ACCEPTABLE USE OF INFORMATION TECHNOLOGY (IT) FACILITIES POLICY AND GUIDELINES FOR STUDENTS

Purpose

AIB provides Information Technology facilities (IT facilities) to support its teaching and learning, Research, administrative and business activities. IT facilities includes all computing and communication equipment, software, services, data and dedicated building space used in connection with information technology, which is owned by, leased by or used under licence or agreement by AIB.

AIB recognises its responsibility to ensure the appropriate use of its IT facilities and that it must be protected from damage or liability resulting from the unlawful or inappropriate use of its IT facilities. Users of AIB IT facilities are responsible for adhering to the provisions of this policy and guidelines.

Scope

This policy applies to AIB current and prospective students accessing software applications, systems, facilities, or services provided by AIB. This includes, but is not limited to:

- Authorised personnel, including:
    - Students with access to an authorised accounts (as defined below in section 1).

- Unauthorised personnel, including:
    - Recognised affiliates
    - Members of the public

Definitions

Unless otherwise defined in this document, all capitalised terms are defined in the glossary.

Policy

1. Authorised Personnel

1.1. It is a requirement that every person who accesses AIB IT facilities must be authorised to do so.

1.2. Authorisation to access a service is recognised through users being granted access through user accounts, created, and managed by the AIB Technology Team. Any account information provided is for the exclusive use of the new user.

1.3. It is prohibited for any user to create new user accounts in any system they are provided access to.

1.4. Users must provide evidence of their eligibility to use AIB's IT facilities, on request from the Academic Dean, Chief Executive Officer, or the Technology Director. Such evidence may be written approval such as an email, contract, or account confirmation.

1.5. All user accounts created within this process are reviewed as part of the periodic review. User accounts not actively used in systems will be disabled, to reduce the surface area of any potential cybersecurity attack. Users are not notified of their account being disabled and will need to raise an Student Support ticket to have their access reinstated.

1.6. All users with an authorised account must comply with this policy and guidelines when using AIB's IT facilities.

2. Users of AIB public sites and social media

2.1. AIB provides IT facilities for the use of members of the general public who do not have any formal relationship with AIB. Examples of such facilities are AIB websites are the marketing website and social media feeds.

2.2. These users will not be issued with user accounts and will only be subject to sections 3.3 and 3.5 of this policy. In addition, their use of AIB IT facilities must comply with State and Commonwealth laws and any additional guidelines issued by AIB in relation to their use of the facilities.

3. Acceptable Use

3.1. IT facilities are provided to support AIB's teaching and learning, Research, administrative and business activities.

3.2. IT facilities are not provided for recreational or personal use unless specifically stated in the guidelines.

3.3. Users of AIB IT facilities must comply with AIB's requirements for acceptable use. Specific activities that constitute acceptable use include, but are not limited to:

(a) Information security

i) Ensuring that the confidentiality and privacy of data within AIB systems is maintained.

ii) Being responsible for the safekeeping of the data they access as a condition of being granted access to use AIB’s information systems.

iii) Ensuring bulk data exports and imports are not undertaken in any AIB system, unless written approval from the Chief Executive Officer or Technology Director is provided.

iv) Reporting of any breach of security immediately to the Student Central team at studentcentral@aib.edu.au.

v) Being aware that the unauthorised release or use of data inadvertently obtained may lead to legal action.

(b) Facilities security

i) Ensuring the security of their computer or device by logging off or locking their device when it is left unattended.

ii) Ensuring any services provided by AIB are primarily utilised for AIB's teaching and learning, research, administrative and business activities, and that any personal use unrelated to study is limited, reasonable and appropriate and must not:

A. Contravene AIB policy or State and Commonwealth laws.

B. Interfere with official use of IT facilities, or

C. Interfere with a student's obligations to AIB.

iv) Seeking advice from the Student Central team if they have doubt concerning their authorisation to use any technology service or about whether a particular use is acceptable.

(c) Announcements and communications

i) Only sending general messages to public groups, news groups, or specific work groups for the purposes of your educational studies, unless the forum is specifically provided for general communication.

ii) Only sending messages that are of a professional manner, and don’t contravene any of the requirements of this policy.

iii) Always communicating in compliance with the provisions of the Spam Act and Privacy Act.

3.4. Specific activities that constitute unacceptable use include, but are not limited to:

(a) Security violations

(i) Deliberate, unauthorised access to IT facilities.

(ii) Unauthorised attempts to identify or exploit weaknesses in IT facilities.

(iii) Deliberate impersonation of another individual using their login credentials, e-mail address or other means, without written consent of the Chief Executive Officer or the Technology Director.

(iv) Handling passwords incorrectly, including:

A. Sharing password or MFA response codes with others.

B. Sharing passwords in communications applications, such as email, messaging, or chat applications.

C. Storing usernames and passwords in text files, documents or note applications.

(b) Facility violations

(i) Deliberate, unauthorised corruption or destruction of IT facilities (including deliberate introduction or propagation of computer viruses).

(ii) Deliberate, unauthorised corruption or destruction of data in any system.

(iii) Unauthorised attempts to make AIB IT facilities unavailable.

(iv) Use of AIB IT facilities to gain unauthorised access to third party services.

(v) Use of AIB IT facilities in unauthorised attempts to make third party services unavailable.

(vi) Use which deliberately and significantly degrades the performance of AIB IT facilities for other users.

(vii) Behaviour acting in a manner which, in the opinion of the Chief Executive Officer or the Technology Director, causes or is likely to cause damage to AIB IT facilities.

(c) Software violations

(i) Make use of, or copy, software contrary to the provisions of any licensing agreement entered into by AIB. The onus is on students to consult with

Student Central to clarify the permitted terms of use if they wish to use any software for purposes other than those for which AIB has a licence.

(d) Service violations

(i) Sign up on behalf of AIB for any SaaS, without written consent of the Chief Executive Officer or the Technology Director.

(ii) Continual use of SaaS offerings that have been deemed to no longer meet the cybersecurity requirements of AIB, and for which students have been notified of discontinued use.

(e) Information violations

(i) Unauthorised use of data or information obtained from the use of IT facilities.

(ii) Any use of material provided to you from AIB or via the Learning Portal except for the purpose of your own research or study or with the express permission of the copyright owner. Note you need to attribute the author of material you copy. Refer to the AIB Copyright Policy and the AIB Style Guide for referencing material used in research or study.

(iii) Make use of, disseminate or copy, intellectual property provided by AIB outside of its defined intent, either in communications or published as learning materials, except with the express permission of the Academic Dean, Chief Executive Officer or the Technology Director.

(iv) Storing of any data or documents owned by AIB in any SaaS environment, or sharing information from any SaaS environment, where AIB does not have management access.

(v) Unauthorised disclosure of confidential information a user may have access to.

(f) Personal violations

(i) Violation of the privacy of personal information relating to other individuals.

(ii) Use of IT facilities to harass, threaten, bully or otherwise engage in unwelcome actions towards another individual(s).

(iii) Use of IT facilities to access, create, 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 teaching and learning or research (if the material is a legitimate part of teaching and learning or research, an appropriate warning should be given).

(g) Identity and representation violations

(i) Represent themselves, in messages or otherwise, as someone else, fictional, or real, without providing their real identity or username.

(ii) Give the impression that the writer is representing, giving opinions, or making statements on behalf of AIB via communications, unless appropriately authorised to do so.

(iii) Use of IT facilities to transmit commercial or advertising material on behalf of a person or business other than AIB, or otherwise benefit a business other than AIB.

3.5. Users must also comply with AIB's other policies and procedures, and other guidelines as released on the AIB website.

3.6. If any unacceptable use of AIB IT systems is detected, it must be reported to Student Central. Students can report suspected unacceptable use of AIB IT systems via the quality@aib.edu.au email address.

3.7. Behaviour which breaches this policy may also breach Commonwealth and State law.

4. User Accounts and Passwords

4.1. Users of AIB IT facilities must ensure they comply with AIB's requirements for accessing and securing user accounts. Specific activities that constitute acceptable use include, but are not limited to:

(a) User accounts having one person nominated as the person responsible for that account.

(b) Users selecting passwords that cannot be easily guessed, ensuring they are complex and adhere to the password criteria required by the system being used.

(c) Changing a password immediately if the security of a password has compromised.

(d) Changing their passwords every 90 days.

4.2. Specific activities that constitute unacceptable use include, but are not limited to:

(a) Attempting to determine another user's password.

(b) Permitting others to login to an account provided for your use.

(c) Divulging passwords for any account to others.

(d) Use of student email addresses to sign up for personal service accounts on the internet, such as social media.

4.3. Users are responsible for all activity initiated from their accounts, unless it is established that the activity was done by a third party who gained access to the user's account through no fault of the user.

5. Email Communication

5.1 Users of AIB IT facilities must ensure they comply with AIB's requirements for managing email accounts to mitigate the ongoing cyber risk profile. Specific activities that constitute acceptable use include, but are not limited to:

(a) Proactive assessment of emails before interaction to ensure that phishing email links are not clicked on, and personal details are not provided to attackers.

(b) Relinquishing access to the mailbox without deleting all historic emails, so that it can be archived by AIB at the end of the engagement.

6. AIB Responsibility

6.1 AIB will take reasonable steps to maintain and secure its IT facilities and protect its IT facilities from unauthorised and unacceptable use.

7. Monitoring Use

7.1 AIB reserves the right to monitor any and all aspects of its IT facilities to determine if a user is acting unlawfully or violating this policy, the associated documents listed this policy.

7.2 Such monitoring may include, but is not limited to, individual login sessions, the internet sites visited by users and the content of electronic communications.

7.3 Monitoring may be done with or without prior notice to the user. Procedures relating to monitoring use are listed in Appendix A.

8. Enforcement

9.1. Users of AIB IT facilities are responsible for adhering to the provisions of this policy and guidelines.

9.2. AIB may take remedial action and suspend user access with or without prior notice in response to suspected breaches of this policy or guidelines.

9.3. Breaches by students that constitute misconduct will be addressed by the relevant student disciplinary procedures. See the **Related Policies and Procedures** section.

9.4. Sanctions for failing to comply with this policy and guidelines or the associated forms/policies, may include:

(a) Immediate withdrawal of access to IT facilities, with or without prior notice;
(b) Action taken under AIB's relevant disciplinary procedures for students;
(c) Criminal or other penalties imposed by State or Commonwealth legislation;
(d) Financial compensation sought by AIB.

8.5 Allegations that constitute misconduct or breaches of the law will be referred to the appropriate authority for investigation. AIB will give that authority all reasonable assistance requested, including disclosing:

(a) Relevant financial and personal data which may be held by AIB.
(b) Data which may be limited by contractual obligation including copyrighted software and software that is patented or which contains trade secrets.

9. Exceptions

9.1. Requests for exceptions to this policy must be authorised by the Chief Executive Officer or the Technology Director. Such requests must be made in writing to AIB (quality@aib.edu.au) and will be evaluated based on the case, and supporting evidence/documentation, presented to support it.

10. Implementation and Review

10.1. The Chief Executive Officer and the Technology Director have authority to amend this policy and any guidelines issued.

11. Communication

11.1. This policy will be published and available on the AIB Website for all students to access and review.

Related Policies and Procedures:

Academic Integrity Policy and Procedure
Copyright Policy and Procedure
Privacy Policy and Procedure
Records Management Policy and Procedure

Student Code of Conduct Policy
Student Complaints, Grievances and Appeals Policy and Procedure

Responsibility:

Technology Director

Related Legislation:

While not an exhaustive list, the following Commonwealth legislative instruments are of particular relevance to the use of AIB IT facilities:

The Copyright Act (1968)
The Crimes Act (1914)
The Criminal Code Act (1995)
The Cybercrime Act (2001)
The Spam Act (2003)
The Privacy Act (1988)

Current Status:	**Version 2**
Approved By:	Executive Committee
Effective From:	**31 January 2024**
Date of Approval:	31 January 2024
Previous Versions:	3 September 2020 4 June 2020 21 May 2018
Date of Next Review:	31 January 2027

APPENDIX A – GUIDELINES FOR STUDENTS: USE OF IT FACILITIES

1. Copyright Legislation

1.1 Copyright law restricts the copying of software and other material subject to copyright (documents, emails, music, broadcasts, videos etc.) except with the express permission of the copyright owner. (The copyright of an email is owned by the sender, or the sender's employer.)

Refer to the AIB Copyright Policy for more details.

1.2 Email and Copyright: The copyright of an email message is owned by the sender, or the sender's employer. Copyright owners have a variety of rights, including the right to reproduce their work and the right of communication to the public. Forwarding something to an email discussion list would be construed as 'to the public'. Consider the expectations of the originator:

(a) Did that person set any conditions on the further communication of their email?
(b) Expect that it would not be forwarded to anyone else; or
(c) Would not be forwarded to a particular recipient?

2. Privacy Legislation

2.1 A member of staff may expect some privacy in relation to their use of the computer and email and internet resources AIB makes available to them at work. Despite the use of individual passwords, privacy is limited in the following ways:

(a) Use of computers, email and the internet as well as data on internet sites visited, downloads made and emails sent/received, can be accessed by IT administrators.
(b) It is possible to retrieve deleted records from back-ups and archives.

2.2 Besides technological limitations on privacy, there are other factors that can impinge on privacy. The Office of the Privacy Commissioner provides information on the privacy legislation and how it applies to use of IT by employees. It shows that there are exemptions to the Privacy Principles and an employer's logging of staff activities (email and internet) is not contrary to the legislation as long as it is done lawfully and fairly.

To ensure fairness, AIB has provided these guidelines to inform staff about its practice of monitoring and accessing records relating to the use of AIB IT facilities, including computers, email and the internet.

2.3 For information on how AIB protects the privacy of information it holds in relation to its students, see the Records Management Policy and Procedure.

2.4 AIB also informs members of the public about how AIB monitors their use of AIB website. Refer to the AIB Privacy Policy.

3. Freedom of Information Act

3.1 Under the Freedom of Information (FOI) Act of South Australia, a document is defined as "anything in which information is stored or from which information may be reproduced". Email messages created in the course of fulfilling duties relating to employment are official records covered by the State Records Act (1997) and the Freedom of Information Act (1991) and are subject to the same requirements as hard copy records. The content of these emails remains the property of AIB and may be subject to release in accordance with the FOI Act.

4. Spam Act 2003

4.1 All email messages sent from a AIB email account must comply with the Spam Act 2003. This Act dictates the regulation of commercial e-mail and other types of commercial electronic messages.

4.2 The Spam Act makes allowance for AIB, which is classified as an "educational institution", to send email messages to currently enrolled students about its goods or services. Therefore, any unsubscribe requests are not adhered to until the student withdraws from or completes the course.

4.3 Other electronic messaging, including emails, instant messaging, SMS, and other mobile phone messaging may be identified as spam if it does not fall into this category.