Acceptable Use of ICT Procedure

1. Purpose and Scope

1.1 The Acceptable Use of ICT Procedure operationalises the Acceptable Use of ICT Policy by
- 1.1.1 clarifying the responsibilities of users of AIAT ICT systems and resources;
- 1.1.2 identifying inappropriate uses of AIAT ICT systems and resources;
- 1.1.3 defining limited Personal Use of AIAT ICT systems and resources;
- 1.1.4 describing the types of access and monitoring activities that will occur.

1.2 This procedure applies to all AIAT students, academic and non-academic staff and all members of Boards and Committees.

2. Definition

Refer to *Glossary of Terms.*

3. Procedure

3.1 Authorised Users
- 3.1.1 It is a requirement that every person who accesses AIAT ICT systems and resources must have an authorised user account for their exclusive use.
- 3.1.2 Authorised accounts will only be issued to staff employed by AIAT, currently enrolled students, visiting academics, contractors or consultants engaged by AIAT, or other recognised affiliates of AIAT.
- 3.1.3 Access to AIAT ICT systems and resources will be provided in adherence to the Principle of Least Privilege, so that authorised users will only be provided with the minimum privileges and access rights required to perform their job functions as approved by their manager.

3.2 General use
- 3.2.1 All authorised users must take all reasonable steps to protect their account from unauthorised use.
- 3.2.2 Passwords and access to ICT systems and resources must not be shared.
- 3.2.3 Staff may access, use or share AIAT proprietary information only to the extent it is authorised and required to carry out activities that relate to the duties of their role.
- 3.2.4 Ensure sensitive information is only shared using secure methods of transmission via AIAT ICT systems and resources.
- 3.2.5 Take precautions to ensure that screens displaying sensitive or critical information are not seen by unauthorised persons in public areas and are locked when unattended.
- 3.2.6 Comply with the terms of use that apply to particular software or services.
- 3.2.7 When authorised users bring their own device, they must comply with the BYOD Procedure.

3.3 Device Security

3.3.1 Staff provided with devices (computers, tablets, mobile phones) are responsible for their physical security.

3.3.2 All computing devices, including BYOD, must be configured to comply with the best-practice guidelines when connecting to the AIAT network. Specifically;

a. Passcode or password should be configured on device with automatic screen lock after a period of inactivity.
b. Security software such as antivirus and personal firewall should be installed.
c. Operating system and applications should be kept up to date.
d. Only digitally signed software from trusted sources should be used.
e. Encryption and "remote wipe" features should be enabled for mobile devices when available.

3.3.3 Authorised users are strongly encouraged to either log off or leave screensavers locked when leaving their devices unattended to reduce risk of unauthorised use of their account.

3.3.4 Devices that are compromised by a malware, or determined to pose threat to the security of AIAT ICT systems and resources and other users, may be blocked from connecting to the AIAT network until the sources of threats have been removed.

3.4 Data Security

3.4.1 All electronically held AIAT data should be stored in such a way that it is backed up regularly. This can be achieved by:

a. storing data on AIAT approved systems;
b. storing data on an AIAT network drive or system; or
c. storing data on an AIAT endorsed cloud based storage.

3.4.2 All AIAT data should be captured and maintained in a manner that ensures its quality and integrity.

3.4.3 Use of file storage facilities (e.g. removable media) or unapproved services to store AIAT data is not allowed unless authorised by the CEO.

3.4.4 External storage devices (e.g., USB, removable hard drives) used to store AIAT data must be encrypted. Removable storage should not be used as a primary storage facility.

3.4.5 AIAT staff must not transfer data to external parties unless approved by the CEO or the data owner. Approval will only be granted where data is transferred using secure mechanisms.

3.4.6 All electronically held AIAT data should be captured, stored and disposed of in accordance with the AIAT Records Policy.

3.5 Email

3.5.1 The privacy and integrity of information transmitted by email cannot and is not guaranteed by AIAT. These communications should not be regarded as being confidential.

3.5.2 Staff and students

a. must use extreme caution when opening e-mails received from unknown senders, which may contain malware, viruses or other malicious content; and
b. should avoid opening attachments or hyperlinks that are from suspicious emails; and
c. report suspect emails to the IT Support Officer.

3.5.3 The AIAT email address must be used for the delivery of all official AIAT email.

3.5.4 Staff and students must not send messages to a large number of recipients (e.g. all staff, all students, alumni) without approval from the CEO or Head of Institute.

3.5.5 Staff must not use personal email services (e.g., Google Mail, Yahoo Mail) for the storage of AIAT data or to undertake any AIAT business transactions.

3.5.6 Staff must not automatically forward the entire contents of their mailbox, voicemail or other communications accounts to another AIAT staff member or an email address or service that is external to AIAT.

3.6 Internet

3.6.1 Authorised users are permitted to access the internet for academic, work, research-related purposes and communications with staff and other students.

3.6.2 The IT Support Officer may deny or restrict an authorised users access to internet sites that are reasonably considered to contain inappropriate or malicious content.

3.7 Telephone Services

3.7.1 Calls to premium telephone numbers or international numbers are not to be made unless approved beforehand by the CEO.

3.8 Mobile Phones for business use

3.8.1 The CEO may authorise the allocation to a staff member of an AIAT owned mobile telephone in the following circumstances:

a. where staff member is required in the performance of his or her official duties to:
   - monitor AIAT ICT systems and resources outside normal working hours;
   - attend to an emergency or breakdown on the AIAT premises;
   - be available to respond and attend quickly to a critical incident or urgent ICT problem; or
b. where the CEO is satisfied that the duties and responsibilities of a position to which a staff member is appointed warrant the allocation of an AIAT owned mobile telephone.

3.8.2 Staff members who acquire an AIAT owned mobile telephone shall:

a. ensure that precautions are taken to secure the mobile telephone against theft or damage; and
b. be accountable for all calls made from the mobile telephone.

3.9 Limited Personal Use

3.9.1 AIAT allows limited Personal Use of the AIAT ICT systems and resources. Such use will comply with the requirements outlined in this procedure and in related ICT policies. Personal Use may be monitored as per item 3.11.

3.9.2 Authorised users will consider the following conditions for Personal Use:

a. it does not interfere with the performance of your job, studies or other AIAT responsibilities;
b. interfere with the use or access of other users;
c. damage the reputation or operations of AIAT;
d. impose unreasonable additional costs on AIAT; and/or
e. does not breach any AIAT policies or procedures.

3.10 Unacceptable use of ICT

3.10.1 Unacceptable use includes but is not limited to:

a. engaging in any activity that is in breach of AIAT's policies or procedures, or illegal under local, state, commonwealth or international law.
b. accessing data, network, a server or an account for any purpose other than conducting research, teaching and learning; and supporting the administration of AIAT.
c. circumventing user authentication or security of any host, network or account.
d. changing the security settings on computer equipment or devices (e.g., remove or disable anti-virus software).
e. executing any form of network spoofing and monitoring which will intercept data not intended for the user's host.
f. intentionally introducing any program or device that would degrade AIAT's ICT systems and resources.
g. deliberate, unauthorised corruption or destruction of ICT systems and resources (including deliberate introduction or propagation of computer viruses).
h. using ICT systems and resources to access, create, store, transmit or solicit material, which is obscene, defamatory, discriminatory in nature, or likely to cause distress to some individuals or cultures, where such material is not a legitimate part of learning and teaching or research. Clear examples of such material include, but are not limited to materials that:
    - Contain sexually explicit images or descriptions.
    - Advocate illegal activity.
    - Advocate intolerance or hatred for others.
    - Are bullying or harassing in any way.
    - Breach state and / or federal law.
i. utilising AIAT internet to access explicit material including pornography.
j. transmission or use of material which infringes copyright held by another person or AIAT.
k. uploading, downloading, installing or distributing unlicensed or inappropriately licensed software.

l. interfering with or denying service to another user.
m. sending unsolicited email messages, including sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
n. acquisition and/or use of cloud–based and third-party ICT services without approval from the CEO.
o. effecting security incident(s) in a manner that negatively impacts AIAT or its staff or students.
p. providing information about, or lists of, AIAT ICT users to parties outside AIAT.
q. use which deliberately and significantly degrades the performance of ICT systems and resources for other users (including the downloading of large video files not related to learning and teaching and research).
r. interfering with or attempting to interfere with the investigation of a breach of AIAT policy by:
    - Electronic means – concealing, modifying or erasing the evidence of a breach.
    - Physical means – disposing of or altering hardcopy records.
    - Social means – disseminating false statements.
s. using AIAT ICT systems and resources for unauthorised commercial activities or unauthorised personal gain.

3.10.2 Inappropriate behaviour with respect to the use of AIAT ICT systems and resources includes, but is not limited to the following actions:
a. Breach the AIAT Privacy Statement impacting the protection of personal information.
b. Participate in gambling activities such as may be provided by casino and internet-based gambling sites.
c. Misrepresent him/herself or AIAT.
d. Make fraudulent offers of products, items, or services originating from any AIAT account.
e. Operate a business using AIAT ICT systems and resources.
f. Violate any State, Commonwealth or international laws.

3.11 Access to and Monitoring

3.11.1 AIAT reserves the right to access and monitor:
a. any computer or other electronic device owned or controlled by AIAT; and
b. any computer or other electronic device connected to the AIAT network. AIAT reserves the right to remove access or disconnect systems and services where risk is identified to AIAT.

3.11.2 AIAT will monitor the access and use of its ICT systems and resources, including the content of all electronic communications for, but not limited to the following purposes:
a. where it is required by law.

b. to enable or facilitate investigations or enquiries into alleged misconduct, violations of law, AIAT policies or AIAT procedures or complaints.
c. to protect the security of ICT systems and resources.
d. to protect personal information as per AIAT's Privacy Policy.

3.11.3 Access to an authorised user's computer or other electronic devices must be authorised by the CEO. Access may be authorised for circumstance including, but not limited to
a. unlawful activities or
b. breaches of AIAT policies and procedures.

3.11.4 Access to location services on devices must be authorised by the CEO. Access may be authorised for circumstances including, but not limited to:
a. suspected breaches of AIAT policies and/or procedures by an authorised user; or
b. unlawful activities; or
c. lost/stolen devices; or
d. locate missing staff; or
e. facilitating an emergency response in times of crisis;
f. providing information to relevant emergency services sector organisations for the purpose of staff safety; or
g. other reasons as determined appropriate by the CEO.

3.11.5 Access to and monitoring includes, but is not limited to, email, websites, server logs and electronic files. Information obtained under this approval will be treated as confidential, and only disclosed to relevant parties.

3.11.6 AIAT may keep a record of any monitoring or investigations.

3.12 Reporting Security Incidents or Potential Breaches

3.12.1 All authorised users must
a. report any actual or suspected security weakness, breach or threat involving AIAT ICT systems and resources to the IT Support Officer as soon as possible.
b. report lost loss or theft of AIAT devices (computers, tablets, mobile phones) to their manager or the IT Support Officer;
c. report a loss or theft of an external storage device which contains AIAT data to their manager or the IT Support Officer;
d. respond to potential incidents or events, including un-authorised system usage, as directed by the IT Support Officer;
e. immediately report any suspected breach of the Acceptable Use of ICT Facilities policy or this procedure, to their manager or the IT Support Officer; and
f. immediately report the loss of passwords or if their account has been breached to their manager or the IT Support Officer.

3.13 Breaches of ICT Acceptable Use Policy

3.13.1 Where there is an allegation of non-compliance and the IT Support Officer considers it necessary to act immediately to prevent AIAT learning and teaching,

research and/or administrative functions from being disrupted, the IT Support Officer may:

a. remove or disable an authorised users' access to AIAT ICT systems and resources and/or
b. restrict or remove an authorised users' access to AIAT ICT systems and resources pending further investigation, disciplinary and/or judicial action.

3.13.2 The IT Support Officer will inform the authorised user of any action in writing within 5 working days of the action being taken.

3.13.3 All suspected breaches are to be managed in accordance with the

a. Staff Code of Conduct for staff and Board members; and
b. Student Code of Conduct for students.

3.14 Expiry of Accounts

3.14.1 All authorised users whose relationship with AIAT ceases will be notified prior to their accounts being disabled.

3.14.2 Prior to the authorised user's account being disabled, it is the authorised user's responsibility to ensure that all files and email messages on their account are stored in accordance with the AIAT Records Policy. They must not copy, delete, erase or alter in any way data (including emails) related to AIAT business.

3.14.3 Where an authorised user is unable to comply with item 3.14.2 before leaving AIAT (for instance, due to illness or death), the relevant manager of that authorised user may request that the CEO arrange for a nominated AIAT authorised user to be granted access to view and deal with the records associated with the account before it is disabled.

3.14.4 AIAT will not provide email data to authorised users after they have left AIAT except when explicitly approved by the CEO.

4. Roles and responsibilities

4.1 The CEO is responsible for overseeing the provision of ICT systems and resources as required for AIAT.

4.2 Staff and Students are responsible for

4.2.1 complying with all ICT policies and procedures; and

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

4.2.3 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 policy and procedure.

4.3 Staff are responsible for ensuring all ICT systems and resources are:

4.3.1 for the staff member's use only; and

4.3.2 used for AIAT research, teaching and learning; and the administration of AIAT only.

4.4 Staff are responsible for ensuring devices and accessories assigned to them are:

4.4.1 not loaned to anyone who is not an AIAT staff member;
4.4.2 securely stored when not on AIAT premises; and
4.4.3 returned to AIAT in good working order when the staff member leaves the organisation.

4.5 Staff using ICT systems and resources have a responsibility to promptly report to their manager and the CEO:
4.5.1 the loss, theft, damage, and technical issues to AIAT devices (computers, tablets, mobile phones) or external storage devices; or
4.5.2 the theft, loss or unauthorised disclosure of AIAT proprietary information.

4.6 The IT Support Officer will
4.6.1 manages suspicious emails;
4.6.2 monitor ICT resources;
4.6.3 deny or restrict access to internet sites when appropriate;
4.6.4 receive reports regarding loss or theft of AIAT devices and external storage devices;
4.6.5 receive reports on potential ICT incidents or ICT breaches; and
4.6.6 remove, disable, or restrict access to AIAT ICT systems and resources.

5. Procedure Details

Institution	Australian Institute of Advanced Technologies (AIAT)
Procedure name	Acceptable Use of ICT Procedure
Procedure Reference No.	PROC – 36a
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 Procedure BYOD Procedure Information and Communications Technology Policy Staff Code of Conduct Staff Performance Policy Student Code of Conduct Student General Misconduct Procedure
Related Legislation	Higher Education Standards Framework (Threshold Standards) 2021 (HESF) Crimes Act 1914 (Cth Australia) Cybercrime Act 2001 (Cth Australia) Copyright Act 1968 (Cth Australia) SPAM Act 2003 (Cth Australia)

	Telecommunications (Interception and Access) Act 1979 (Cth Australia) Surveillance Devices Act 2016 (SA)
References	AIAT has referred and benchmarked with the following institutions and policies during the creation of this procedure: Adelaide University (2016) IT Acceptable Use Procedures Curtin University (2018) Information and Communications Technology (ICT) Appropriate Use Procedures Flinders University (2017) Acceptable Use of Technology Procedures Griffith University (2018) Information Technology Code of Practice James Cook University (2017) Information and Communications Technology Acceptable Use Policy James Cook University (2017) ICT Acceptable Use Procedure Monash University (2018) Information Technology Acceptable Use Procedure University of Newcastle (unknown) Information Technology Conditions of Use Policy, *retrieved 28 Oct 2021* University of Queensland (2021) Information and Communication Technology – Policy University of South Australia (2005) Acceptable use of Information Technology (IT) facilities
Date of approval	31 March 2022
Review date	December 2024
Policy Category	Operational

6. Document Version Control

Document No	PROC – 36a	Last Modify Date	Summary of Changes
Version No	1.0	NA	Initial version approved by Board of Directors
	1.01	31/3/2022	Clarified need to report loss of passwords and/or breaches of a user's account immediately. Fixed typos and policy number
Created Date	Dec 2021		