Mobile Devices Policy

1. Purpose

Mobile Devices are important tools for UNSW College and their use is supported by the Company to achieve business goals. While the portability makes these devices useful, it may also introduce issues due to risks associated with inappropriate use and security of the information being transmitted and/or stored on these devices.

The purpose of this Policy is to:

(a) establish a management framework that governs the allocation and use of Mobile Devices and associated mobile service packages; and

(b) inform Employees of their obligations in relation to the proper use and care of Mobile Devices.

2. Scope

This Policy applies to all UNSW College Employees, (including full-time, part-time, casual employee and fixed term contractors) and their use of either personal or Company owned Mobile Devices to:

(a) attach to the UNSW and UNSW College network; or

(b) connect to UNSW College IT infrastructure; or

(c) store, display, or process UNSW College business data.

3. Policy statement

3.1. Provisioning

(a) The provision of a Company-owned Mobile Device and/or Company-funded Mobile Service to an Employee must be authorised by a Business Unit Manager.

(b) Whether or not an Employee is eligible to be issued with a Company funded Mobile Device and/or a Mobile Service is based on the responsibilities of the position and the requirement for such a device and/or service to enable the Employee to complete their duties, including, but not limited to Employees who are required to be:

i. on call after hours and/or when travelling
ii. away from their desks for a substantial amount of time
iii. contactable on an ad-hoc basis
iv. using Mobile Devices in a teaching and learning environment.

(c) Employees will only be issued with UNSW College-approved Mobile Devices. Please refer to the UNSW College Standard IT Equipment List for details of the approved list of Mobile Devices.

(d) All Mobile Devices, SIM cards and accessories purchased by UNSW College remain the property of the Company.

3.2. User Responsibilities

(a) All use of Mobile Devices, Company or personally owned, which utilise UNSW College network resources, will be subject to the provisions of the UNSW College Acceptable Use of ICT Resources Policy (Staff) and the IT Security Policy.

(b) UNSW College owned Mobile Devices are issued to Employees primarily for business use. Outgoing phone calls, email and web access should be limited to Company-related work. Limited personal use is acknowledged, however where personal Usage is deemed excessive, Employees may be required to reimburse the Company for costs incurred.

(c) The relevant Business Unit Manager is responsible for verifying and authorising invoices for payment associated with the purchase of Mobile Devices, accessories and ongoing call costs.

(d) Personally owned Mobile Devices are acceptable to use for accessing UNSW College network resources. If corporate data is synchronised to the Mobile Device, further conditions apply in accordance with the IT Security Policy (the section on Bring Your Own Device).

(e) UNSW records Usage and call details for Company owned Mobile Devices. Records may be accessed by authorised Employees for audit and investigation purposes, and may be subpoenaed as evidence.

(f) An Employee who wishes to port their private mobile number to the UNSW College account needs to obtain the approval of the relevant Business Unit Manager.

Employees must be aware that the Company may decide to retain the number based on criteria under 3.5(d) if/when they leave the Company.

3.3. International Roaming

(a) UNSW College data plans for mobile phones are national plans. International roaming is turned off by default on all Company-owned Mobile Devices and private numbers which are ported to the UNSW College account.

(b) Employees travelling overseas must seek the consent of their Business Unit Manager when requesting international roaming to be enabled on their Mobile Devices. Employees are responsible for ensuring that international roaming is enabled as required, prior to their departure. Any costs incurred because of failure to enable international roaming may be determined to be the sole responsibility of the Employee.

(c) International use of these data plans is an additional charge and is not included in the monthly download limit. Employees should use Wi-Fi to access the internet or email via their mobile network outside of Australia.

3.4. Security Guidelines

(a) It is the responsibility of any Employee who utilises the UNSW College network for the purpose of accessing or processing Company Sensitive Information using a Mobile Device to take appropriate measures at all times to safeguard that information, per the IT Security Policy.

(b) Storing Company owned Confidential Information and/or Sensitive Information in the cloud must be vetted by IT. Passwords, sensitive or proprietary information

may be stored on Mobile Devices if absolutely necessary, i.e. for justified academic or business need. Sensitive Information in the cloud must be encrypted.

(c) If Mobile Devices are used to temporarily store Company owned data, these must be moved to network drives (e.g.: X:, T:, M:, H: drives) within 24 hours of gaining access to the UNSW College network drives.

(d) If serious vulnerabilities are found on Company owned Mobile Devices, remote synchronising will be disabled and data on the Mobile Device may need to be wiped.

(e) Circumventing security on Company owned Mobile Devices is prohibited (i.e.: no alternate operating systems, no jailbreaking or unlocking of iPhones, no sideloading of custom or unverified applications outside of official App Store(s)).

(f) Privately owned Mobile Devices which have been jailbroken will not be allowed to synchronize with the Global email system.

(g) The physical security of a Company owned Mobile Device is the sole responsibility of the Employee. Employees must take all reasonable precautions to safeguard their Company owned Mobile Devices and should be aware that UNSW College does not have insurance for Company owned Mobile Devices.

(h) If a Company-owned Mobile Device is lost or stolen the content will be wiped remotely by UNSW College IT. The information that will be wiped may include all content such as photos, videos and files stored on the Company-owned Mobile Device. The Employee's password for their UNSW College computer network account will also be reset as a security precaution.

(i) Immediately report any damage, loss or theft of Company owned Mobile Devices to the UNSW College IT Helpdesk, and contact the Mobile Carrier to inform them of the same (see 3.4 (j) below)

(j) At the date of this Policy the Mobile Carrier for UNSW College is Optus. Employees should immediately contact Optus on 13 39 37 (or +61 2 8082 5678 if you are overseas) if the theft/loss occurs outside of business hours.

(k) Replacing lost Company owned Mobile Devices must be approved by the relevant Business Unit Manager.

(l) UNSW College IT will enforce device encryption and enforce a PIN on Company managed mobile devices, via a Device Management Profile which must be accepted to enable access to Company data and systems.

3.5. Ending Employment

(a) All Company owned Mobile Devices, SIM cards and accessories must be returned on termination of employment or expiration of the contract with the Company. If a Company owned Mobile Device is not returned the Employee will be charged the cost of its replacement, the SIM card will be cancelled and the device will be locked, rendering the device useless.

(b) Any outstanding excessive phone bills must be paid for by the Employee when they leave the Company.

(c) An Employee who wishes to take the mobile phone number when they leave the Company must obtain approval from their relevant Business Unit Manager. This

applies to both Company issued mobile numbers and mobile numbers that have been transferred from private accounts to the UNSW College account. Assessment and approval will be made on a case by case basis by each Business Unit.

(d) Under the following circumstances, Employees will not be allowed to take the mobile number with them:

a. where the mobile number is an advertised contact number; and/or

b. where it is not in the interest of UNSW College to release the mobile number.

3.6. Workplace Health & Safety

(a) Employees must ensure that their use of Mobile Devices is in accordance with NSW and Commonwealth Government legislation (e.g. The Motor Traffic Act). UNSW College is not liable for any offences committed by an Employee when using a Mobile Device in breach of this legislation.

(b) Employees many incur fines and loss of demerit points if caught using mobile phones whilst driving. It is the sole and personal responsibility of the Employee to pay these fines. Please refer to the Service NSW website for further information.

3.7. Breach of this Policy

Failure to comply with this Policy may result in:

(a) the suspension of any or all rights to use Company owned Mobile Devices and other IT resources; and/or

(b) disciplinary action in accordance with the Managing Unsatisfactory Performance and Conduct Procedure.

4. Roles, responsibilities and delegations

Role	Responsibility
Chief Executive Officer	Approver of this Policy
Head of IT	Implementation, dissemination, and review of this Policy.
IT Helpdesk Team Leader	Day-to-day implementation of this policy and is the first point of contact for all enquiries that relate to this Policy.
Compliance Manager	Administration and publishing of this Policy.
UNSW College Staff	Assisting in the implementation of and adherence to this Policy.

5. Definitions

Definitions and Acronyms	
Business Unit	means any organisational unit of UNSW College. Without limiting any business units or divisions that may be formed from time to time, these include the following business units: (a) Academic; (b) Students; (c) Finance; (d) Human Resources; (e) Information Technology; (f) Legal & Compliance; and (g) Sales & Marketing.
Business Unit Manager	means a manager responsible for the relevant Business Unit's budget that will fund the purchase and any on-going costs of a Mobile Device.
Confidential Information	includes, but is not limited to, any trade or business secrets, customer or client details and lists, supplier details and lists, the identity and source of the Employer's suppliers, pricing information, marketing information, strategic information, financial information, or any other information that you know or reasonably know to be confidential or sensitive to the business of the Employer.
Cloud Storage	means a model of networked online storage where data is stored in virtualised storage pools generally hosted by third parties and in locations not owned by UNSW College.
Employee	means an employee of UNSW College or UNSW employed on a permanent, casual or fixed-term basis.
International Roaming	means the ability to use a mobile phone on another mobile network overseas while still being billed by an Australian mobile service provider.
Jailbreaking	means the process of removing the limitations on devices, running the iOS and Android operating systems. Jailbreaking permits root access to the operating system, allowing the download of additional applications, extensions and themes that are unavailable through the official Apple Store or Android Play Store. For the purpose of this Policy, this term is used to refer to any unsanctioned operating system changes made to a Mobile Device.
Mobile Device	means laptop computers, Tablet Devices, smartphones and other such devices which have functions such as email, web browsing, and file editing as well as traditional mobile phone facilities. Examples include, but are not limited to: iPhones, Android based devices, iPads, Microsoft Surface Pro tablets and laptop computers.

Mobile Carrier	means a service provider that supplies connectivity services to mobile phones and Tablet Devices.
Mobile Service	means a Mobile Device plan which may include, without limitation, voice and data services, delivered by a Mobile Carrier which is paid for by UNSW College
Remote Wipe	means a security feature that renders the data stored on a device permanently inaccessible. Wiping may be performed locally or remotely by a network administrator.
PIN	means Personal Identification Number, which is a secret code used as a security feature that prevents other people from using your device, without also knowing this code.
Sensitive information	has the meaning given to it in the Privacy Act 1988 (Cth) from time to time. As at the effective date of this Policy, it is defined to mean: (a) information or an opinion about an individual's: i. racial or ethnic origin; or ii. political opinions; or iii. membership of a political association; or iv. religious beliefs or affiliations; or v. philosophical beliefs; or vi. membership of a professional or trade association; or vii. membership of a trade union; or viii. sexual orientation or practices; or ix. criminal record; that is also Personal Information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
Tablet Device	means a portable computer that uses a touchscreen as its primary input device.
Usage	means making calls, sending messages, transferring data, and performing other services via a Mobile Device and mobile service package or other network services.

Related Policy Documents and Supporting Documents	
Legislation	N/A
Policy	• Acceptable Use of ICT Resources Policy (Staff) • IT Security Policy
Procedures	Managing Unsatisfactory Performance and Conduct Procedure
Forms	N/A

Policy Governance

Mobile Devices Policy	
Category/Business Group	Information Technology
Published Externally (Yes/No)	Yes
Approver	Chief Executive Officer
Responsible Officer	Chief of Staff
Contact Officer	Head of Information Technology
Effective Date	17/08/2023
Next Review Date	17/08/2026
Version	3.0

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
3.0	Sarah Lightfoot, CEO	11 August 2023	17 August 2023	Updated as per feedback from the 2022 cyber security audit, including: · • clause 4 - adding a definition of PIN • Clause 5.1 - adding the words 'Company owned' and 'Company funded' • Clause 5.3(b) – clarifying the responsibility for ensuring international roaming is switched on • Clause 5.4(e) – adding that sideloading of unverified applications is prohibited • Clause 5.4(l) added

				• Clause 5.6(a) – adding that UNSW College is not liable for any offences committed by an Employee • updating hyperlinks; • administrative updates. • Updated all references to 'UNSW Global' to 'UNSW College', following rebranding in May 2023 • Cosmetic changes applied across the document to ensure consistency with other policies
2.0	Rob Farage, CEO	08/12/2017	08/12/2017	N/A

Please visit our website to ensure that you have the latest version of this Policy. Policies are available at: unswcollege.edu.au/about/policies