POLICY NUMBER: 01

Mobile Device and Service Policy

Prepared by	IT Services Division
Approving Authority:	FNU Council
Date Approved:	May 2013
Date Revised:	11 July 2022
Date Approved:	01 October 2022
Next Review:	01 April 2025
Version Number:	2.0

1. Purpose

1.1 The Fiji National University (FNU) is committed to providing Information and Communication Technology (ICT) resources to support, enable and enhance its activities. This includes the provision of a mobile phone, a data enabled mobile device (pocket Wi-Fi) or a data allowance to staff to facilitate official communications.

1.2 This policy governs the provision, and use of FNU-issued mobile devices and the responsibility of its users. It is adjunct to the Acceptable use of FNU ICT Resources Policy.

2. Policy Scope

2.1 This policy applies to all FNU staff who use mobile devices and services owned by the University.

2.2 Mobile devices refer to all FNU issued mobile phones and mobile internet broadband devices that provide voice and data services.

2.3 This policy should be read in conjunction with the Code of Conduct Policy.

3. Policy Principles

3.1 The following roles meet the criteria for the allocation of a University provided mobile phone:

3.1.1 Senior Leadership Team – the Vice-Chancellor and members of the Senior Leadership Team (SLT).

3.1.2 Incident management – staff who play a key role in managing key hazards and risks on and off the campus and should be available after hours (24 x 7) and where a mobile phone is required to ensure they are mitigating against key hazards that could affect staff, students and the FNU community. Staff issued a mobile phone are required to be always available in order to adequately support the performance of their critical services to the University.

3.1.3 Research – Under this scenario a device/service should not belong to a particular individual for use outside of that research purpose. Staff who would like to purchase phone hardware and data services under an external fund may do so with approval from the Dean of the College. The purchasing should however fall within the conditions of the grant.

3.2 Mobile phone models will be standardised for the roles in 3.1.1 and 3.1.2.

3.3 The provision of a mobile device for incident management roles must firstly be endorsed by the respective Dean or Director before it is approved by the Director IT Services whose budget will fund its purchase and on-going costs.

3.4 Support for work from home (WFH) – In exceptional circumstances and only after approval from their respective Dean or Director (budget holder), staff may be provided a data allowance to enable WFH for an extended duration.

3.5 When travelling overseas on official business:

3.5.1 Subject to 3.5.2 below, staff may purchase a pre-paid SIM from that country and replace it with the locally-issued one when they arrive in Fiji.

3.5.2 Purchase and use of SIM card when in China is not permitted.

3.5.3 Data roaming and international phone calls (i.e. use of FNU issued SIM overseas) is not permitted and would not be reimbursed.

3.5.4 Staff may use calling and messaging applications such as Viber and Microsoft Teams to stay in contact.

3.6 Members of the University allocated a mobile phone or hand-held device are responsible for its proper use, care, maintenance and safekeeping. Negligence in this matter may result in the recovery of costs from the individual member concerned.

3.7 For any misuse of the mobile service, the user will be required to pay for all related charges.

3.8 To ensure mobile phone security and to avoid any unauthorized access, the device must have password/ pin set to restrict access to the approved device holder only. The mobile phone will be secured with a University-supplied security application to prevent data loss and leakage in case of theft and loss of phone.

3.9 All staff provided a mobile phone, shall have their phone numbers recorded on the University email address list

3.10 When a user no longer requires, is no longer eligible for a mobile device or leaves the university then the device and related accessories must be returned to the Division of ITS.

4. Monitoring usage

4.1 FNU employs various measures to protect the security and privacy of its users' ICT accounts and ICT resources. This includes backup, logging of activity and monitoring of general usage trends and patterns.

4.2 In addition, FNU may monitor individual usage and records in accordance with this Policy.

4.3 FNU reserves the right to examine and access all data on its ICT resources to ensure that any use of its ICT resources complies with the law and any relevant policies and procedures.

5. Misuse

5.1 All users must comply with the conditions of use set out in this policy. If any user breaches the conditions of use in the Policy, the University may take disciplinary action. In serious cases, this may include termination of employment or expulsion from the University.