Bishop Middleham Parish Council

IT Policy

DOCUMENT CONTROL	
Version Number	V1 – 2026
Adopted on	8th April 2026
Reviewed	
Next Review	April 2028

Applies to: All councillors, the Clerk/RFO, volunteers, and contractors using council IT systems or accessing council data

1. Purpose of this Policy

This IT Policy ensures Bishop Middleham Parish Council complies with Assertion 10 of the Annual Governance and Accountability Return (AGAR), requiring appropriate and secure IT systems, controls to protect data and systems, and clear procedures for access, security, backup, and incident reporting. This policy supports the Council's Data Protection Policy, HR Data Protection Policy, Privacy Notice, and Retention & Disposal Policy.

2. Scope

This policy applies to all council-owned devices, personal devices used to access council email or data, cloud services (OneDrive, email hosting), specialist software (Rialtas, Pear Mapping), and website hosting and email services (Franklin Web / A2 Hosting). It covers all councillors, the Clerk, volunteers, and contractors.

3. IT Systems Used by the Council

- Council-owned devices: Windows laptop (Clerk only), council-owned mobile phone (Clerk only).
- Software: Microsoft 365, McAfee antivirus, Rialtas accounting software, Pear Mapping software.
- Cloud services: OneDrive (Microsoft), email hosting via Franklin Web / A2 Hosting.
- Backups: OneDrive automatic cloud backup; no local backups used.

4. Access Controls

Only the Clerk has access to the council laptop and mobile phone. Councillors access only their @bishopmiddleham-pc.gov.uk email accounts. Contractors access only the data required for their function. No shared devices are used. Access to systems is removed immediately when a councillor or contractor leaves.

5. Password and Authentication Requirements

Strong passwords must be used on all devices and accounts. The Clerk's laptop uses password protection and facial recognition. Councillors must secure personal devices with a password or biometric lock. Passwords must not be shared. Multi-factor authentication (MFA) should be enabled where available.

6. Use of Personal Devices (Councillors)

Councillors may use personal devices to access their council email accounts only if the device is secured with a password or biometric lock, has up-to-date antivirus protection, is kept updated with security patches, and does

not store council documents permanently. Lost or stolen devices must be reported immediately to the Clerk.

7. Data Storage and Security

All council documents must be stored in OneDrive or on the Clerk's laptop. Paper records must be kept in locked storage. No council data may be stored on USB sticks or external drives. No data may be stored permanently on councillors' personal devices. Email attachments should be downloaded only when necessary and deleted after use.

8. Software Updates and Patching

The Clerk must ensure the council laptop and mobile phone install updates promptly. Councillors must keep personal devices updated if used for council business. Antivirus software must be active and up to date.

9. Third-Party Providers

The Council uses the following third-party providers: Franklin Web / A2 Hosting (website and email hosting), Microsoft OneDrive (cloud storage and backup), Durham County Council (payroll processing), Rialtas (accounting software), Pear Mapping (mapping software). All providers must meet UK GDPR security standards.

10. Email and Communications Security

Councillors must use only their official gov.uk email addresses for council business. Personal email accounts must not be used. Sensitive information must not be sent unencrypted. Phishing emails must be reported immediately to the Clerk.

11. Use of WhatsApp

The Council has adopted WhatsApp as an official communication tool for internal discussions. WhatsApp may be used for informal conversations relating to agenda items; however, it must not be used for decision-making or for the sharing of confidential, sensitive, or personal data. Councillors must ensure that any device used to access WhatsApp is secured with a password or biometric lock.

For security purposes, general discussion messages are automatically cleared every 90 days.

Notwithstanding this automatic deletion, WhatsApp messages relating to council business **may fall within the scope of the Freedom of Information Act (FOIA)**. Councillors must therefore forward any WhatsApp messages relevant to a valid FOI request to the Clerk upon request.

The Council's official communication channel for all formal correspondence and decision-related matters remains the council email system.

12. Backups and Business Continuity

OneDrive provides automatic cloud backup of council files. In the event of device failure, files can be restored from OneDrive. The Clerk is responsible for ensuring backup integrity. The Chair must be informed if the Clerk is unavailable during an incident.

13. Incident Reporting and Cybersecurity

All IT issues, suspected breaches, or suspicious activity must be reported immediately to the Clerk and the Chair (if the Clerk is unavailable). Incidents include lost or stolen devices, unauthorised access, malware or ransomware, phishing attempts, and accidental data disclosure. The Clerk will follow the Data Breach Procedure and notify the ICO if required.

14. Prohibited Activities

Using personal email for council business, sharing passwords, installing unauthorised software, storing council data on USB sticks, using public Wi-Fi without a secure connection, and forwarding council emails to personal accounts.

15. Training and Awareness

The Council will provide training or guidance on secure use of personal devices, email security, recognising phishing attempts, password best practice, and data protection responsibilities.

16. Review

This policy will be reviewed every two years or sooner if legislation, technology, or council activities change.

End of policy.