Name of Procedure	Collaborate *Plus* Bring Your Own Device (BYOD) Procedure
Description of Procedure	This Procedure outlines acceptable use guidelines including ACU IT support for Portable Devices which are used within the ACU environment
Procedure applies to	☒ University-wide ☐ Specific (*outline location, campus, organisational unit, etc.)*
	☐ All Staff ☒ All Students & Visitors ☐ Staff and Students
Procedure Status	☒ New Procedure ☐ Revision of Existing Procedure
Description of Revision	New

Approval Authority	Niranjan Prabhu
Governing Authority	Information Communication Technology Advisory Committee
Responsible Officer	Director, Information Technology

Approval Date	15 September, 2017
Effective Date	15 September, 2017
Date of Last Revision	15 September, 2017
Date of Next Procedure Review*	15 September, 2018

** Unless otherwise indicated, this Procedure will still apply beyond the review date.*

Related Legislation, Policies, Procedures, Guidelines and Local Protocols	Information Security Policy Information Security Procedure Acceptable Use of IT Facilities AARNET Access Policy Telecommunications Usage Policy **IT Catalogue of Services *TBC*

Table of Contents

1. Background Information

The Bring Your Own Device (BYOD) Procedure sets out the requirements of both the users of the devices and ACU's responsibilities in supporting these devices.

ACU makes computer facilities available to students through the library and computer labs, but students (& visitors) may choose to bring their own device for use on campus. There are a number of courses offered within ACU where BYOD required with their unit outline – students are notified of this requirement by the unit coordinator upon commencing the units work.

2. Procedure Statement

ACU recognises the benefit of students and visitors using their own devices and is committed to supporting this practice.

3. Procedure Purpose

The Purpose of the BYOD Procedure is to:

- Define which BYOD/s are permitted for use within the ACU Information Technology Environment
- Define the support arrangements in which ACU will assist BYOD/s users
- Affirm the ACU Information Security Procedure and Procedures for BYOD/s

4. Application of Procedure

This Procedure applies to all students and visitors who use a BYOD/s within the ACU Information Technology Environment AND have current ACU assigned credentials.

5. Procedure Principles

5.1 Acceptable Devices

Due to the nature of evolving technology, a broad definition of acceptable devices includes:

- Portable device/s with a current manufactured supported licenced operating system running either Apple OS, Microsoft, orAndroid, with the most recent patching available for that operating system.
- A portable device with current manufactured supported antivirus protection with the most recent patching available (currently only iOS devices are excluded as no antivirus protection is avaialble)
- A portable device that has wireless standards with the capabilities of 802.11n 5Ghz and can connect via WAP2 Enterprise encryption
- iOS and Android devices must not be jailbroken or Rooted (as defined), this ensures a secure BYOD and protects the ACU Network from risk

5.2 Access

- All users are required to conform to the Acceptable Use Procedure
- Access to the internet is solely for education purposes and will be at no cost to students and visitors provided they have current ACU assigned credentials

5.3 ACU Support

As BYOD/s are not, nor can be, standardised, ACU does not provide any warranty or support for BYOD/s other than written documentation available on the ACU web site.

For students and visitors, in-person support is provided by ACU within the library through the student jobs on campus support programme. The support provided in this programme is limited to:

- Assistance with the connection of your BYOD/s to the ACU Wireless network
- Assistance with accessing student email
- Assistance with ACU assigned credentials
- Assistance with Anti-Virus installation
- Assistance with printing via wireless printing
- Assistance with the connection of your BYOD/s to the ACU AV equipment in the Collaborate *Plus* space
- Providing generalised advice
-

Support will managed as first come first serve, but can be booked in for set times

No other forms of support will be supplied by ACU as BYOD/s are personal devices. The following examples of support will not be provided by ACU:

- Installation of ACU provided applications
- VPN setup
- Places to recharge a BYOD/s
- Physical security of the device, the university will not be held accountable for lost or stolen BYOD/s
- Installation of user applications and troubleshooting existing ones
- Instruction on how to use applications
- Installation and troubleshooting operating systems

Devices purchased through the ACU IT Purchasing Portal (that are not a special quote and from the standard list of offerings) have different support arrangements and are not considered a BYOD/s. Support arrangements are outlined through the IT Catalogue of Services.

5.4 Damage and Loss

The owners of a BYOD/s bring their device/s to the University at their own risk and are only covered through owner insurance. In addition, the owner is responsible for backing up the data on their device.

In cases of malicious damage or theft of another student's device, existing University processes for damage to University or another student's property apply. The University does not provide accidental damage or theft cover for 3rd party (student owned) devices and shall therefore not be liable for any damages or theft that occurs on the University premises unless the device was under the direct control of a staff member.

Under no circumstances should devices be left in unsupervised areas (including, but not limited to, University grounds, open building spaces, specialist areas, library, offices, unlocked classrooms or toilets). Any device left in these areas is at risk of being stolen or damaged. If a device is found in an unsupervised area, it will be taken to lost property.

6. Roles and Responsibilities

6.1 University's Responsibilities

Through the ACU Information Technology Directorate, ACU must ensure that there is appropriate documentation available, so ACU Students can make use of their BYOD/s within the ACU environment and self-support.

ACU will only provide the support listed above at (5.3)

ACU will ensure an appropriate wireless network.

6.2 Users Responsibilities

All users of BYOD/s must make sure:

- The operating system is up to date, and all patches/updates have been installed
- There is anti-virus protection installed on the device, and it is up to date
- That their BYOD/s have correctly licenced software installed on it
- That their BYOD/s have appropriate battery life and they are completely charged before being brought to the University
- Maintain physical security for the BYOD/s
- Maintain virtual security for the BYOD/s including pins and passwords
- Clearly label the BYOD/s with ownership details and contact numbers
- Understand the limitations or the manufacture's warranties for their BYOD/s, both in duration and in support provided
- Take out insurance coverage for their own BYOD/s to protect any accidental damage, theft or loss.
- Operate their BYOD/s so that they do not disrupt those around them (e.g. use headphones, take phone calls away from anyone else, etc.)
- Purchase and use BYOD/s protective casing, additional or spare battery packs and appropriate changing cables and chargers
- The BYOD/s are safe and secure during travel to and from University and throughout the day
- The BYOD/s must not be used to copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner
- The BYOD/s must not be used to take photos or make video or audio recordings of any individual or group without the express permission of each individual being recorded and the permission of an appropriate staff member
- Consider ergonomics (is this device comfortable to use for an entire University day)
- Have additional backup storage such as portable hard drive or USB flash drive for all data

7. Procedure Review

This Procedure must be reviewed every two years or a shorter period where technological circumstances warrant an earlier review, this may be initiated by the Director of Information Technology

8. Further Assistance

Further enquiries should be directed to the Information Technology Director

9. Glossary of Terms

BYOD/s - Bring Your Own Device (BYOD) can refer to one or more laptops, tablets, mobile phones, surface pros, smart watches, and other such devices that have the ability to run from a power source including a battery

ACU IT – Australian Catholic University Information Technology Directorate

User – An ACU Student or Visitor who is currently operating/using a BYOD/s

ACU Network – The computing environment found within the Australian Catholic University. All wireless networks where ACU Provided User Credential allow access.

Operating System Patch/Update – A patch/update is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches/updates usually called bug fixes or bug fixes, and improving the usability or performance.

Jailbroken – iOS jailbreaking is the process of removing software restrictions imposed by Apple's on iOS and TV OS. It does this by using a series of software exploits. Jailbreaking permits root access to iOS, allowing the downloading and installation of additional applications, extensions, and themes that are unavailable through the official Apple App Store.

Rooted - Rooting is the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android sub systems.

Portable - The device can be easily carried, held, and operated by hand.