BYOD Procedure

1. Purpose and Scope

1.1 The BYOD Procedure sets out the terms of use for 'bring your own device' (BYOD) within AIAT. Its purpose is to:

1.1.1 allow users to BYOD for study or work purposes, and access AIAT information when and where it is needed; and to

1.1.2 ensure that AIAT systems and data are protected from unauthorised access, use or disclosure.

1.2 This procedure applies to

1.2.1 all AIAT students, academic and non-academic staff and all members of Boards and Committees who utilise a physical or wireless connection to AIAT network infrastructure.

1.2.2 any device or accompanying media that may be used to access the systems and data of AIAT, whether it is used within or outside your standard working or study hours.

2. Definition

Refer to *Glossary of Terms.*

Authorised user is a person issues with an AIAT authorised account as per the guidance in the Acceptable Use of ICT Procedure.

Bring Your Own Device (BYOD): the use of any electronic device not owned or leased by AIAT, and which is capable of storing data and connecting to a network (e.g., wireless, 4G, physical connection), to access or connect to AIAT's IT services, data and networks. This includes but is not limited to mobile phones, smartphones, tablets, laptops, notebooks and portable storage devices.

3. Procedure

3.1 Authorised users may bring their own device to access or connect to AIAT's IT systems and networks, provided they meet the obligations of this procedure and the Acceptable Use of ICT Procedure.

3.2 This procedure applies to all authorised users and all devices that connect to the AIAT network, other than AIAT owned, leased or supported devices.

3.3 The following devices may not be attached to AIAT's network infrastructure:

3.3.1 devices which are specifically designed for network access, such as switches, Wi-Fi access points and hubs.

3.4 AIAT cannot guarantee that any particular combination of system and device will operate, however AIAT aims to make AIAT systems and interfaces accessible across a wide range of devices and platforms.

3.5 AIAT reserves the right to inspect and verify that AIAT data has been removed from the device at the end of its use within the AIAT environment or when a device is at end of life.

3.6 AIAT may perform a remote wipe of AIAT data in order to prevent unauthorised access.

3.7 By choosing to BYOD, the user gives consent for AIAT to interrogate such devices to ensure appropriate use, as defined by the Acceptable Use of ICT policy and procedure.

3.8 AIAT is not responsible for any damage or loss that occurs to any personal device.

3.9 Limited support may be provided to assist users in accessing AIAT systems and networks.

3.10 Device Owners will not be prevented from installing software or applications on their device. However, AIAT may block access to AIAT ICT services and networks if any software, applications or data present a threat to AIAT ICT systems and resources.

3.11 AIAT at its own discretion, may:

- 3.11.1 de-register any BYOD at any time without warning; or
- 3.11.2 de-register a BYOD that has not consumed AIAT ICT services for more than 12 months.

3.12 Users who choose to BYOD must:

- 3.12.1 ensure that the operating system, firmware and installed software is obtained from an authorised source, is up to date and that required security patches have been applied to protect against known vulnerabilities;
- 3.12.2 employ security solutions where available, including anti-virus, firewall and threat intelligence capabilities;
- 3.12.3 not perform system administration of any AIAT system using a BYOD device, without prior approval from the IT Support Officer or CEO;
- 3.12.4 remove or transfer all AIAT data from the device or associated storage when no longer required or when the device is decommissioned;
- 3.12.5 perform regular data backups of all AIAT data;
- 3.12.6 immediately inform the IT Support Officer if any personal device carrying AIAT data is lost or stolen;
- 3.12.7 assume sole responsibility for operating system, the device and any personal applications running on the device;
- 3.12.8 ensure the software and services being used on the device for work related to AIAT are compliant with the conditions of use specified in the software license or within any license agreement between AIAT and the vendor;
- 3.12.9 ensure the device supports password or pin authentication and that this is enabled; and
- 3.12.10 ensure that the device has the automatic lock enabled.

4. Roles and responsibilities

4.1 Staff, Students and members of Boards and Committees are responsible for

4.1.1 complying with all ICT policies and procedures; and

4.1.2 understanding that use of AIAT ICT systems and resources are subject to Australian laws and other relevant AIAT policies; and

4.1.3 understanding that access to some third party applications and content have separate contractual arrangements and terms and conditions, which may apply over and above this procedure.

5. Procedure Details

Institution	Australian Institute of Advanced Technologies (AIAT)
Procedure name	BYOD Procedure
Procedure Reference No.	PROC – 36b
Procedure Approval	Board of Directors
Procedure Authority	Executive Management Group
Responsible Officer	CEO
Governance Reference Threshold Standards	HESF 2021: 2.1.2, 7.3.3
Related Documents	Acceptable Use of ICT Policy Acceptable Use of ICT Procedure Information and Communications Technology Policy
Related Legislation	Higher Education Standards Framework (Threshold Standards) 2021 (HESF)
References	AIAT has referred and benchmarked with the following institutions and policies during the creation of this policy: ANU (2019) Procedure: Bring your own device Australian Catholic University (2021) Bring Your Own Device (BYOD) Policy for students University of Newcastle (unknown) Information Security BYOD Procedure, *retrieved from web on 4 Nov 2021*
Date of approval	31 March 2022
Review date	December 2024
Policy Category	Operational

6. Document Version Control

Document No	PROC – 36b	Last Modify Date	Summary of Changes
Version No	1.0	NA	Initial version approved by Board of Directors

	1.01	31/3/2022	Fixed typos; new policy number
Created Date	Dec 2021		