Mobile Communication Device Policy

Section 1 - Key Information

Policy Type and Approval Body	Administrative – Vice-Chancellor
Accountable Executive – Policy	Chief Information Officer
Responsible Manager – Policy	Senior Manager, Security, Risk and Compliance
Review Date	28 May 2027

Section 2 - Purpose

(1) The purpose of this Policy is to provide guidelines and regulations for the appropriate use of the mobile devices provided by La Trobe University. Mobile Devices include but not limited to smartphones, tablets, laptops, and wearable devices.

Section 3 - Scope

(2) Applies to:

a. all campuses;
b. all staff, students, contractors, visitors, and external affiliates.

(3) This Policy excludes certain fixed devices and specialised communication equipment within the University premises. Excluded devices include, but are not limited to:

a. Fixed Devices: This Policy does not apply to fixed communication devices such as lift phones, emergency call boxes, and stationary telephones located within the University buildings.
b. IoT (Internet of Things) Devices: IoT devices, including sensors, smart appliances, and other interconnected devices, are not governed by this Policy unless they are explicitly used for mobile communication purposes.
c. Emergency Phones: Dedicated emergency phones installed throughout the University for immediate access to emergency services are excluded from the scope of this Policy. These phones serve specific emergency communication functions and operate independently of personal mobile devices.

(4) Whilst the aforementioned devices are exempt from the Procedures outlined in this Policy, users are expected to use them responsibly and in accordance with their intended purposes.

Section 4 - Key Decisions

Key Decisions	Role
Authorise mobile, data and/or telephony plans with any carrier on behalf of the University	Chief Information Officer
Approve the purchase of mobile communication devices within their area	Budgetary Heads

Section 5 - Policy Statement

(5) The University recognises the importance of mobile communication devices in facilitating academic, administrative, and personal communication within the campus community. This Policy aims to establish procedures and expectations for the responsible use of mobile devices to ensure the integrity, security, and productivity of University operations.

(6) Users are expected to adhere to the following principles:

a. Responsible Use: Mobile devices should be utilised in a manner that respects the rights and privacy of others and does not disrupt the educational or work environment.
b. Data Security: Users must take appropriate measures to safeguard University data accessed or stored on their mobile devices, ensuring compliance with security protocols and best practices.
c. Network Connectivity: Mobile devices should be connected to the University's wireless network in accordance with established network security policies and procedures.
d. Prohibited Activities: Certain activities, such as harassment, unauthorised access to data, or engagement in illegal or inappropriate content, are strictly prohibited on mobile devices within University premises.
e. Emergency Preparedness: In emergency situations, users should utilise mobile devices responsibly to communicate with emergency services or University authorities, refraining from spreading misinformation or panic.
f. Compliance and Enforcement: Violations of this policy may result in disciplinary action in accordance with University regulations. The University reserves the right to inspect or confiscate mobile devices suspected of misuse.

(7) Through adherence to this Policy, the University seeks to foster a culture of responsible mobile communication that enhances collaboration, productivity, and safety within the campus community.

Section 6 - Procedures

Part A - General

(8) General procedures cover the acquisition, allocation, usage, and management of mobile communication devices and services. Users must comply with the Procurement Policy and Procedure, and a comprehensive list of approved mobile communication devices which can be found at Service Catalogue - Mobile Communication Devices. This list is updated periodically by the Information Services (IS) Executive to ensure it remains current.

Part B - Purchase of Mobile Communication Devices & Services

Procurement process

(9) The acquisition of mobile communication devices and services shall adhere to the University's Procurement Policy and Procedure.

(10) Unless specifically authorised in writing by the Chief Information Officer (CIO), users are not permitted to enter into any mobile, data and/or telephony plan with any carrier on behalf of the University, regardless of funding source or device ownership. There should be no plans entered into on behalf of the University independent of IS, whether on University or privately-owned phones. Unauthorised plans will be cancelled, and the carrier may be advised to recover costs from the user responsible for entering into the plan.

(11) The following applies to the procurement of University owned mobile communication devices:

a. all new and replacement mobile communication devices must be requisitioned through the Service Catalogue - Mobile Communication Devices;
b. the University will determine which carrier it purchases SIM-enabled mobile services from;
c. the University reserves the right to change carriers;
d. the University will determine the suppliers of the SIM enabled mobile communication devices;
e. the University will determine the approved standard mobile communication devices to meet the defined business requirements, accounting for coverage;
f. independent purchases of mobile communication devices will not be reimbursed by the University and University Purchasing Cards must not be used for such purchases; and
g. all contracts for calls, text and data should be entered into through IS under this contract.

(12) Budgetary heads are responsible for approving the purchase of mobile communication devices within their area.

(13) Any non-standard device request for mobile communication devices must be approved by both a member of the Senior Executive Group (SEG) and the budget holder to ensure the business requirements cannot be met with the standard device.

Part C - Eligibility Criteria for Mobile Communication Devices & Services

(14) Staff members may receive a University-owned mobile communication device based on demonstrated business necessity or contractual agreement.

(15) Requests for non-standard devices must be approved, and eligibility criteria for tablet devices are outlined.

(16) Staff are restricted to having one data carrier (SIM) per person. Requests for exceptions to this must be approved in writing by the relevant budget holder.

(17) Requests for tablet devices are required to include a justification in the ASK Services request that is endorsed by the Line Manager and relevant budget holder.

(18) Staff are only eligible for an iPad/Tablet where:

a. Information Services is satisfied there is a legitimate, demonstrated business need (specifying either WIFI or Cellular connection) that cannot be met by the staff member’s computing device.
b. Information Services is satisfied there is a legitimate, demonstrated research need (specifying either Wi-Fi___33 or Cellular connection).

(19) This can include but is not limited to:

a. a need for the staff member to always be easily contactable;
b. a need for the staff member to be available outside business hours to assist with critical business functions;
c. the staff member being required to make frequent and/or prolonged travel outside the campus locations;

d. the role requires the incumbent to work across multiple locations/sites but remain contactable;
e. a need for staff to work in location where there is limited access to a fixed phone (e.g. outdoor staff);
f. a need for staff to perform a specific security or OH&S function;
g. a need for staff to be easily contactable by customers or external organisations; and
h. the staff member being required to use these devices to provide support for the University community.

(20) A staff member transferring to a different position within the University may be required to return the mobile communication device and have the associated phone number re-assigned to another staff member.

Part D - Schools and Divisions

(21) There are occasions where a mobile communication device will be allocated to a School or Division (or other Business Unit) rather than an individual, for example:

a. locked iPads for use exclusively on Open Days/events;
b. a requirement to be on an on-call roster;
c. the business function uses telemetry equipment;
d. excursions and field trips;
e. the business function has a need to use these devices to provide support for the University community;
f. temporary use by a University visitor (including honorary and adjunct academics).

(22) A specific member of staff must be nominated by the budgetary head to take responsibility for the allocated device and to oversee its use. It is incumbent on the responsible nominated staff member to maintain an accurate written record of the devices allocated to the work area, and who they have been allocated to, always, and to present this upon request to IS.

Part E - Responsibilities

Responsibilities of Line Managers

(23) The Line Manager has the following supervisory responsibilities:

a. assess which positions in their area need a mobile communication device;
b. ensure users understand and observe the appropriate Statutes, Policies and Procedures;
c. ensure devices are only obtained through approved channels, i.e. Service Catalogue - Mobile Communication Devices;
d. ensure users are aware of the need to arrange access to global roaming (voice and/or data) with IS via ASK Services for their device if they are travelling overseas on official University business for the period the user is away.This must be requested through ASK Services and approved at least 5 days in advance;
e. approve the use of global roaming (voice and/or data) for official overseas travel and ensure the appropriate roaming packs have been applied. Note: global roaming will be automatically disabled outside of the approved period;
f. approve the use of international calling and ensure appropriate calling packs have been applied;
g. assess and authorise requests from users to take a University owned mobile communication device with them while on planned personal leave beyond three months if there is a demonstrated business need. Advise the user on the need to make alternative arrangements for voice and data services while overseas;
h. request IS (via ASK Services) cancel accounts for unused mobile communication devices and return the unused devices and SIM to IS;
i. make users aware that mobile communication device usage will be monitored and that they may be required to

justify their use;

j. on receipt of the periodic account monitor the usage of the device;
k. request users to identify any personal use of the device and may request the user to reimburse the University for the cost associated with personal use.

Responsibilities of Users

(24) Mobile communication devices owned by the University are to be used appropriately, responsibly and ethically.

(25) Users are responsible for all activities associated with the device. The use of these devices is subject to the Use of Computer Facilities Statute 2009. In addition, users of these devices must observe the following:

a. familiarise themselves with the Use of Computer Facilities Statute 2009 and this Policy;
b. ensure the use of device abides by the Statutes, Policies and Procedures of the University;
c. immediately report lost/stolen/broken mobile communication devices to IS via ASK Services;
d. familiarise themselves with operating the device; take time to read and understand the instructions and manuals provided, and seek clarification if required;
e. by default, your phone number will be automatically published in the University staff online directory once it has been ported to the La Trobe account or a new number is established. If you wish to hide your number from the directory, you will need to log a request with IS via ASK Services;
f. return the device and SIM to their line manager if the device is no longer required or upon request;
g. must take reasonable care of the device, maintain the device in good working order subject to reasonable wear and tear, and take all reasonable precautions to prevent loss, damage or theft. Any repairs or replacements will be funded by the department;
h. where necessary, arrange device repair via IS or IS's designated channels/suppliers as outlined in ASK Services;
i. University mobile communication devices must not be used to access premium services;
j. avoid incurring international roaming charges associated with voice and data usage, however, where there is a demonstrated need for international voice and/or data services, make appropriate arrangements with IS via ASK Services for global roaming (voice and/or data). By default, international roaming is disabled, and needs to be requested and approved at least 5 days prior to travel should this be required for business purposes;
k. must ensure important corporate data and information stored on the mobile communication device is backed up;
l. take all practicable steps to secure the mobile communication device and the information contained within the device;
m. if it is a requirement to take University owned mobile communication device while on planned personal leave beyond three months, the user must seek permission from the approving supervisor and make alternative arrangement for access to data and voice services if travelling overseas;
n. to prevent malware, avoid installing software from non-verified sources on University mobile communication device;
o. keep data cost at a minimum. Where available, users should access data on their mobile communication device via a secured wi-fi service.

Part F - Termination of Employment

(26) All University owned mobile communication devices and associated accessories including SIM card are to be returned to the line manager upon termination of relationship with the University.

(27) All equipment should be returned in good working order subject to reasonable wear and tear.

(28) The Line Manager is responsible for returning the device, SIM card and accessories to IS unless an alternative arrangement is made with IS by the budget head. Should the device not be returned to the University, or not returned in good working order, the University will take measures to recover the costs of the device. This could include legal action.

(29) If requested, the University may agree to transfer mobile phone numbers registered in its name to departing staff members where the staff member has had exclusive use of the number, providing the transfer takes effect within one month of the termination date. This does not apply where the mobile phone number was allocated to a business function or published in a corporate publication (excludes personal business cards). Payment of any costs associated with the transfer, such as a cancellation of contract fee is at the discretion of the budget head. Any such costs will be borne by the approving School or Division.

(30) The University will reallocate the number or cancel the service if the transfer is not in effect one month after the termination date.

(31) These conditions also apply to employees who move to a role which no longer sees them eligible for a mobile communication device.

Part G - Transfer of Mobile Device & Service

(32) When a mobile communication device is no longer required by an individual, the School or Division line manager must return the device to IS. Where appropriate, IS may reissue the device after ensuring it is in proper working order.

Part H - Broken or Unwanted Mobile Devices

(33) All broken or unwanted University mobile communication devices are to be returned to IS. These devices will be disposed of, repaired or reused appropriately. Any costs associated with improper device care will be passed onto the holder’s cost-centre.

(34) IS will manage the disposal or salvage of all Mobile Communication Devices at its discretion. This includes requests for individuals to purchase broken/unwanted devices to ensure that the device has been appropriately wiped/restored to factory settings and that fair market value for the used device is applied.

Part I - IS Initiated Service Termination and Device Revocation

(35) The University may, at its discretion, independently terminate services as part of its fleet management operations. Automatic termination may be initiated in situations including but not limited to:

a. SIM has not registered usage in at least four months;
b. SIM is registered as assigned to an employee whose employment was terminated.

(36) University management will regularly review mobile communication device usage and reserves the right to revoke approval for a University mobile communication device at any time.

Part J - Device Disposal, Refresh & Replacement

(37) The device is to be returned to IS Service Desk at end-of-life toe ensure it is appropriately wiped of corporate data and recycled.

(38) The replacement of a lost or damaged device is subject to approval by the relevant Line Manager. Replacements for lost or damaged devices may not be new or equivalent device and are at the discretion of IS.

(39) The University may choose to replace the mobile communication device for reasons of changing business requirement or technological changes.

(40) The standard device refresh period is 36 months with the cost of any replacement device needing to be funded by the users cost centre and approved by the budget holder for the cost centre.

Part K - Monitoring

(41) The University reserves the right to monitor usage of University owned mobile communication devices. All monitoring requests require appropriate business justification and written approval from the relevant Senior Executive Group member.

(42) The use of University owned mobile communication devices are subject to the conditions outlined in the Use of Computer Facilities Statute 2009, the Code of Conduct and include additional conditions as follows:

a. Line Manager(s) and/or relevant senior management are provided with regular summary usage report for the purpose of monitoring usage against this Policy;
b. where there is a suspicion of misuse, itemised bills will be made available to the direct Line Manager(s) and/or relevant senior executive;
c. the University will from time to time audit the records of a University issued mobile communication device to ensure compliance with this Policy and any specific budget guidelines as part of its regular audit cycle.

Part L - Security

(43) Mobile communication devices may contain confidential, personal and sensitive corporate information. The University will impose security requirements to protect the data. This includes steps outline in the Use of Computer Facilities Statute 2009.

(44) All University owned mobile communication devices will be centrally managed and accessed via a MDM. All devices must be configured with a password, PIN or biometric identification in order to gain access to the device.

(45) The University is entitled to implement settings to enable the remote wiping of the device at any time if there is a security issue with the device. Users are advised to ensure that any personal content on the device such as photographs and videos are backed up elsewhere.

Part M - Use of Personal Devices

(46) Users are permitted to use a personal mobile communication device to access the University's network and facilities.

(47) All such use is subject to the Use of Computer Facilities Statute 2009 and any other applicable policies and procedures.

Section 7 - Definitions

(48) For the purposes of this policy:

a. Compliance and Enforcement: Adherence to policy guidelines and consequences for violations, including disciplinary actions and device inspection or confiscation by University authorities.
b. Data Security: Measures taken to safeguard university data accessed or stored on mobile devices, ensuring compliance with security protocols and best practices.

c. Emergency Phones: Dedicated devices installed on University campuses for immediate access to emergency services, independent of personal mobile devices.

d. Emergency Preparedness: Responsible use of mobile devices during emergency situations to communicate with emergency services or University authorities, avoiding the spread of misinformation.

e. Fixed Devices: Communication equipment permanently installed within University premises, such as lift phones, emergency call boxes, and stationary telephones.

f. IoT (Internet of Things) Devices: Connected devices with sensors or smart capabilities, excluding those specifically used for mobile communication within the University context.

g. Line Manager: Direct supervisor responsible for overseeing the use of mobile communication devices by staff members within their department or unit.

h. Mobile Communication Device: Any handheld electronic device capable of sending or receiving calls, messages, or data, including but not limited to smartphones, tablets, laptops, and wearable devices, used for communication purposes within the university community.

i. Network Connectivity: Connection of mobile devices to the university's wireless network in accordance with established security policies and procedures.

j. Personal Devices: Private mobile communication devices owned by individuals, used to access university networks and facilities in accordance with policy guidelines.

k. Prohibited Activities: Actions such as harassment, unauthorised data access, or engagement in illegal or inappropriate content on university mobile devices.

l. Responsible Use: Utilisation of mobile devices in a manner that respects the rights and privacy of others and does not disrupt educational or work environment.

m. Senior Management: Higher-ranking university officials, including Vice-Chancellor, Deputy Vice-Chancellors, and Divisional Directors, responsible for overseeing policy implementation and enforcement.

n. Service Catalogue - Mobile Communication Devices: A centralised repository listing approved mobile devices available for acquisition and usage within the university, maintained by Information Services (IS) Executive.

o. SIM (Subscriber Identity Module): A memory card inserted into mobile devices to identify and authenticate users on the network, providing access to voice and data services.

p. University Premises: All physical locations owned or operated by the University, including campuses, buildings, facilities, and associated areas.

q. Use of Computer Facilities Statute 2009: University regulations governing the use of computer resources, including mobile devices, for academic, administrative, and personal purposes.

r. Wi-Fi Enabled Devices: Mobile devices capable of connecting to wireless networks for data transmission, including smartphones, tablets, laptops, and other portable gadgets.

Section 8 - Authority and Associated Information

(49) This Policy is made under the La Trobe University Act 2009.

Status and Details

Status	Current
Effective Date	28th May 2024
Review Date	28th May 2027
Approval Authority	Vice-Chancellor
Approval Date	28th May 2024
Expiry Date	Not Applicable
Responsible Manager - Policy	David Hird Senior Manager, Security, Risk and Compliance
Author	David Hird Senior Manager, Security, Risk and Compliance
Enquiries Contact	Information Services 03) 9479 1500

Glossary Terms and Definitions

"student" - Student is defined in the La Trobe University Act 2009 as: (a) a person enrolled at the University in a course leading to a degree or other award; or (b) a person who is designated as a student or is of a class of persons designated as students by the Council.

"staff" - Staff means any person employed by the University as per the definition in the La Trobe University Act 2009 (Vic).