BLACKBIRD LEYS PARISH COUNCIL
Information Technology Policy

Applies to	The Parish Clerk and all councillors
Council IT setup	Council-owned laptop (Clerk); councillors use personal devices (BYOD)
Storage	Dropbox (primary document storage), Google Drive, and Parish Online
Email	clerk@blackbirdleyspc.gov.uk (authority-owned domain)
Date adopted	31 March 2026
Review date	March 2027
Related policies	Data Protection Policy and Privacy Notice

1. Purpose

This policy sets out how the Parish Clerk and councillors should use IT equipment and digital systems when carrying out council business. Its purpose is to protect the council's data, maintain public trust, and ensure compliance with data protection law and the requirements of Assertion 10 of the Annual Governance and Accountability Return (AGAR).

Blackbird Leys Parish Council recognises that it operates with a larger councillor body than some smaller authorities. This policy is written to reflect its actual IT arrangements and is proportionate to its size and resources.

2. Scope

This policy applies to:

- The Parish Clerk, in the use of the council-owned laptop and council email account
- All councillors, when using personal devices to access council systems, email, or documents

3. Council IT Equipment

3.1 The Clerk's Laptop

The council owns one laptop, used solely by the Clerk to carry out council business. The Clerk is responsible for its care and security.

- The laptop must be kept physically secure when not in use
- It must be password protected and locked when unattended
- It must not be used by family members or other individuals
- Council data must be saved to the council's cloud storage systems, not stored locally where avoidable
- The laptop must be kept up to date with software and security updates
- If the laptop is lost, stolen or significantly damaged, this must be reported to the Chair of the Council immediately

3.2 Passwords and Security

The Clerk is responsible for all password management for council systems.

- All accounts must use a strong password. The National Cyber Security Centre (NCSC) recommends using three random words (e.g. PurpleCandleRiver)
- Passwords must not be shared or written down in an insecure location

- Where available, Multi-Factor Authentication (MFA) should be enabled — this means confirming your identity by a second method such as a code sent to your phone
- A sealed copy of critical passwords should be held by the Chair, for emergency use only
- If a password is suspected to have been compromised, it must be changed immediately

4. Use of Personal Devices (Councillors)

The council recognises that councillors use their own smartphones, tablets or laptops to carry out council business, including reading emails and accessing council documents. This is acceptable provided the following conditions are met.

Councillors using personal devices for council business must:

- Use their council email address (not a personal email address) for all council-related correspondence
- Ensure their device is protected with a PIN, password or biometric lock
- Not forward council emails to personal email accounts
- Keep council documents within the council's designated storage systems — files must not be saved to personal cloud storage accounts
- Ensure that council information cannot be viewed by other household members
- Report to the Clerk immediately if a device used to access council systems is lost or stolen
- Delete any locally cached council data from their device if they leave the council

No councillor is required to use a personal device for council business. The Clerk can provide documents and agendas by other means if preferred. Councillors who do use personal devices are personally responsible for the security of those devices. The council cannot provide technical support for personal devices.

5. Email

The council's official email address is hosted on an authority-owned .gov.uk domain. All official council communications must use this address.

- The council email account must be used for all council business — personal email accounts must not be used for council matters
- Councillors must use their council email address when corresponding on council business
- Be cautious of unsolicited or unexpected emails, especially those asking you to click links or provide login details (phishing). If in doubt, do not click — contact the Clerk
- Do not open email attachments from unknown senders
- Emails containing personal data about residents or others should be treated with care and not forwarded unnecessarily

6. Council Document Storage

The council uses three systems for document storage and sharing, all managed by the Clerk:

- Dropbox — the council's primary document storage for working files and council documents
- Google Drive — used for collaborative working and document sharing as required
- Parish Online — used for asset-related information and public-facing council data

The following rules apply to all three systems:

- All council documents must be stored in the council's designated systems, not in personal storage accounts
- Councillors may be given view or edit access to specific folders as required
- Access will be removed when a councillor leaves the council
- Council documents must not be shared externally without the Clerk's authorisation
- Files must not be copied or downloaded to personal cloud storage (e.g. personal Dropbox, iCloud, personal Google Drive)

7. Working from Home

The Clerk works from home. The following precautions apply:

- The laptop must not be used on public or unsecured Wi-Fi networks for council business where this can be avoided
- The screen should be positioned so that council information cannot be seen by others
- Printed council documents must be stored securely and disposed of by shredding
- Backups of essential council data are maintained via the council's cloud storage systems

8. Data Protection

All use of IT equipment and systems must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Full details are set out in the council's Data Protection Policy and Privacy Notice.

- Personal data about residents, councillors or others must only be used for the purpose for which it was collected
- Personal data must not be stored on personal devices or personal cloud storage
- Any suspected data breach must be reported to the Clerk immediately so it can be assessed and, if necessary, reported to the Information Commissioner's Office (ICO)

9. Acceptable Use

IT equipment and council systems must be used appropriately and professionally. The following are not permitted:

- Using the council email address or storage systems for personal matters
- Accessing, downloading or sharing inappropriate, offensive or illegal content
- Installing unauthorised software on the council laptop
- Representing personal views as those of the council on social media or online

Councillors should be mindful of the Nolan Principles and the Members' Code of Conduct in all online activity that relates to their role on the council.

10. Reporting Problems

Any of the following must be reported to the Clerk (or, if involving the Clerk, to the Chair of the Council) as soon as possible:

- Loss or theft of any device used to access council systems
- A suspected data breach or unauthorised access to council data
- Receipt of suspicious emails or suspected phishing attempts
- Any other IT security concern

11. Review

This policy will be reviewed annually, or sooner if there is a significant change to the council's IT arrangements or relevant legislation.

Adopted by Blackbird Leys Parish Council	**Next review due**
Date: 31.03.2026 Signed (Chair): Imade Edosomwan	Date: March 2027 Version: 1.0