintains appropriate registration with the Information Commissioner's Office (ICO) .

2.2 Computer Misuse Act 1990

All users must comply with the **Computer Misuse Act 1990** which prohibits unauthorized access to computer systems. Specifically, users must not:

- Access or attempt to access council systems or data without authorization or in excess of granted authorization
- Enable unauthorized access to council systems, including by sharing passwords or access credentials
- Modify, delete, or interfere with council systems, software, or data without explicit authorization
- Create or introduce malware, including viruses, ransomware, or other harmful code to council systems
- Use council systems to commit any unlawful act or facilitate offenses under the Computer Misuse Act

Violations of the Computer Misuse Act may result in **criminal prosecution** with penalties including unlimited fines and imprisonment of up to 14 years for serious offenses.

2.3 Malicious Communications Act 1988 and Online Safety Act 2023

Users must comply with the **Malicious Communications Act 1988** and relevant provisions of the **Online Safety Act 2023** when using council communication channels. Specifically, users must not:

- Send or cause to be sent any communication that is grossly offensive, indecent, obscene, or menacing
- Make persistent use of communications networks to cause annoyance, inconvenience, or anxiety
- Send communications containing false information intended to cause distress, anxiety, or harm
- Engage in cyber-flashing or sharing intimate images without consent
- Encourage or assist serious self-harm through electronic communications

Communications offenses may result in **criminal liability** and disciplinary action, including removal from council position.

2.4 YLCA Compliance Standards

This policy aligns with the **Yorkshire Local Councils Associations (YLCA)** guidelines for parish councils, which emphasize:

- Maintaining clear, documented policies for IT and data protection
- Designating responsible officers for data protection and IT security
- Implementing appropriate technical and organizational security measures
- Providing regular training for council members and staff
- Conducting periodic reviews of policies and procedures
- Maintaining proper records of processing activities and data breaches

2.5 SAPPP 2025 Digital Compliance Requirements

This policy fulfills the requirements of Assertion 10: Digital and Data Compliance in the Annual Governance Statement as outlined in the SAPPP 2025 Practitioners' Guide. The Council acknowledges that having a written IT policy is no longer just best practice but a mandatory requirement for smaller authorities effective April 2025 .

3 Acceptable Use Policy

3.1 Authorized Use of IT Resources

Council IT resources are provided for official council business only. Limited personal use is permitted only if it: does not interfere with council operations; complies with this policy and all applicable laws; does not incur additional costs to the council; and does not violate the Council's ethical standards. Users must not use council IT resources for:

- Personal financial gain or commercial activities
- Political campaigning (except in official council capacity)
- Harassment, discrimination, or offensive behavior
- Illegal activities or accessing illegal content
- Extensive personal entertainment or gaming

3.2 Account and Access Management

All users must access council systems using unique individual accounts – shared accounts are strictly prohibited unless explicitly authorized for specific service accounts. Users must not **share passwords** or other authentication credentials with anyone, including colleagues or administrative staff. The Council will implement strong password requirements mandating minimum length (12 characters), complexity (mix of character types), and regular changes (every 90 days). **Multi-factor authentication (MFA)** should be enabled for all systems containing personal or sensitive data. User accounts should be reviewed quarterly and promptly disabled when users leave council service or change roles .

3.3 Prohibited Activities

The following activities are strictly prohibited on council IT systems:

- Attempting to access data or systems without authorization
- Unauthorized copying, distribution, or removal of council data
- Circumventing security measures or testing system vulnerabilities without authorization
- Accessing or distributing offensive, obscene, or illegal material
- Installing unauthorized hardware or software on council systems
- Using unauthorized external cloud services or file-sharing platforms for council data
- Connecting unauthorized storage devices (e.g., USB drives) without security scanning

4 Data Protection and Management

4.1 Data Processing Principles

The Council will process personal data in accordance with the data protection principles as outlined in the **UK GDPR and Data Protection Act 2018** . The Council's data processing activities will adhere to the following principles:

Table: Data Protection Principles Implementation

Principle	Description	Implementation
Lawfulness, fairness, transparency	Process data lawfully, fairly, and transparently	Privacy notices, lawful basis documentation
Purpose limitation	Collect for specified, explicit, legitimate purposes	Clear purpose statements, compatibility assessments

Data minimization	Adequate, relevant, and limited to what is necessary	Data collection reviews, field minimization
Accuracy	Accurate and kept up to date	Validation procedures, regular data reviews
Storage limitation	Kept in identifiable form no longer than necessary	Retention schedules, automated deletion
Integrity and confidentiality	Secured against unauthorized access	Encryption, access controls, security policies

4.2 Data Subject Rights Procedure

The Council should establish a formal procedure for handling data subject requests in accordance with data protection legislation. The Council Clerk (as DPO) will manage all requests regarding:

- **Subject Access Requests (SARs)**: Respond within one month with requested information
- **Rectification**: Correct inaccurate or incomplete personal data without undue delay
- **Erasure**: Delete personal data where no lawful basis for processing exists
- **Restriction**: Temporarily suspend processing of disputed data
- **Data portability**: Provide data in structured, commonly used, machine-readable format
- **Automated decision-making**: Ensure meaningful human intervention in significant decisions

All requests will be logged and tracked to ensure compliance with statutory timeframes. The Council may verify the identity of requestors before processing requests.

4.3 Data Retention and Disposal

The Council will maintain a **data retention schedule** specifying retention periods for all categories of personal data, based on legal requirements and business needs. Financial

records will be retained for **7 years** to support audits, while other records will be retained in accordance with statutory requirements. Data will be disposed of securely using appropriate methods: paper records will be cross-shredded; digital storage media will be physically destroyed or securely wiped using approved methods; cloud storage will be permanently deleted using provider-specific secure deletion tools.

4.4 Data Breach Response

The Council will implement a data breach response plan outlining steps to contain, assess, and respond to suspected data breaches. All suspected breaches must be reported immediately to the Council Clerk (DPO). The Council will:

- Contain the breach and assess its likely risks
- Notify the ICO within 72 hours if required under UK GDPR
- Inform affected data subjects where there is a high risk to their rights and freedoms
- Document all breaches regardless of whether notification is required
- Implement corrective actions to prevent recurrence

5 Communications Standards

5.1 Email and Electronic Communications

Council email accounts are provided for official communications and must be used professionally. All official communications must use council-owned email addresses (e.g., clerk@barwickandscholespc.org) rather than personal email accounts to ensure continuity and prevent data loss when personnel change . All emails containing personal data must be encrypted or transmitted securely. Users must not:

- Send sensitive data via email without encryption or password protection
- Click on suspicious links or attachments from unknown senders
- Use "Reply All" unnecessarily or disclose email addresses without consent
- Auto-forward emails to external accounts without authorization
- Engage with spam, or mass unsolicited communications

5.2 Social Media Policy Implementation

The Council adopts and incorporates its existing Social Media Policy (updated 2025) as an integral part of this IT Policy. The Social Media Policy establishes guidelines for both official council social media use and personal use by council members and staff when referencing the council.

5.2.1 Official Social Media Use

- Only authorized personnel (typically the Clerk or Chairperson) may create, maintain, or post on official council social media accounts
- All content must be professional, accurate, and aligned with the council's values and objectives
- Confidential or proprietary information about the council, its employees, or stakeholders must not be disclosed
- Engagement with users should be constructive and positive, avoiding responses to inflammatory or inappropriate comments
- The council's website remains the primary source for official information, with social media directing users to the website for comprehensive details

5.2.2 Personal Social Media Use

- Council members and staff should differentiate between personal opinions and official council positions when discussing council matters
- Users are expected to interact respectfully on social media, avoiding content that could be considered discriminatory, harassing, or defamatory
- If mentioning the council, users should adhere to the council's branding guidelines and avoid negative or inappropriate references
- Users must not disclose confidential information about the council, its clients, or stakeholders

5.2.3 Social Media Security

- Strong, unique passwords must be used for all official social media accounts
- Multi-factor authentication should be enabled where available
- Official social media accounts must not be accessed from public or unsecured devices

- Any suspected unauthorized access to social media accounts must be reported immediately to the Council Clerk

5.3 Recording and Monitoring

The Council may monitor use of IT systems to ensure security, compliance, and proper use. Monitoring may include:

- Logging of website visits and network traffic
- Scanning of emails for malware and security threats
- Review of system access and user activity
- CCTV monitoring of Council premises

Users will be informed of monitoring activities through this policy. By using Council IT systems, users **consent to reasonable monitoring** for these purposes.

6 Security Policies

6.1 Access Control

The Council will implement the **principle of least privilege**, granting users access only to data and systems necessary for their role. Access rights will be **reviewed quarterly** and adjusted following role changes. All access to sensitive systems and data should require multi-factor authentication. Third-party access will be granted only under written agreement with appropriate security commitments. All remote access should use secure encrypted connections (VPN).

6.2 Device Management

All devices used to access Council systems or data, including personally owned devices (BYOD), must:

- Be password protected with automatic lock screens
- Have encryption enabled for all storage
- Run approved antivirus and security software
- Keep operating systems and applications updated

- Not be left unattended in public places

Personally owned devices must be explicitly authorized for Council use and may be subject to security scanning.

6.3 Network Security

The Council will implement and maintain:

- Firewall protection for all internet connections
- Secure Wi-Fi with encryption for official networks
- Separate guest networks with no access to internal systems
- Regular vulnerability scanning and security assessments
- Network segmentation to limit access to sensitive systems

6.4 Software and Cloud Services

All software and cloud services must be **approved in advance** by the Council Clerk. Users must not install unauthorized software or subscribe to cloud services. The Council will:

- Maintain an inventory of all software and services
- Ensure regular updates and security patches are applied
- Prefer UK-based data centers for cloud services where feasible
- Establish data processing agreements with all third-party providers

7 Incident Response and Reporting

7.1 Reporting Procedure

All suspected security incidents, policy violations, or data breaches must be reported **immediately** to the Council Clerk (DPO). Reports should include:

- Date and time of the incident
- Persons involved or affected
- Systems or data impacted
- Description of what occurred

- Actions already taken

The Council will not **retaliate against** anyone for reporting suspicions in good faith, unless found threw investigation and evidence to have conducted this behaviour deliberately.

7.2 Investigation Process

The Council Clerk will:

- Investigate all reported incidents promptly
- Document findings and actions taken
- Notify the Council Chairperson of significant incidents
- Engage law enforcement if criminal activity is suspected
- Implement corrective actions to prevent recurrence

7.3 Business Continuity

The Council will maintain **regular backups** of critical systems and data. Backups will be:

- Performed at least monthly
- Stored securely
- Tested regularly for integrity and restoration capability
- Encrypted to protect confidentiality

8 Policy Management and Administration

8.1 Training and Awareness

All users should receive **comprehensive training** on this policy upon appointment and **annual refresher training** thereafter if required or requested. Training will cover:

- Data protection principles and responsibilities
- IT security best practices
- Recognizing and reporting security threats
- Specific procedures for handling personal data
- Updates on legal and regulatory changes

8.2 Policy Review and Updates

This policy will be reviewed annually or following significant changes in technology, legislation, or Council operations. The Council Clerk will recommend updates to ensure continued compliance with relevant legislation including the **Data Protection Act 2018**, **UK GDPR**, **Computer Misuse Act 1990**, and **Malicious Communications Act 1988**. Changes will be approved by full Council resolution .

8.3 Enforcement and Violations

Violations of this policy may result in **disciplinary action**, up to and including dismissal for employees or removal from council position for members. Serious violations may also result in **civil or criminal liability** under applicable laws. The Council will consider all relevant factors when determining appropriate sanctions, including the nature and severity of the violation, whether it was intentional or reckless, and the user's history of compliance.

8.4 Approval and Implementation

This policy was approved by resolution of the Barwick and Scholes Parish Council on 03/11/2025 and takes effect immediately. The policy supersedes all previous IT-related policies and will be made available to all users and published on the Council website in accordance with transparency principles.

Appendix A: Related Documents and Legislation

- Data Protection Act 2018
- UK General Data Protection Regulation
- Computer Misuse Act 1990
- Malicious Communications Act 1988
- Online Safety Act 2023
- Barwick and Scholes Parish Council Privacy Policy
- Barwick and Scholes Parish Council Social Media Policy (2021)
- YLCA Guidelines for Parish Councils

- SAPPP 2025 Practitioners' Guide

Appendix B: Incident Report Form
(Template for reporting security incidents) under development

Appendix C: Data Processing Inventory
(Register of personal data processing activities) under development and review to determine necessity

Appendix D: Retention Schedule
(Detailed data retention periods by data category) under development and review to determine necessity

Appendix E: Social Media Policy Summary
(See stand alone Social Media Policy in policy libary)

This policy will be reviewed annually or following significant legislative changes. Next scheduled review: November 2026.