Policy Title: Mobile Devices and University Subscribed Home Internet Services

Policy Owner: **Chief Information Officer**

Keywords: **mobile device, information security, information systems**

Policy Code: **PL271/it050**

1. INTENT

The purpose of this policy is to define accepted practices and responsibilities for the use of any Mobile Device that connects to the University's network and information systems and for the use of Subscribed Home Internet Services used for University business.

2. ORGANISATIONAL SCOPE

This policy applies to any individuals who access and/or use the University network from any type of Mobile Device.

3. DEFINITIONS

TERM	DEFINITION
University Owned Mobile Devices (UOMD)	Any Mobile Phone, Smartphone, tablet, laptop, or hybrid device issued by the University
Personally Owned Mobile Devices (POMD)	Any personally owned Mobile Phone, Smartphone, tablet, laptop, or hybrid device
Personally Subscribed Home Internet Services (PSHIS).	Internet services procured by a staff member primarily for personal use
Responsible Manager	School Dean or Service Centre Director or delegate with the authority and responsibility to expend and manage costs against the University's cost centre
Security Functions	Any capability of the device that increases the security posture of that device, e.g. PIN, Passwords, Biometric Access, inbuilt security features

University Subscribed Home Internet Services (USHIS).	Internet services provided to a staff member at a location other than their workplace, under the University provider contract

4. POLICY CONTENT

4.1 User Responsibilities

Open collaboration within and beyond the University is at the core of the University's academic purpose and will be supported and secured in the application of information security policies.

The University has significant investment in digital assets in the form of data, information and information systems that require appropriate handling and management. To this end, the University expects Mobile Device users to assume personal responsibility for any device that connects to the University network, contains University information, or accesses the University's technology systems. Users are responsible for the appropriate use of a USHIS.

4.2 Access to Information Systems

The University permits the individual use of Mobile Devices that access the University's network, technology systems and information and USHIS, subject to the following:

- Users accept all relevant Policies, Standards and Procedures as defined in Section 7;
- Users complete any required Fringe Benefits Tax declarations;
- The device software is kept updated, with PIN and/or biometric access controls active where available; and
- The University reserves the right to deny or disconnect access to the network or other services without prior notification.

For the purposes of enforcing this policy and to meet the University's legal and regulatory requirements, the University reserves the right to monitor Information Systems and technology usage and to examine any information gathered from that monitoring.

4.3 Damage, Loss or Theft

The University takes no responsibility for damaged, lost, or stolen Personally Owned Mobile Devices.

If a Mobile Device (POMD or UOMD) containing University data is lost or stolen, the loss or theft must be reported to the IT Service Desk within 24 hours.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

In relation to this policy, the following positions are responsible for the following:

5.1 Policy Owner

The Chief Information Officer has overall responsibility for the content of this policy and its operation in the University.

5.2 Manager, Information Security

Manager, Information Security is responsible for ensuring that a formal review and re-approval of this policy takes place at least annually, and after any significant change to the business or threat environment.

5.3 Staff/students/contractors/other relevant individuals

Staff/students/contractors/other relevant individuals are required to comply with the content of this policy and to seek guidance in the event of uncertainty as to its application.

6. COMPLIANCE, EXEMPTIONS AND SANCTIONS

Compliance with this Policy is mandatory.

Exemptions to this Policy must be approved as outlined in the Information Security Exemptions procedure.

Non-compliance with this Policy may result in the device being disconnected from the University network, or access to the Subscriber line being revoked.

7. RELATED DOCUMENTS:

The policy is supported by the following Policies, Standards and Procedures:

- Information Security Policy
- Acceptable Use of Information Technology Policy
- Mobile Devices and University Subscribed Home Internet Services Guidelines
- Privacy Policy
- Information Classification and Handling Guidelines
- Student/Staff Code of Conduct
- ECU Code of Conduct
- Email Policy
- Copyright Policy
- Social Media Policy
- Information Security Exemption Procedure (draft)
- Strategic Procurement Policy and Guidelines

8. CONTACT INFORMATION

For queries relating to this document please contact:

Policy Owner	Chief Information Officer
All Enquiries Contact:	Manager, Information Security
Email address:	infosec@ecu.edu.au

9. APPROVAL HISTORY

Policy Approved by:	Vice-Chancellor
Date Policy First Approved:	7 December 2016
Date last modified:	June 2017
Revision History:	June 2017 • Change of policy title - previously titled Mobile Device Use; • Added content on procurement/internet services.
Next Revision Due:	June 2018 This policy will be periodically reviewed to ensure compliance with legal and financial requirements, remain reflective of the current technological landscape, and address current and future business needs. This process will occur no less than annually.
TRIM File Reference	SUB/77669

Guidelines

These guidelines are intended to provide information to Schools and Service Centres on the sourcing, use and termination/disposal of University Owned Mobile Devices (UOMD) or University Subscribed Home Internet Services (USHIS). This document also provides information related to the use of Personally Owned Mobile Devices (POMD) that connect to the University's network.

1. Sourcing of University Owned Mobile Devices (UOMD) or University Subscribed Home Internet Services (USHIS).

1.1 A Responsible Manager may allocate a UOMD and/or the use of a USHIS to staff with a demonstrated business need and as part of the staff member's agreed role. This includes:

- being contactable when away from their desk;
- traveling frequently;
- being contactable when outside of the University; or
- being contactable outside of working hours.

1.2 Once an approval has been sought from the Responsible Manager, the staff member is required to complete an FBT declaration as part of the service request in ServiceNow. This declaration states that the UOMD and/or USHIS is intended to be primarily for business purposes.

1.3 Non-staff Council Members are not required to complete the FBT declaration above.

1.4 The issuance of the UOMD and/or USHIS must be approved by the Responsible Manager and reviewed periodically for ongoing applicability:

- every time a UOMD is due to be replaced; or
- when a substantial change in the duties of the staff's position occurs.

1.5 A UOMD that is a smart device will be issued with a standard feature set, including Mobility Management Software or any software deemed necessary by the University.

1.6 Lost or stolen UOMDs must be reported to ITSC within 24 hours.

1.7 Replacement of UOMD that are:

- still working - can only occur at a minimum of every two years; and
- lost and/or stolen - will be replaced at the discretion of the Responsible Manager.

1.8 Schools and Service Centres must procure UOMD and/or USHIS from the University's Preferred Supplier as per the Strategic Procurement Policy and associated Guidelines.

1.9 For Personally Subscribed Home Internet Services (PSHIS) funded on an ad hoc/short-term basis, staff must arrange their own connection and seek reimbursement from the University for the estimated business usage of that connection, for the period the service is required for business purposes.

1.10 The University reserves the right to revoke approval for a UOMD and USHIS at any time.

2. Use of University Owned Mobile Devices (UOMD) or University Subscribed Home Internet Services (USHIS)

2.1 Usage and Expense

2.1.1 The Staff member is responsible for the proper physical use, care and maintenance of their UOMD.

2.1.2 The Responsible Manager in School or Service Centre is responsible for the UOMD and USHIS allocation, usage and expenses in their respective area until the end of the contract term.

2.1.3 The associated monthly service fee, covering the UOMD and USHIS, will be charged to the appropriate School or Service Centre's cost centre.

2.1.4 The Responsible Manager (or delegate) must report all cost centre changes or expiry dates via a service request in ServiceNow for ITSC to update within the Supplier's billing portal.

2.1.5 Individuals are responsible for turning off global data roaming. If required, staff members who are travelling internationally must seek approval from the Executive Dean or Director.

2.1.6 Calls to international numbers and global roaming (voice and data) usage (if enabled and not part of the monthly service fees and/or roaming package) are charged in addition to the monthly service fees. They are billed at the contractually agreed international and global roaming rates and are charged directly to the respective cost centre.

2.1.7 Staff members must access data on UOMD via University Wi-Fi services or free Wi-Fi services (e.g. hotel, airport) wherever possible, whist remaining aware of any information security risks of free Wi-Fi services.

2.1.8 On procurement of a UOMD the user will be allocated a national data quota. Excess Usage Charges will be charged to the School or Service Centre.

2.1.9 Staff members must not seek reimbursement from the University for the payment of apps, or digital media in iTunes, the App Store, or the Google Play store that are purchased for private use.

2.2 Security for University Owned Mobile Devices (UOMD)

2.1.10 Any access of the University's information or information systems through use of a UOMD must be in accordance with University policy, standards and procedures as defined in Section 7 of the Policy.

2.1.11 To protect the University's information and information systems, the University expects all device users to assume certain responsibilities for any device that contains University data, connects to the University network, or accesses the University's technology systems. To that end:

- The University is not responsible for backing up your UOMD or ensuring continuity of access to personal apps and data;
- The University requires that you keep your device software current with PIN and/or biometric access controls active where available. If this requirement is not met, the device may be quarantined with limited access, or denied access to the network until the device is compliant with these requirements;
- The University, for network security purposes, may require the installation of a Mobility Management Software Agent, or any other software deemed necessary, on the UOMD;
- The UOMD may be remotely wiped (i.e., erasing all data and applications) by the University if it is lost or stolen;
- For the purposes of maintaining University data security, University provided information sharing capability (for example, Box) must be used for the purpose of sharing University information between devices;

- Access credentials for devices connected to University internal systems must not be provided to any other individual, and each device in use must be explicitly granted access after agreeing to the terms and conditions of this document; and
- Access to University information systems will be monitored to meet the legal and fiduciary responsibilities of the University.

3. Disposal/Termination of University Owned Mobile Devices (UOMD) or University Subscribed Home Internet Services (USHIS).

3.1 At the conclusion of their employment, staff must ensure the UOMD is Sanitised and returned to their Responsible Manager. The Responsible Manager must either reassign the UOMD to another staff member or arrange for its decommissioning. The Responsible Manager must ensure that payment of a USHIS is terminated.

3.2 Once Sanitised, the Responsible Manager must arrange for all decommissioned phones to be disposed of at Mobile Muster (www.mobilemuster.com.au).

3.3 UOMD when returned at the conclusion of employment or when the device is no longer required may attract a remediation charge to the respective cost centre if they are:

- Found to have unreasonable wear and tear; or
- deemed unusable.

3.4 If for any reason the UOMD and/or USHIS is no longer intended primarily for business purposes, the staff member is required to cancel the UOMD and USHIS, or contact the FBSC Tax Management Team for further advice.

3.5 All UOMD must be registered and remain as the property of the University.

3.6 Porting out a mobile number for personal use is subject to the approval of the Responsible Manager.

4. Personally Owned Mobile Devices (POMD)

4.1 Any access of the University's information or information systems using a POMD must be in accordance with University policy, standards and procedures as defined in Section 7 of the Policy.

4.2 To protect the University's information and information systems, the University expects all users to assume certain responsibilities for any device that contains University data, connects to the University network, or accesses the University's technology systems. To that end:

- The University is not responsible for backing up the device or ensuring continuity of access to personal apps and data;
- The University does not provide support for POMD but will use best efforts to assist in connecting Compliant Devices to the University's network;
- The University requires that you keep your device software current with PIN and/or biometric access controls active where available. If this requirement is not met, the device may be quarantined with limited access, or denied access to the network until the device is compliant with these requirements; and
- The University is not responsible for damage, corruption or security breach of personal devices connected to the University's network.

Definitions

TERM	DEFINITION
Excess Usage Charges	Fees charged by the Supplier(s) for any excess usage above the allocated quota of the individual Subscriber Plan
FBT	Fringe Benefits Tax
Mobility Management Software Agent	A service that enables the University to deploy and support applications to mobile devices and to enforce policies that maintain the desired level of security of University information held or stored on mobile devices
Personally Owned Mobile Devices (POMD)	Any personally owned Mobile Phone, Smartphone, tablet, laptop, or hybrid device that connects to the University's network
Personally Subscribed Home Internet Services (PSHIS).	Internet services procured by a staff member primarily for personal use but have some use for University business purposes
Responsible Manager	School Dean or Service Centre Director or delegate with the authority and responsibility to expend and manage costs against the University's cost centre
Sanitised	Removing all information from the phone, including call history, contact details, text messages or other data and installed applications and resetting the phone to factory state. A phone must be sanitised according to the manufacturer's instructions for factory reset after any information to be retained is transferred to the new device
Security Functions	Any capability on the device that increases the security posture of that device, e.g. PIN, Passwords, Biometric Access, inbuilt security features
University Subscribed Home Internet Services (USHIS).	Internet services provided to a staff member at a location other than their workplace, under the University provider contract
University Owned Mobile Devices (UOMD)	Any Mobile Phone, Smartphone, tablet, laptop, or hybrid device issued by the University

CONTACT INFORMATION

For queries relating to this document please contact:

Guideline Owner	Chief Information Officer
All Enquiries Contact:	Manager, Information Security Management
Email address:	infosec@ecu.edu.au

APPROVAL HISTORY

Policy Approved by:	University Executive
Date Policy First Approved:	2nd November 2016
Date last modified:	January 2018
Revision History:	Inclusion of the financial requirements for mobile devices and internet.
Next Revision Due:	This guideline will be periodically reviewed to ensure compliance with legal and financial requirements, remain reflective of the current technological landscape, and address current and future business needs. This process will occur no less than two yearly.