Mobile Device and Service Policy

1 Purpose

To establish the management framework that governs the allocation and use of Mobile Devices and associated Mobile Services Packages (hereafter referred to as Services) within the University including the:

- eligibility and approval process for the allocation, revocation and disposal of Mobile Devices and Services
- enunciation of the responsibilities of users and management including the process for monitoring Mobile Device Usage costs and Services
- provision of guidance for the acceptable Usage of Mobile Devices and Services.

2 Scope

This policy applies to all University Members who use any Mobile Devices and Services owned by the University.

3 Policy Statement

The University establishes the management framework that will apply to the allocation and monitoring of Mobile Devices and associated Services that it funds. The University is committed to the Acceptable Use of ICT Resources and is required to demonstrate that Mobile Devices and Services are only allocated to University Members with the primary purpose of conducting University business. Acceptable use will vary depending on the role of the individual, and/or the business function performed for which a Mobile Device and Service have been provided. Regular monitoring and oversight of Mobile Device and Service Usage will occur to assure acceptable and appropriate use and that Usage charges are within these acceptable bounds.

4 Principles

The following principles will apply:

1. The provision of a Mobile Device and Service must be authorised by an Approving Officer with responsibility for the Division and/or Department funding that will fund the purchase and any on-going costs.

2. The provision of and on-going commitment to fund the costs associated with the issuance of a Mobile Device and Service will be based on a demonstrated University business need and associated with a staff member's position or the performance of a University business function.

3. The Divisional Head will be the final arbiter in respect to matters arising from Principle 1 and 2.

4. Where a Mobile Device and Service is allocated to enable performance of a University business function, the Mobile Device will be allocated to a nominated staff member within the business unit who will be responsible for ensuring appropriate use of the Mobile Device and associated Services.

5. Mobile Devices that have been upgraded to a new model or replaced must be returned to ICT Services for reassignment or disposal.

6. Individual users of Mobile Devices and Services are required to comply with the requirements of the University Policy for the Acceptable Use of ICT Resources together with the Code of Conduct and Acceptable Use Guidelines outlined in the Procedure for Mobile Device and Service. Limited personal use is acknowledged, however re-imbursement of costs incurred may be required where personal use is deemed excessive.

7. Individual users acknowledge that where Restricted Information and Personal Information are stored on Mobile Devices, they shall implement measures to prevent unauthorised access to this information such as data encryption. ICT Services will provide guidance on security measures that should be considered.

8. The Approving Officer is responsible for taking reasonable steps to ensure that the Mobile Device and any Service are returned by staff members to whom these have been allocated:
    a. upon cessation of employment in the designated role and/or business unit

    b. when taking a period of Extended Leave of a personal nature.

9. The Approving Officer will ensure that the Mobile Device allocated to a staff member travelling overseas is connected to an appropriate overseas data plan for the duration of the overseas travel.

10. The Chief Information Officer is responsible for:
    a. Managing and reviewing contracts associated with the provision of Mobile Device carrier services, equipment, data plans and packages to ensure that value for money is achieved.

    b. Approving the connection of Mobile Devices, including BYOD, to the University carrier service and specifying the security requirements and settings that will

apply.

c. Coordinating the disposal of Mobile Devices.

d. Monitoring and reporting Usage against data plans to Approving Officers when data plan Usage is likely to exceed the standard plan quota.

e. Distributing Mobile Device and Service Usage accounts to the Approving Officer to enable Usage monitoring consistent with this policy.

11. The Mobile Device always remains the property of the University unless otherwise agreed. Approval to transfer a University Mobile Device number must be authorised by the Chief Information Officer.

5 References

Nil.

6 Schedules

This policy must be read in conjunction with its subordinate schedules as provided in the table below.

7 Policy Information

Accountable Officer	Chief Information Officer
Responsible Officer	Chief Information Officer
Policy Type	Executive Policy
Policy Suite	Mobile Device and Service Procedure
Subordinate Schedules	
Approved Date	20/10/2017
Effective Date	20/10/2017
Review Date	17/10/2028
Relevant Legislation	
Policy Exceptions	Policy Exceptions Register
Related Policies	Acceptable use of ICT Resources Policy

	Assets Policy Code of Conduct Policy Handling Personal Student Information Policy and Procedure ICT Information Management and Security Policy Intangible Assets Policy Portable and Attractive Items Policy Privacy Policy
Related Procedures	Assets Procedure Intangible Assets Procedure Motor Vehicles and Travel Fatigue Procedure
Related forms, publications and websites	Asset/PAI Disposal Request Form
Definitions	**Terms defined in the Definitions Dictionary**
	Personal Information Is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Restricted Information Information should be classified as Restricted when the unauthorised disclosure, alteration, or destruction of that Information could cause a significant level of risk to the University or its affiliates. Restricted Information includes Information protected by the State or Commonwealth privacy regulations and Information protected by confidentiality agreements. The highest level of Security Controls should be applied. Access to Restricted Information must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job (e.g. need-to-know). Access to Restricted Information must be individually requested and then authorised in writing by the Information System Custodian. Restricted Information is highly sensitive and may have personal privacy considerations, or

may be restricted by law. In addition, the negative impact on the institution should this Information be incorrect, improperly disclosed, or not available when needed, is very high.

University Members

Persons who include: Employees of the University whose conditions of employment are covered by the UniSQ Enterprise Agreement whether full time or fractional, continuing, fixed-term or casual, including senior Employees whose conditions of employment are covered by a written agreement or contract with the University; members of the University Council and University Committees; visiting, honorary and adjunct appointees; volunteers who contribute to University activities or who act on behalf of the University; and individuals who are granted access to University facilities or who are engaged in providing services to the University, such as contractors or consultants, where applicable.

Definitions that relate to this policy only

Approving Officer

Financial Delegation and HR Delegation Category 4 or above

BYOD

Bring your own device

Extended Leave

More than six weeks leave.

Division and/or Department

Refers to an organisational unit or units of the University and includes all Divisions, all Schools, all Departments, all Projects, all Research Centres, Business Units and all sub sections or sub groups of these units.

Mobile Device

Any laptop or notebook computer, phone, Personal Digital Assistant (PDAs), iPad or tablet, or any emerging voice or data device that accesses a commercial mobile telecommunications service, that is provided to a University staff member and paid for by the University for the purposes of fulfilling individual or business unit work requirements.

Mobile Service Packages

	The Mobile Device carrier and Mobile Device charging plan. **Usage** All calls, messages, data transfers, and services that are attributable to a Mobile Device and Mobile Service Package.
Keywords	
Record No	13/799PL