Bring Your Own Device (BYOD) Policy for Students

Section 1 - Policy Statement

(1) ACU recognises the benefits generated by students using their own devices and is committed to supporting this practice.

Section 2 - Policy Purpose

(2) This Policy sets out the roles and responsibilities of both the users of the devices and ACU's in supporting them and their devices.

(3) This Policy seeks to:

a. define acceptable devices as Bring Your Own Device (BYOD) for use within ACU information technology environment;
b. define support arrangements in which ACU will assist BYOD users; and
c. affirm the Information Security Policy and Information Security Procedure for BYOD and user obligation.

Section 3 - Application of Policy

(4) This Policy applies to all students who utilise BYOD within the ACU information technology environment and have current ACU assigned credentials.

Section 4 - Definitions

Term	Definition
Acceptable Device	A portable device with a current manufacturer supported licensed operating system running either Windows, macOS, iOS, or Android, with the most recent system update available for that operating system. 1. The portable device must have current wireless capability and support ACU network security requirement. 2. The portable device must have current wireless capability and support ACU network security requirement. ACU reserves the right to deny devices that do not meet these requirements from connecting to ACU networks and mark those devices as unacceptable.
ACU Assigned Credentials	Username and password that allows a user to access the ACU Network.
ACU Network	The computing environment found within the Australian Catholic University. All wireless networks where ACU assigned credentials allow access. This can also include any use of ACU's federated access.

Term	Definition
Agreed period	Agreed period is based on the software licensing agreement at ACU. Once a student has completed their studies at ACU, the software must be removed.
BYOD	Bring Your Own Device.
Malicious Software	Malicious software also known as Malware refers to any malicious program that causes harm to a computer system or network. Malicious software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits. Tampered software that has been jailbroken or rooted are also considered malicious software.
Network Security Requirements	Network security requirements are defined as per the Information Security Policy and Information Security Procedure.
Portable Device	A device that can be easily carried, held and operated by hand.

Section 5 - Policy Principles

Support Arrangements for BYOD Users

(5) The scope of IT support provided for BYOD users are:

a. assistance with connecting acceptable BYOD to ACU wireless network. No wired connections permitted;
b. assistance with accessing ACU student email;
c. assistance with using wireless printing; and
d. provide general IT advice. ACU will only provide technical advice specific to ACU network and systems. Students should seek external professional technical support for non-ACU related matters for their BYOD.

There are Two Ways to Access BYOD Support for Students

In-person Support

(6) In-person support is only available during the semester from the Information Technology support desk at selected campuses. To receive in-person support:

a. student must be present with the BYOD throughout the whole support session. Staff will not attend to a BYOD without its owner present;
b. best efforts will be made to assist the student with their chosen device. ACU does not guarantee that all issues can be resolved for the BYOD that is brought in; and
c. any support request not covered under clause (5) will be refused.

Support through online resources

(7) Additional support via online resources is available through AskACU. Information on virtual labs and software available for students' BYOD are frequently updated. AskACU will have the latest repository for reference.

Section 6 - Roles and Responsibilities

University's Responsibilities

(8) The University will ensure that:

a. an appropriate level of support (including online documentation) as outlined in Section 5 in this Policy is made

available to students; and

b. an appropriate wireless network is made available within ACU campuses.

User's Responsibilities

(9) All users of BYOD are responsible for ensuring:

a. maintenance of physical security of the BYOD. Students who bring their device to the University, do so at their own risk and are only covered through their own personal insurance for any theft or damage (intentional or unintentional);
b. devices should not be left unsupervised as it is at risk of being stolen or damaged. ACU is not responsible for any loss;
c. maintain a backup of their data;
d. meets the requirements as outlined in the definition of an acceptable device within this Policy, including:
    i. an up to date anti-virus protection installed on the device;
    ii. PIN and / or passwords enabled upon start-up and / or login;
    iii. and adhere to the Information Security Policy and Information Security Procedure as well as the ICT Acceptable Use Policy; and
e. if ACU software is made available to be installed on the BYOD, it must be removed after the agreed period is over.

(10) If a BYOD has been flagged as a security risk to the ACU Network, wireless access will be blocked to the device. Impacted students will be contacted by AskACU.

Section 7 - Review

(11) This Policy must be reviewed every three years. The Chief Information and Digital Officer may initiate a shorter review period.

(12) Unless otherwise indicated, this Policy will still apply beyond the review date.

Status and Details

Status	Current
Effective Date	28th February 2024
Review Date	30th April 2024
Approval Authority	
Approval Date	28th February 2024
Expiry Date	Not Applicable
Responsible Executive	Russell Parker Chief Information and Digital Officer
Responsible Manager	Russell Parker Chief Information and Digital Officer
Enquiries Contact	Mary Futol Executive Manager, Deputy Vice-Chancellor (Corporate) Information Technology