INFORMATION TECHNOLOGY POLICY AND PROCEDURE

Policy Code	STU05
Policy Lead	Chief Executive Officer/Principal
Approving Authority	Board Of Directors
Approval date	01 March 2024
Commencement date	08 March 2024
Next Review Date	March 2027
Version	2024.1
Relevant legislation or external requirements	National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code) (NC: 6.1.5, 6.3, 6.4, 8.22, 11.2.3) Higher Education Standards Framework (Threshold Standards) 2021 (HESFs: 2.1.2, 2.1.3, 3.3.2, 3.3.3, 7.3) Australian Privacy Principles Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act) Privacy and Personal Information Protection Regulation 2014 (2014-549) Privacy Code of Practice (General) 2003 (NSW)
Related ASA Documents	Cyber Security Framework Student Support Framework Business Continuity Policy Business Continuity Plan Critical Incidents Policy Critical Incidents Procedures Critical Incident Plan Diversity and Equity Policy and Procedure Learning Resources Policy and Procedure Privacy Policy and Procedure Records and Information Management Policy and Procedure

1. Purpose

This Policy and Procedure supports the use, management, and support of information technologies (**IT**) at Australian School of Accounting (**ASA**). It recognises the increasingly essential use of information technology by both staff and students. ASA aims to ensure that such usage supports the student learning experience, as well as the administrative and business operations of ASA.

2. Scope

This document applies to all ASA applicants, students, staff, directors, officers, external appointees on any ASA board or committee, volunteers, and contractors.

3. Principles

This Policy is based on the following principles:

- Information technologies will be used in a way that is appropriate and effective in supporting ASA's functions and strategic objectives.
- All students require access to devices during formal teaching and learning sessions and out of hours to complete personal study and complete tasks and assessments.

- Staff and students will be provided with appropriate access, training, and support in the use of supplied technologies.
- Information technologies will be used, secured and appropriately archived with due consideration for privacy and confidentiality and secured in accordance with national and state government privacy regulations and requirements.

4. Definitions

Term	Definition
BYOD	Any electronic device owned, leased, or operated by an employee, contractor, affiliate or student of ASA which is capable of storing data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers and netbooks.
data	Any and all information stored or processed through a BYOD. ASA data refers to data owned, originating from, or processed by ASA systems.
device	Device refers to any electronic equipment that is able to connect to the internet and complete teaching and learning activities. Devices include laptops, tablets and notebooks. Whilst mobile phones can perform some tasks, they do not meet the minimum requirements for study use.
Digital Communication	Digital communication: including social media, emails, the internet, online learning, messaging applications, forums, communication platforms, chats
information technologies	Digital systems and tools enabling information including; Student Management System (SMS), Learning Management System (SMS), Microsoft Office 365 and collaboration tools (SharePoint, OneDrive, Microsoft Teams), ASA Servers/Network Mapping,
Learning Technologies	Digital systems and tools enabling learning and teaching.
Unsupported Technologies	All online and mobile technologies including software, hardware and networks which allow user participation and interaction, which are not supported by ASA's information technology provisions.
Wipe/wiping	A security feature that renders the data stored on a BYOD inaccessible. Wiping may be performed locally or remotely, by a system administrator.

5. Policy Statement

Inclusion of information technologies in academic and business processes and activities will be based on relevance, efficiency, reliability, and effectiveness in achieving stated goals. This document does not prohibit the use of other technologies; however, they may not be supported by ASA's systems or processes.

Access to ASA's information technologies will be subject to any applicable licensing agreements and hosting arrangements and will require appropriate authentication and authorisation of users.

ASA supports information technologies that enhance and support the educational quality of ASA. Students will be supported to access supported technologies to fulfil their needs as a student of ASA. ASA will seek to ensure that no student is disadvantaged by accessibility or connectivity issues and will mitigate this disadvantage where possible.

6. Onboarding and Offboarding

6.1 Training

Initial training is provided at orientation for students, and initially during the induction process for staff.

During Orientation, students will receive initial training on the Learning Management System (LMS), the Student Management System (SMS) and how to access available support if they experience difficulties. Students will receive specific information and assistance in developing skills in course or unit specific technology associated with their field of education.

All students who commence a course in 2024 and onwards will be required to supply their own device to formal teaching and learning sessions. Any device requirements or charges are outlined in the Letter of Offer each student receives prior to accepting a place at ASA. Students will not be required to purchase software that is essential for their course as all required software and applications, or subscriptions will be included in tuition fees. Students who are experiencing difficulties accessing information technology in various forms will be supported as described in the *Student Support Framework*. More information on learning resources is available in ASA's *Learning Resources Policy and Procedure*.

Staff information technology requirements are identified through the *Staff Induction Checklist* which is completed by their direct manager. Staff training will be conducted by relevant staff and overseen by their manager during their induction and probation periods.

6.2 Support

Students are required to meet ASA's entry requirements as outlined in the *Student Admissions Policy* and associated procedure. Students are expected to be able to responsibly, appropriately and effectively use technology tools, systems and hardware, to perform basic functions. Basic functions include the ability to: maintain a functional device and ensure a legal and supported operating system is installed, download and run applications and relevant updates, connect to available networks, such as Wi-fi, and devices as appropriate, and manage their device's battery life.

Students may seek informal support and assistance in their use of information technology through their lecturers or peers. Students are also able to seek assistance before, during, or after class or whilst on campus from Student Experience staff.

It is expected that all staff have appropriate knowledge and understanding of technology as outlined within their relevant Position Description. Staff may seek assistance from their peers or manager for minor support and training assistance.

ASA provides technical assistance and support through an externally contracted company. This support can be accessed via the following avenues:

- IT Support- mail to: servicedesk@asahe.edu.au
- Student Support- mail to: info@asahe.edu.au or call: 1300 672 076

6.3 Access

Staff users will have access to the following devices and systems:

- A dedicated laptop with 2 monitors, a keyboard and mouse. A docking system enables power and connectivity. IT Support must install or uninstall programs where required.
- Staff members who need to use ASA credentials can log into any other devices using their ASA Office365 log in.
- Microsoft Office 365 and collaboration tools (SharePoint, OneDrive, Microsoft Teams).
- ASA Servers / Network Mapping
- Learning Management System (LMS). Initial staff user access, with appropriate access levels, is set up by the Academic team.

- ASA's Student Management System (SMS). Initial staff user access, with appropriate access levels, is managed by the Director of Student Services.

Student users will be set up and trained in the following systems:

- Students should have access to their own device, preferably a laptop rather than a tablet.
- Students may borrow an ASA laptop whilst on campus. A basic Microsoft Office 365 account.
- Access to the Learning Management System (LMS) which is a portal for most learning resources. The Student Experience team sets up student access and provides basic assistance.
- ASA's Student Management System (SMS) which provides grades and allows students updates to personal information. The Student Experience team sets up access and provides basic assistance.

Additional information on learning technologies access can be found in the *Student Handbook* and the *Learning Resources Policy and Procedure.*

6.4 Termination of access

When authorised users leave ASA, their user accounts and access are archived and retired. All staff and student licensed software users are made inactive after leaving ASA.

Staff ceasing employment with ASA are responsible for ensuring that a professional handover is carried out to appropriate staff. This can include; refining documents, categorising and filing emails, and contacting any internal or external correspondents to make them aware that the email address will be retired.

While copies of personal data are acceptable, ASA business documents remain ASA intellectual property. No departing staff member is permitted to take any ASA property in any shape or form; by either physical or digital means or by sending to an unauthorised person.

7. Acceptable Use

7.1 Conduct

Users must behave in a courteous and respectful manner when using information technology. All users of ASA's learning technologies have a responsibility to observe all relevant legislation, standards, and codes with respect to privacy, confidentiality, intellectual property, discrimination, harassment, and defamation, as well as to all relevant policies of ASA. This applies to all information communication technologies, resources, and infrastructure regardless of location. For further information please refer to the *Student Code of Conduct* and *Staff Code of Conduct*.

ASA's guidelines on Generative AI are covered in the *Student Assessment Policy* and *Student Assessment Procedure.*

Users of ASA's facilities, resources, or infrastructure must comply with this document, and all ASA policy suite which details acceptable use. Specific activities that constitute prohibited use include, but are not limited to:

- The corruption, damage, destruction, or suspension of IT facilities, resources, or infrastructure, including, but not limited to
    - actions which deliberately and significantly degrades the performance of IT

facilities, resources, or infrastructure for other users, including the downloading of large files that are not required by ASA,

- introduction or propagation of computer viruses;
- attempts to identify or exploit weaknesses in facilities, resources, or infrastructure;
- unauthorised attempts to make facilities, resources or infrastructure unavailable.

- Impersonation of another individual by the use of their login credentials, email address or other means.
- Attempts to gain unauthorised access or perform actions within ASA or third parties' facilities, resources, or infrastructure with non-authorised goals or outcomes.
- Unauthorised use of data or information obtained from the use of IT facilities.
- Violation of privacy or confidentiality and the unauthorised disclosure of information, regardless of whether this data was obtained legitimately or otherwise.
- Transmission or use of material which infringes copyright or violates software licensing agreements or breach of privacy.
- Any use of IT facilities, resources, or infrastructure to access, create, transmit or solicit material, which is illegal or prohibited by law, obscene, defamatory, discriminatory, or likely to cause distress.
- Use of IT facilities, resources, or infrastructure to harass, threaten other individuals, or transmit unsolicited commercial or advertising material.

8. Monitoring by ASA

ASA will monitor the effectiveness and performance of its information technology facilities, resources, and infrastructure to continually monitor risk. Performance of approved and supported technologies will be monitored and regularly reviewed to ensure they also continue to meet requirements and deliver value. Recommendations for change, improvement or new systems will be data driven and based on the quality, suitability and reliability of systems.

Monitoring of computers, and activities performed on computers, is performed as a part of routine IT practices by ASA's IT Support. ASA reserves the right to monitor content and usage of IT activities within its devices, systems, and network for security and value monitoring. ASA is committed to responding promptly to any potentially damaging publication, including withdrawing services from users and removing any unacceptable materials.

9. Management

9.1 Reporting issues

ASA will take all reasonable steps to ensure reliable and robust IT facilities, resources, and infrastructure. In the event of unscheduled and unforeseen outages, students will not be disadvantaged. Risk management procedures will be in place to minimise service disruption or outages. All information technology issues should be reported to ASA immediately to: servicedesk@asahe.edu.au.

Further information is available within the *Critical Incidents Policy* and associated procedure and plan, and the *Business Continuity Policy* and associated plan.

9.2 Breaches of Conduct

Reporting a breach in the acceptable usage of IT may vary depending on the type of breach or the impact to the affected person(s).

Where a technical breach has occurred that has implications for the business or legal aspects, the CEO may:

- act immediately to prevent any continuation of the alleged breach pending an investigation;
- promptly notify other authorities; and
- advise students or staff of code of conduct policies and direct student or staff to discontinue the breach immediately.

A student may report technical issues to a member of the Student Experience team for initial assistance resolving the issue. This may require escalation to technical support.

Any student may report a more serious breach of acceptable use by requesting an interview with any staff member they feel comfortable speaking with about their complaint. Alternatively, students may submit a complaint form. If a complaint involves a member of Senior Management, students may request a meeting with the CEO by sending an email to principal@asahe.edu.au.

If an investigation of a breach requires students or staff use of IT to be examined or monitored, they will not necessarily be notified.

Allegations that constitute breaches of the law will be referred to an appropriate authority for investigation.

10. Security

10.1 System and Application Backups

ASA's servers and drives are backed up twice per day; saved for thirty days; with a window recovery of sixty (60) days.

ASA's LMS replicates data in near real-time and data is backed up daily. The LMS platform creates daily offsite database backups of data and content including, course content, student submissions, student-created content, analytics, rubrics, learning outcomes, and metadata.

ASA's SMS data and files are backed up every night and multiple backup copies are kept in multiple locations.

ASA's financial data is backed up and protected online, keeping it always available to access when financial staff log in.

10.2 Alerts

Microsoft 365 system alerts are monitored 24/7 and are issued when the following occurs:

- unauthorised system access;
- unplanned system modification; or
- system or physical security intrusion.

10.3 Passwords

ASA passwords are encrypted, and passwords must be changed every ninety (90) days. Staff will receive reminders to change passwords accordingly. Accounts are set to lock after 5 invalid

log-in attempts. Group or shared passwords are not permitted.

10.4 Anti-Virus Software

ASA uses a well-established security software suite that consists of anti-malware, intrusion prevention and firewall features for server and desktop computers. This software is installed and active on all devices and patches are installed and configured as required.

10.5 Network Firewall

ASA has a hardware appliance firewall installed. This is updated weekly and provides:

- Advanced Security, Monitoring, and Management
- Sophisticated Routing Features
- Integrates with UniFi® Controller Software
- Manages the Wi-Fi network from a Single Control Plane
- Data separation via Virtual Local Area Networks (VLAN)
- Remote Firmware Upgrade
- Users and Guests
- Guest Portal/Hotspot Support

10.6 Bring your own Device (BYOD)

ASA students are required to bring their own device to their classes. Outlined below are the procedures relating to the BYOD usage:

- Students are authorised to bring their own device to access or connect to ASA's IT services, data and networks, provided they meet the obligations of this procedure.
- This procedure applies to all users and all devices that connect to the ASA network, other than ASA owned or supported devices.
- Devices which are specifically designed for network access, such as WIFI access points may not be attached to ASA's network infrastructure.
- ASA aims to make ASA 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.
- Students will consult their letter of offer for specific details regarding the technical specifications of their devices for usage at ASA.
- ASA deserves the right to inspect and verify that ASA data has been removed from the device at the end of its use within the ASA environment or when a device is at the end of life.
- ASA may perform a remote wipe of ASA data in order to prevent unauthorised access.
- By choosing to BYOD, the user gives consent for ASA to interrogate such devices to ensure appropriate use, as defined in this policy and procedure.
- ASA is not responsible for any damage or loss that occurs to any personal device.

ABN: 85 617 180 079_TEQSA PROVIDER: PRV14313_CRICOS PROVIDER: 03847F

10.7 Digital CCTV

ASA has full security camera coverage via digital CCTV, with records kept on a regular cycle stored on a network attached storage device. Backup copies are kept on the ASA file server at remote, commercial data centre.

11. Privacy

ASA will take reasonable precautions to ensure that all information technologies are managed securely, protected from misuse, loss, unauthorised access, modification, or disclosure. Further information is contained in the *Privacy Policy and Procedure*.

12. Roles and Responsibilities

The CEO is responsible for all information technology contracts and service agreements.

IT Support will provide a regular report to the CEO for communication to the Board of Directors on IT developments, IT security and IT breaches.

The Academic Dean, or delegate, is required to ensure appropriate facilities, resources and infrastructure is in place to enable quality learning and teaching delivery. An up-to-date list of required technology resources, including hardware, software, and other items, to ensure quality academic delivery must be maintained.

Staff are required to:

- develop and maintain their technological skills appropriately for their role;
- support student access to ensure no student is disadvantaged;

ASA retains the right to impose reasonable penalties or disciplinary action against any staff member for failing to comply with appropriate use of information technologies as per this document and the *Staff Code of Conduct*.

Students are responsible for:

- ensuring they are aware of minimum technology requirements at ASA;
- engaging in the technology-enabled learning environment;
- seeking support, if required, to learn the digital literacy skills associated with information and learning technologies;
- seeking advice if they do not have access to the minimum technology requirements;
- using facilities appropriately, including ensuring material and equipment is treated respectfully, securely and ethically;
- refrain from storing, transmitting or installing any software, or any other material that is not explicitly part of formal teaching activities or work;
- using the Wi-Fi for activities related to study at ASA only; and
- using ASA student emails when communicating with ASA staff.

ASA retains the right to impose reasonable penalties or disciplinary action against any student failing to comply with appropriate use of information technologies as per this document and the *Student Code of Conduct*.

13. Relevant HESFs

This Policy and the associated Procedure comply with the Higher Education Standards Framework (Threshold Standards) 2021. The following are relevant excerpts and specify that:

Standard 2.1 Learning Environment – Facilities and Infrastructure

2. Secure access to electronic information and adequate electronic communication services is available continuously (allowing for reasonable outages for maintenance) to students and staff during periods of authorised access, except for locations and circumstances that are not under the direct control of the provider.
3. The learning environment, whether physical, virtual or blended, and associated learning activities support academic interactions among students outside of formal teaching.\

Standard 3.3 Learning Resources and Educational Support

2. Where learning resources are part of an electronic learning management system, all users have timely access to the system and training is available in use of the system.
3. Access to learning resources does not present unexpected barriers, costs or technology requirements for students, including for students with special needs and those who study off campus

Standard 7.3 Information Management

3. Information systems and records are maintained, securely and confidentially as necessary to:
    a. maintain accurate and up-to-date records of enrolments, progression, completions and award of qualifications
    b. prevent unauthorised or fraudulent access to private or sensitive information, including information where unauthorised access may compromise academic or research integrity
    c. document and record responses to formal complaints, allegations of misconduct, breaches of academic or research integrity and critical incidents, and
    d. demonstrate compliance with the Higher Education Standards Framework.

14. Version Control

This Policy and Procedure has been reviewed and approved by the Australian School of Accounting Board of Directors as at December 2023 and is reviewed every three years.

This Policy and the Procedure, is published and available on the Australian School of Accounting website https://www.asahe.edu.au/policies-and-forms/.

Change and Version Control				
Version	**Authored by**	**Brief Description of the changes**	**Date Approved:**	**Effective Date:**
2024.1	Director Learning and Innovation	Updated BYOD information.	01/03/2024	08/03/2024
2023.1	Project Officer	Updated policy to include expanded content on information technologies, HESFs references, changes in regulatory compliances. Benchmarked against 6 other Higher Education Providers.	12/12/2023	18/12/2023
Previous version archived. New Policy code and numbering system implemented.				
3.0		Annual review – BoD approval	06/07/2021	
2.0		New course accreditation		

1.0		Council approval		