Bring Your Own Device (BYOD) Policy

Policy	08S
Officer Responsible	Manager Information Technology
Last Review Date	22/09/2026

Strategic Policy

Contents

1. Policy Objective 3
2. Purpose 3
3. Scope 3
4. Definitions 3
5. Policy Statement 3
6. Approval Requirements 4
7. Minimum Security Requirements 4
8. Access to Council Information 4
9. Acceptable Use 4
10. Support and Costs 5
11. Loss, Theft or Security Incident 5
12. Privacy and Monitoring 5
13. Removal of Access 5
14. Breach of Policy Exemptions 5
15. Related Policies and Documents 5
16. User Acknowledgement 6

1. Policy Objective

To provide clear requirements for the approved use of personally owned devices when accessing Blayney Shire Council systems and information, while protecting Council data, maintaining cyber security controls and supporting efficient work practices.

2. Purpose

Blayney Shire Council recognises that personally owned devices can support flexible, timely and efficient communication. This policy sets the conditions under which a personally owned device may access Council email, calendars, contacts, applications, systems or information. It ensures users understand their responsibilities for protecting Council information, complying with Council requirements and reporting any loss, theft or suspected compromise.

3. Scope

This policy applies to Councillors, employees, contractors, consultants, volunteers, temporary staff and other authorised users who request or are granted access to Council systems from a personally owned device. Covered devices include mobile phones, smartphones, tablets, laptops, personal computers and any other personally owned device capable of storing information or connecting to Council systems.

4. Definitions

Term	Meaning
BYOD	Bring Your Own Device: a personally owned device used to access Council systems, information, services or applications.
Council information	Information created, received, accessed, stored or transmitted in the course of Council business.
Mobile Device Management	Council-approved controls used to manage access, protect information, apply security settings, remotely lock a device or remove Council information where required.
User	Any person authorised to access Council systems, applications, services or information.

5. Policy Statement

BYOD access is a privilege, not an entitlement. A personally owned device may only access Council systems where there is an authorised business requirement, approval has been granted and the device complies with Council security requirements. Council may deny, restrict, suspend or revoke access where a device, user or arrangement presents an unacceptable risk.

6. Approval Requirements

- BYOD access must be approved by the Manager Information Technology or a delegated officer before connection to Council systems.
- Access must be limited to the systems, applications and information required for Council business.
- The user must acknowledge this policy before access is enabled.
- Re-approval may be required when the device, role or business need changes.

7. Minimum Security Requirements

- The device must use a supported operating system and current security updates.
- The device must be protected by a passcode, password, biometric control or another Council-approved authentication method.
- Multi-factor authentication, encryption and automatic locking must be enabled where required or available.
- The device must not be jailbroken, rooted or modified to bypass security controls.
- Council approved mobile device management, application protection, conditional access and security controls must not be removed, disabled or bypassed.
- Council may block devices that no longer meet security requirements.

8. Access to Council Information

- Council information must only be accessed through Council approved systems and applications.
- Council information must not be intentionally stored outside approved Council systems unless authorised.
- Council records must be captured and stored in approved Council recordkeeping systems.
- Users must prevent unauthorised people from viewing or accessing Council information, including when devices are used in public places.
- Unapproved cloud services, messaging applications, removable media and artificial intelligence services must not be used to store or process Council information.

9. Acceptable Use

- Users must act lawfully, ethically and professionally and comply with Council policies, employment obligations and relevant legislation.
- Council credentials and authentication factors must not be shared.
- Users must not circumvent security controls or install applications that compromise Council systems or information.
- Council systems must not be used to access, store, transmit or distribute unlawful, inappropriate or unauthorised material.
- Users must follow all Council directions concerning device security and access.

10. Support and Costs

Council IT support for BYOD devices is limited to Council approved connectivity, authentication and access to Council systems. Unless expressly approved in writing, Council is not responsible for personal hardware, software, data recovery, telecommunications charges, warranties, repairs or performance issues.

11. Loss, Theft or Security Incident

Users must immediately report a lost or stolen device, suspected unauthorised access, malware infection, accidental disclosure or other security incident to the IT Department. Council may disable access, require credential changes, remotely lock a supported device, remove Council information or direct other protective action

12. Privacy and Monitoring

Council respects personal privacy; however, activity involving Council systems, accounts, applications and information may be logged, monitored, audited or investigated in accordance with Council policy and applicable legislation. Council security controls will be used for Council business, information protection and cyber security purposes. Users should maintain personal backups because Council is not responsible for personal data loss resulting from authorised security action.

13. Removal of Access

BYOD access must be removed when employment, engagement or authorised access ends, the business requirement ceases, the device no longer meets security requirements or Council directs removal. Council information must be transferred to approved systems or removed as directed, and users must cooperate in confirming that Council information is secured or deleted.

14. Breach of Policy Exemptions

Failure to comply may result in removal of BYOD access, investigation, disciplinary action and/or referral to relevant authorities. Any exemption must be approved in writing by the General Manager or delegated officer and may be time-limited or subject to additional controls.

15. Related Policies and Documents

- 01D Code of Conduct for Staff
- 01B Code of Conduct for Councillors
- 07S Mobile Device Usage Policy
- 08A Email and Internet Policy
- 08C Information Technology Security Access Policy
- 11B Records Management Policy

16. User Acknowledgement

Users approved for BYOD access must acknowledge that they have read, understood and agree to comply with this policy before access is enabled.

End of Policy

	Date	Minute
Adopted:	**22/09/2026**	**2609/013**
Last Reviewed:		
Next Review:	**27/08/2030**	