BARTON-LE-CLAY PARISH COUNCIL

IT POLICY

1. Purpose

This IT Policy sets out how Barton le Clay Parish Council ("the Council") manages and uses information technology resources, digital communications, data processing and storage, and website/email systems. The aim is to ensure that the Council meets its legal and regulatory obligations under the Data Protection Act 2018, UK GDPR and supports the Council in answering "Yes" to Assertion 10 ("Digital & Data Compliance") in its Annual Governance Statement.

2. Scope

This policy applies to:

- All elected members (Councillors) of the Council
- All employees (clerks, administrative staff) of the Council
- Contractors, volunteers, and others who access or use the Council's IT systems or process Council data
- All devices, software, email accounts, website hosting, cloud solutions used for Council business (whether Council-owned or personal devices used for Council business)

3. Governance & Responsibilities

- The Council bears overall responsibility as Data Controller for the personal data it processes, and as Data Processor where applicable.
- The Clerk (or designated Responsible Officer) is responsible for overseeing the implementation of this policy, coordinating IT and data compliance, liaising with any external IT/data advisors, and reporting to the Council.
- Councillors and staff must comply with the policy, complete any required training, and promptly report any IT incidents (security breaches, data loss, unauthorised access).
- Any new IT system, website change, or cloud service must be approved by the Clerk (or designated officer) and assessed for risks (security, data protection, accessibility) before implementation.

4. Email and Domain Use

- All Council-related communications must use a generic Council email address hosted on a domain owned and controlled by the Council (or via a service where the Council owns the domain). Free consumer email services (e.g., Gmail, Hotmail) must **not** be used for Council business.
- Examples: the parishclerk@bartonleclay-pc.gov.uk
- Councillors should not use personal email accounts for Council business.
- Email accounts must have password protection, be encrypted where feasible, and use two-factor authentication (2FA) where available.
- When a Councillor, staff member or contractor leaves the Council, their email account access must be revoked and access to shared folders or archives secured.
- Barton-le-Clay Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

5. Website and Accessibility

- The Council's website must fully comply with the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.
- The website domain should be Council-owned. The site must publish all required documents under the Transparency Code for Smaller Authorities (e.g., minutes, agendas, AGAR, expenditure above £100, asset register) and contain a current accessibility statement.
- The Clerk (or a delegated officer) is responsible for regular review of the website (links, accessibility, content publication) and annual or periodic external audit of compliance.

6. Data Protection & Digital Governance

- The Council processes personal data and must do so lawfully, fairly and transparently, in line with UK GDPR principles.
- A data audit must be maintained, documenting the categories of personal data held, the purpose(s) for processing, lawful basis, retention periods, where data is stored, who has access, how it is shared, how it is disposed of.
- Personal data should only be stored on Council-approved systems. Use of personal devices or unmanaged cloud services must be risk-assessed and approved in advance.
- Data breach protocol: Any suspected data breach must be reported immediately to the Clerk, investigated, documented, and, if required, notified to the Information Commissioner's Office within the required timescales.
- Data retention and disposal: Personal data shall be retained only as long as reasonably necessary. Secure methods must be used to delete or anonymise data when no longer required.
- Training: All Councillors, staff and relevant volunteers must receive regular training on data protection, cybersecurity risks (e.g., phishing), and this IT Policy.
- Access controls: Data access must be restricted on a "need to know" basis, with role-based permissions* regularly reviewed.
  *(*Schedule of role-based permissions to be implemented by August 2026)*

7. Use of Devices and Software

- Council-owned devices (laptops, tablets, mobile phones) must only be used for authorised Council business; software installations require prior approval. Devices must have up-to-date antivirus and software updates installed.
- Use of personal devices for Council business must be approved in writing with conditions (e.g., encryption, password protection, separation of personal / Council data). All users to complete and sign the *General Data Protection Awareness Checklist and Acceptance of Electronic Summons* Documents.
- Cloud services: Only Council-approved cloud services shall be used to store sensitive Council data or files. Any new service must undergo a security and data protection risk assessment before adoption.
- Back-up procedures: The Council must implement regular back-ups of vital data and test restore capability periodically. Back-ups must be stored securely, ideally off-site or in a separate environment.
- Passwords: All users shall follow secure password policy (strong complexity, avoid reuse, changed periodically) and enable two-factor authentication where available.
- Removable media (USB drives) must not be used without encryption and must be approved by the Clerk.
- Lost or stolen devices: Any loss of a device used for Council business must be reported immediately and remedial action (remote wipe, change passwords) taken.

8. Cybersecurity & Incident Management

- The Council will maintain appropriate security controls to protect its IT systems, software and data, including firewalls, anti-malware, encryption and intrusion detection (where feasible).
- Staff and Councillors will receive regular reminders/training on phishing, social engineering, suspicious attachments/links, and safe email usage.
- Incident response: The Council will maintain an incident response log that captures IT security incidents and the investigations carried out. The Clerk is the designated incident response lead.
- The Council will undertake periodic risk assessments of its IT infrastructure and data processing, and maintain a risk register for digital/data risks, with mitigation actions assigned and tracked.

9. Third-Party Providers & Service Contracts

- Where the Council contracts external IT or cloud service providers, the contract must clearly specify data protection responsibilities, security standards, access controls, data ownership, and incident response obligations.
- The Council will maintain an inventory of all third-party providers used and review their performance and compliance annually or when there is a significant change.

10. Policy Review and Training

- This policy will be reviewed annually by the Council (or sooner if there are significant changes in technology, regulation or the Council’s operations).

- The Clerk will report to the Council on compliance with this policy, any incidents, and any recommended amendments.
- All Councillors, staff and volunteers with IT/data responsibilities will complete induction training and annual refresher training. Training records will be maintained.

11. Monitoring and Enforcement

- Compliance with this policy will be monitored by the Clerk and, where relevant, by the Council's internal auditor or an external reviewer.
- Breaches of the policy may result in disciplinary action (for staff) or in the case of Councillors, referral to the Council's Code of Conduct or appropriate procedures.
- The Council will maintain records of audits, incident reports, training attendance and policy review minutes for audit and transparency purposes.

12. Declaration

By adopting this policy, Barton le Clay Parish Council affirms its commitment to managing its digital presence, data and IT systems in a secure, lawful and transparent manner, in order to satisfy the requirements of Assertion 10 of the Annual Governance Statement: i.e., digital and data compliance.

Assertion 10: Compliance Checklist

Item	Evidence location	Status (Y/N)
1. Council has adopted a formal IT policy, approved by full council, and reviewed annually.	Minutes of meeting + policy document date.	
2. Council uses a domain it owns (e.g., *.gov.uk or *.org.uk) for its official website and email addresses.	Domain registration details; email addresses list.	
3. Free consumer email services (Gmail, Hotmail, etc.) are **not** used for Council business.	Council email policy + review of active email accounts.	
4. All Councillors, staff, contractors using Council email addresses (on Council domain) for Council business.	Listing of users + email audit.	
5. Website meets legal accessibility standard (WCAG 2.2 AA) and has an accessibility statement.	Accessibility audit report + statement on website.	
6. Website publishes required transparency documents (minutes, agendas, AGAR, asset register, expenditure over threshold).	Website pages/screenshots.	
7. Council holds a data audit: what personal data is held, where, why, lawful basis, retention, disposal.	Data audit register.	
8. Personal data stored only on approved systems; use of personal devices/cloud is risk-assessed and approved.	Device policy + risk assessment forms.	
9. Access controls in place: role-based access, review of permissions.	Access log / review minutes.	
10. Back-up and restore procedures exist, tested periodically.	Back-up schedule + test records.	
11. Cyber security safeguards: antivirus/updates/firewall/2FA where available, training for users.	Training log + IT system report.	
12. Incident response log exists; for capturing, investigating and notifying data breaches.	Incident response log + investigating register.	
13. Third-party service providers handling Council data have contracts specifying data protection/security responsibilities.	Contract register + template contract.	
14. Policy is reviewed annually and updated for changes in legislation/technology.	Review schedule + minutes of review.	