

STU09 BRING YOUR OWN DEVICE POLICY AND PROCEDURE

Department	Academic
Approval Authority	Academic Board
Responsible Officer	Registrar
Effective Date for use	1 October 2026
Date of next review	August 2029 (3 years from approval date)

1. Purpose

This Policy and Procedure establishes the requirements, responsibilities, and conditions for students using personally owned devices to access TITAN HIGHER EDUCATION (TITAN/THE) information technology resources, systems, applications, data, and networks.

2. Scope

2.1 This Policy and Procedure applies to:

- All TITAN students who use personally owned devices to access TITAN systems, services, applications, or networks.
- All personal laptops, tablets, smartphones, and other portable computing devices used to connect to TITAN resources.
- All campuses, learning environments, and online learning platforms operated by TITAN.

2.2 This policy does not apply to:

- TITAN-owned devices.
- Devices managed and supported directly by TITAN.
- Network equipment specifically designed for network access such as personal Wi-Fi access points, routers, or network extenders.

3. Policy Statements

- 3.1 TITAN students are required to bring their own device to their learning sessions and activities.
- 3.2 Students are authorised to bring their own device to access or connect to TITAN's IT services, data, and networks, provided they comply with the requirements outlined in this policy and procedure.
- 3.3 TITAN aims to make its systems, applications, and interfaces accessible across a wide range of devices and operating platforms. However, TITAN cannot guarantee that all devices, operating systems, software versions, or configurations will operate successfully with TITAN systems and services.
- 3.4 Students are responsible for ensuring their devices meet the technical requirements specified by TITAN and maintaining their devices in a secure and operational condition.
- 3.5 Students should consult their Letter of Offer and program information for details regarding the minimum technical specifications required for their devices.

4. Policy Principles

TITAN is committed to:

- 4.1 Supporting flexible and accessible learning environments.
- 4.2 Protecting institutional information and technology assets.
- 4.3 Maintaining compliance with privacy, cybersecurity, and information security obligations.
- 4.4 Providing equitable access to learning resources where practicable.
- 4.5 Minimising risks associated with personally owned devices.

5. Procedures

5.1 Students:

- Must ensure that their devices are capable of connecting to TITAN-approved Wi-Fi and network services and meet the technical requirements specified by TITAN.
- Must ensure that they have consulted their Letter of Offer for specific details regarding the technical specifications of their devices for usage at TITAN.
- Are responsible for all costs associated with the purchase, maintenance, repair, insurance, and operation of their devices.

5.2 TITAN:

- Will inspect and verify that TITAN data has been removed from the device at the end of its use within the TITAN environment or when a device is at the end of life.
- TITAN may perform a remote wipe of TITAN data in order to prevent unauthorised access.
- By choosing to BYOD, the user gives consent for TITAN to interrogate such devices to ensure appropriate use.
- Is not responsible for any damage or loss that occurs to any personal device.
- Aims to make their systems and interfaces accessible across a wide range of devices and platforms however cannot guarantee that any particular combination of system and device will operate.

6. Acceptable Use

6.1 Students must:

- Use their devices in accordance with TITAN policies and procedures.
- Access only information and systems for which they have authorisation.
- Protect their login credentials and passwords.
- Log out of systems when not in use.
- Use TITAN networks and systems for legitimate educational purposes.
- Report any suspected security incident, loss, theft, or unauthorised access affecting TITAN information.

6.2 Users must not:

- Attempt to bypass TITAN security controls.
- Introduce malicious software or engage in activities that compromise TITAN networks.
- Share their user credentials with others.
- Access data or systems without authorisation.
- Download, store, or transmit illegal, offensive, or inappropriate material using TITAN systems.
- Connect unauthorised networking devices to TITAN infrastructure.

7. Network Connection Requirements

- 7.1 Devices which are specifically designed for network access, including but not limited to:
- Wi-Fi access points.
 - Wireless routers.
 - Network switches.
 - Mobile hotspot devices acting as access point.
- 7.2 Devices may not be attached to TITAN's network infrastructure unless specifically authorised by TITAN.
- 7.3 TITAN reserves the right to deny or discontinue network access to any device that presents a security, operational, or compliance risk.
- 7.4 All online activities at TITAN will be conducted in accordance with applicable privacy and legal obligations.

8. Security and Monitoring

- 8.1 To protect TITAN information and systems, TITAN may implement security controls, including:
- Network monitoring.
 - Access controls.
 - Device authentication.
 - Security scanning.
 - Threat detection and logging.
- 8.2 Device Security and Patch Currency
- When using your own device, users consent to TITAN performing appropriate monitoring and interrogation of devices connected to TITAN systems and networks to ensure compliance with this policy and procedure.
 - Students must keep the operating system on their device within the manufacturer's supported lifecycle (refer to #9, below). Devices running an operating system that no longer receives security updates from the vendor (for example, an end-of-life version of Windows or macOS) must not be used to access TITAN systems, including the LMS, student email, or campus Wi-Fi.
 - Students must have automatic updates enabled for their operating system and web browser or otherwise ensure security patches are applied promptly after release.
 - Students must have antivirus or anti-malware protection active on the device. Built in protection such as Microsoft Defender or Apple's XProtect satisfies this requirement, a separate paid product is not required.
 - Students must not disable device security features, including firewall, disk encryption, or screen lock, while the device is being used to access TITAN systems.

9. Hardware:

- 9.1 Minimum specifications for laptop:
- 16GB RAM or greater.
 - 512GB SSD or greater (solid state drive only).
 - 13" screen or larger, resolution at least 1920 x 1080.
 - USB-C port (USB 3.2 Gen 1 or later).
 - Wi-Fi 6 (802.11ax) or Wi-Fi 5 (802.11ac) capable.
 - Webcam (USB or integrated).

- An in-built microphone or a headset with headphones and microphone.

9.2 Operating System and Software:

- Minimum: Windows 11 (64 bit) / macOS 14 Sonoma or later.
- Latest version of one of the following web browsers: Google Chrome, Firefox, Safari or Microsoft Edge.

10. Privacy

10.1 TITAN respects the privacy of users and will only access, monitor, inspect, or interrogate devices to the extent necessary to:

- Protect TITAN systems and data.
- Investigate security incidents.
- Ensure compliance with TITAN policies.
- Meet legal or regulatory obligations.

10.2 Students should be aware that information created, stored, transmitted, or accessed through TITAN systems may be subject to monitoring and review.

11. Lost, Stolen, or Compromised Devices

11.1 Students must immediately notify TITAN if a device:

- Is lost or stolen.
- Is suspected to be compromised.
- Contains TITAN information that may have been exposed.
- Is accessed by an unauthorised person.

11.2 TITAN may temporarily suspend access or remotely remove TITAN data until the matter is resolved.

12. Support Services

12.1 TITAN will provide reasonable assistance regarding access to TITAN systems and services.

12.2 However, TITAN does not provide technical support for:

- Personally owned hardware.
- Personal software applications.
- Device repairs.
- Data recovery.
- Operating system issues unrelated to TITAN services.

13. Liability

13.1 TITAN is not responsible for:

- Loss, theft, or damage to any personal device.
- Hardware or software failures.
- Loss of personal data.
- Costs incurred through participation in bringing your own device to campus.
- Interruption of access due to device incompatibility or security requirements.

14. Non-Compliance

14.1 Failure to comply with this policy and procedure may result in:

- Removal of network access.
- Suspension of access to TITAN systems and services.

- Disciplinary action under relevant policies and procedures.
- Legal action where applicable.

15. Roles and Responsibilities

15.1 Students are responsible for:

- Providing and maintain their own devices.
- Ensuring their devices meet TITAN specifications.
- Complying with this policy and procedure.
- Protecting TITAN information and systems.
- Reporting security incidents promptly.

15.2 TITAN is responsible for:

- Maintaining secure systems and networks.
- Providing access to approved services and platforms.
- Monitoring and protecting institutional information assets.

16. Definitions

Definitions for key terms are presented in the Glossary of Terms which may be accessed on the TITAN website.

17. Relevant Legislation, Guides, and/or Websites

17.1 Legislation:

- [Privacy Act 1988](#) (accessed July 2026)

17.2 Guides:

- TEQSA Guidance Note: [Technology-enhanced Learning](#) (accessed July 2026)

18. Related TITAN Documents

- Admissions Policy and Procedure
- Information Technology Acceptable Use Policy and Procedure

19. Version Control

Policy and Procedure Version Control		
Version #	Date of Change	Change Summary
2026.1	July 2026 Approved AB 11.08.2026 Noted BoD 23.09.2026	New Document

Warning –

- Document uncontrolled when printed! The current version of this document is maintained on the TITAN website.