



Mobile Device Usage Policy

Policy	7S
Officer Responsible	Manager Information Technology
Last Review Date	23/06/2025

Strategic Policy

Objective

Provide parameters for the use of corporate Mobile Devices used for access to Blayney Shire Council's corporate systems such as email/calendars, internet browsing and mobile applications used for Council related business.

Purpose

To provide Councillors and staff, referred hereon as "Users", with guidelines regarding the appropriate use of their Council supplied mobile device.

To provide users with mobile devices for use and to assist them in the performance of their duties.

To ensure that users are accessible, facilitate timeliness of responses to Council's customers and to enhance communications.

To facilitate the effective management and administration of costs of business calls relating to the Council's mobile device resources.

To encourage the standard for acceptable use of mobile device resources in the conduct of its business to safeguard users, protect Council assets and ensure compliance with appropriate legislation.

Definition

A "Mobile Device" for the purposes of this policy will be any device that is reliant on a carrier Mobile Network for the purpose of transmission of voice and/or data traffic. Mobile Devices include but shall not be limited to: Mobile Phones, Smart Phones, Laptops and Tablet devices.

Eligibility

A user will be eligible to have a mobile device if it is deemed necessary to their position, for example, if the employee's duties require them to spend time out of the office and/or to be contactable outside the normal hours of work. All mobile devices are provided at the discretion of the department director or General Manager or in the case of Councillors, the Payment of Expenses and Provision of Facilities policy. Any current employee who requires a replacement mobile device will need to fill in the Mobile Device Application Form on Council's Intranet and then forwarded to their manager and director for approval.

Use

While mobile devices are approved on the basis of business benefits and usage, reasonable personal use of devices is acceptable, but users must adhere to the following usage terms:

- The conditions of the Email and Internet Policy must be adhered to.
- The conditions of the Blayney Shire Council's Code of Conduct policy must be adhered to.
- The private usage of devices during business hours must not interfere with the employee's work performance or detract from the employee doing their normal duties.

- Monthly usage details will be accessible to the Manager Information Technology (IT) and Chief Financial Officer for cost management: IT is entitled to query excessive usage costs for mobile devices.
- Loss or theft of the mobile device must be immediately reported to IT. A loan device (if available) will be issued until a permanent replacement is organized. An incident form must also be completed and given to the WHS and Risk Coordinator
- Information stored on the mobile device is not backed up by Council systems, it is the responsibility of the user to backup personal data and to ensure that Council information is stored on Council approved systems for security and backup. Council takes no responsibility for the loss of personal data.
- All mobile devices come data plan deemed appropriate for its usage plan.

Private Use

The approved user is permitted incidental private usage of the mobile device so long it does not incur extra charges in which case the bill will be reviewed, and they will be issued an invoice for reimbursement. This would most likely occur if personal overseas usage has occurred.

Council receives fully itemised records for all mobile devices. Council recognises the users' general rights of privacy, but Council reserves the right to monitor use of mobile devices where it is reasonably justified and/or there are legitimate reasons for doing so. Where Council has concerns, this matter will be referred to the relevant Director or General Manager.

Mobile Devices are fitted with location tracking software and remote wipe/remote lock capability will be enabled. The disabling of such features by users may result in disciplinary action.

Hands Free Operation

The use of mobile devices, 'without hands free', whilst driving is unlawful and the incursion of any penalties and fines will be solely at the user's cost.

Responsibility of Users

Users accept full responsibility for using their Council mobile device in an honest, ethical, safe and legal manner and with regard to the rights and sensitivities of other people. Use must be in accordance with Council policies and all relevant federal and state legislation.

Staff are required to:

- Take good care of the mobile device
- Take all reasonable precautions to ensure that the device is not damaged, lost or stolen. Keep mobile devices clean, and in a serviceable condition to the best of their ability, and
- Report all irregularities or faults/damage of the mobile device immediately to the IT Department.

There are some standard procedures that the user should implement as part of their day-to-day operational use of the mobile device:

- Activate the keypad lock to avoid accidental use of the device
- Mobile devices must not be left in open view in unlocked or unattended vehicles.
- Damaged devices should be returned to the IT Department who will arrange for any repairs to be carried out.

Lost or Stolen Devices

- Any devices that are lost or stolen: Must be reported to the IT Department immediately after discovering the loss of the mobile device (business hours) or first thing the next business day if discovered after hours
- Will be remotely locked and wiped clean of all data if the device can be tracked.
- Must have an Incident Report completed and provided to WHS and Risk Coordinator

Subject to the circumstances in which the mobile device was lost or damaged, Council will be responsible for replacing the device unless carelessness on the part of the user can be shown as the cause of the loss or damage. In circumstances where it has been shown that the user's carelessness contributed to the loss or damage of the device then the user may be required to contribute to the replacement cost.

Installation of Applications on Mobile Devices

Council currently has accounts for mobile applications devices. IT currently holds the passwords for these accounts. If the user of mobile device requires an application to be installed on the device, it must be undertaken by IT and be for business purposes. Justification must also be provided in an email to the IT Manager why the application is required. If the application will incur a cost, then this will be discussed with the user's Director.

Under Cyber Security NSW guidelines TikTok and Deepseek applications must not be installed or used on any Council device.

Council staff are permitted to login to the Mobile devices with personal app accounts but Council will not be responsible for any charges incurred or if the device becomes faulty and needs to be reset or replaced.

Councillors have personal iTunes accounts linked to their Ipad and Council email accounts and are responsible for the upkeep of those accounts Councillors will be provided with a Data plan for their Ipad or laptop device.

Termination of Employment / Conclusion of Term/Change of Position

On termination of employment or conclusion of term of Council (resignation or where not re-elected), the user must return the mobile device to IT including any associated battery chargers or other accessories supplied by the Council for use with the mobile device.

If an employee subsequently changes job position within Council, authorisation by the relevant Director must occur for the mobile device to remain with the employee. Approval will only be given in this circumstance where the use of the mobile device is deemed a necessary requirement of the employee's new job position. If approval is not given the mobile device is to be returned to IT.

Related Policies

Council Code of Conduct
Records Management

Legislative Context

Local Government Act 1993
Local Government (General) Regulations 2021
Workplace Surveillance Act 2005
Workplace Surveillance Regulation 2012

Adopted:	Date: 08/12/2014	1412/006
Lasted Reviewed:	08/12/2014	1412/006
	16/04/2018	1804/010
	21/11/2022	2211/010
	23/06/2025	2506/012
Next Reviewed:	28/09/2029	