

Barton Bendish Parish Council

IT Policy

1. Purpose and Scope

This policy sets out how Barton Bendish Parish Council uses technology to carry out its business securely, legally, and efficiently.

It applies to all councillors, the clerk, contractors, and volunteers who use IT systems or devices to conduct council business whether using council-owned or personal equipment.

2. Council Email Use

- All official council communication must use the council's email domain (e.g. clerk@bartonbendish-pc.gov.uk).
- Personal email accounts must not be used for council business.
- Emails must not be forwarded to private inboxes.
- Passwords must be strong, unique, and changed regularly.

3. Data Protection and GDPR

- Personal data must be handled in accordance with the Council's Data Protection Policy.
- The Council does not routinely collect or store personal data. Where personal data is received (e.g. in public emails), it will only be shared with explicit written consent or as legally required.
- Personal data must not be stored unencrypted on USB drives or cloud platforms without prior approval.
- All Freedom of Information (FOI) or Subject Access Requests (SARs) must be referred to the Clerk.

4. Website Management and Accessibility

- The Clerk is responsible for maintaining the Council website.
- The website will comply with WCAG 2.2 AA accessibility standards.
- The following must be published and kept up to date: meeting agendas & information and minutes, AGAR, councillor contact details, and financial reports.
- An up-to-date Accessibility Statement will be maintained and reviewed as required.

Barton Bendish Parish Council

5. Use of Equipment

- The Clerk uses council-owned equipment, including a laptop and mobile phone. These remain the property of the Council.
- Councillors use personal devices for council communications. These devices must be protected by passwords and have up-to-date antivirus software where possible.
- Council-owned equipment must be returned when a role or project ends.

6. Cybersecurity

- Antivirus software must be installed and regularly updated on council devices.
- Passwords must be strong and not reused across other personal or work accounts.
- All users should be cautious of suspicious emails and phishing attempts.

7. Informal Internal Communications

- The Council operates a WhatsApp group for informal internal updates and reminders only. No council decisions are made or discussed via WhatsApp. Messages in the group are set to auto-delete.

8. Training and Review

- The Clerk and councillors will receive basic guidance on secure IT use and data protection.
- This policy will be reviewed bi-annually or sooner if required by changes in law, guidance, or local procedures.
- Responsibility for updating the policy lies with the Clerk in consultation with the Council.

Adopted Sept 2025

Review Sept 2027