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 include 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.

Scope

This Policy applies to AIB students or prospective students accessing AIB's IT facilities (users):

(a) with authorised accounts (as defined below) and

(b) whether they are using a. AIB provided computing device, a personally owned computing device or a third party owned computing device (such as might be found in a public library or internet cafe).

Definitions

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

Details

1. Users with Authorised Accounts

1.1 It is a requirement that every person who accesses AIB IT facilities must have an authorised user account for their exclusive use. The user account will be provided to students by AIB.

1.2 Authorised accounts will only be issued to currently enrolled students, or other recognised affiliates of AIB. In addition, access to particular systems and types of use may require authorisation by the relevant Head of Department.

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

2. Other Users

2.1 This policy recognises that some AIB IT facilities are provided for the use of members of the general public who do not have any formal relationship with AIB. Examples of such facilities are AIB web sites that are not subject to some form of access control, and limited access to the electronic information resources accessible from the Library where this is permitted by license.

2.2 These users will not be issued with user accounts, and will only be subject to sections 3.3 and 3.4 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 otherwise in the guidelines in Appendix A.

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

(a) deliberate, unauthorised corruption or destruction of IT facilities (including deliberate introduction or propagation of computer viruses)
(b) deliberate, unauthorised access to IT facilities
(c) unauthorised use of data or information obtained from the use of IT facilities
(d) 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)
(e) transmission or use of material which infringes copyright held by another person or AIB
(f) violation of software licensing agreements
(g) use of IT facilities to transmit unsolicited commercial or advertising material
(h) deliberate impersonation of another individual by the use of their login credentials, e-mail address or other means
(i) violation of the privacy of personal information relating to other individuals
(j) unauthorised disclosure of confidential information
(k) use of IT facilities to harass, threaten or otherwise engage in unwelcome attention towards other individuals
(l) unauthorised attempts to identify or exploit weaknesses in IT facilities
(m) unauthorised attempts to make AIB IT facilities unavailable
(n) use of AIB IT facilities to gain unauthorised access to third party IT facilities
(o) use of AIB IT facilities in unauthorised attempts to make third party IT facilities unavailable
(p) use which deliberately and significantly degrades the performance of IT facilities for other users (including the downloading of large video files not related to teaching and learning and research).

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

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

3.6 Behaviour which breaches this policy may also breach Commonwealth and State law. All Users must comply with all relevant State, Federal and International law as well as AIB policy, procedures and guidelines.

4. User Accounts and Passwords

4.1 All user accounts must have one person nominated as the person responsible for that account.

4.2 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.

4.3 Users must select passwords that cannot be easily guessed and they must not divulge passwords to others, including AIB staff and students.

4.4 Passwords must be a minimum of 8 characters in length, using a mixture of numbers and upper case and lower case letters.
4.5 Users must not attempt to determine another user's password.
4.6 If the security of a password is compromised, it must be changed immediately.
4.7 Users are recommended to change their account passwords every 90 days.
4.8 Users are not permitted to authorise others to login using their account.
4.9 Users are prohibited from using another user's account.

5. AIB Responsibility

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

6. Monitoring Use

6.1 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, or any other AIB policy or rule. Such monitoring may include, but is not limited to, individual login sessions, the internet sites visited by users and the content of electronic communications. Monitoring may be done with or without prior notice to the user. Procedures relating to monitoring use are listed in Appendix A.

7. Compliance

7.1 Users of AIB IT facilities are responsible for adhering to the provisions of this policy and guidelines.
7.2 AIB may take remedial action and suspend user access with or without prior notice in response to suspected breaches of this policy or guidelines.
7.3 Breaches by students that constitute misconduct will be addressed by the relevant staff and student disciplinary procedures. AIB will identify the most appropriate AIB policy applicable which may be the Student Misconduct and Discipline Policy or Academic Integrity policy.
7.4 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. Exceptions

8.1 Requests for exceptions to this policy must be authorised by the Chief Executive Officer or the Chief Financial Officer. 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.

9. Implementation and Review

9.1 All Heads of Department or equivalent will be responsible for the dissemination of this policy and guidelines in their respective areas of responsibility.
9.2 The Chief Executive Officer and the Chief Financial Officer have authority to amend this policy and any guidelines issued.

9.3 Both the Guidelines referred to in Related Forms and any additional Guidelines are afforded the status of policy.

10. Communication

10.1 All students have access to this Policy through the AIB website

Related Policies:

Academic Integrity policy
Academic and Non-Academic Grievance Handling Policy
Copyright Policy
Privacy Policy
Student Misconduct and Discipline Policy

Responsibility:

IT Infrastructure Manager

Related Legislation

While not an exhaustive list, the following legislation is of particular relevance to the use of AIB IT facilities:
The Commonwealth Copyright Act (1968)
The Commonwealth Crimes Act (1914)
The Commonwealth Criminal Code Act (1995)
The Commonwealth Cybercrime Act (2001)
The Commonwealth Spam Act (2003)

Current Status:	**Version 1**
Approved By:	Board of Directors
Date of Approval:	21 May 2018
Date of Next Review:	21 May 2020

APPENDIX A- GUIDELINES FOR STUDENTS: USE OF IT FACILITIES INCLUDING EMAIL AND THE INTERNET

Terms of Use

These guidelines are issued by the IT Infrastructure Manager under the authority of the AIB Board of Directors and provide clarification on the practical application of AIB's Policy on Acceptable use of Information Technology (IT) facilities.

Scope

These guidelines apply to all AIB students and the use of all IT facilities including but not limited to email, the internet and AIB Learning Portal.

Definitions

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

Details

1. Student Conduct

1.1. Students should

(a) seek the advice of Student Support if they are in doubt concerning their authorisation to use any IT facility or about whether a particular use is acceptable

(b) use, or copy, software consistent with the relevant licensing agreement and check with Student Support if in doubt

(c) respect copyright and always use or transmit information in a way that does not infringe copyright

(d) ensure that they maintain confidentiality and privacy of data

(e) choose a secure password and keep their user name and password safe

(f) report any misuse or breach of data or physical security, as soon as possible, to Student Support

(g) communicate respectfully when engaging in forum discussions and other activities on the AIB Learning Portal

(h) respect others and not unduly inconvenience other people, through excessive use of IT facilities.

1.2. Students should not:

(a) transmit information or materials (including but not limited to email or on the AIB Learning Portal) that:

(i) contain discriminating or sexually harassing content

(ii) could create an intimidating or hostile work environment for others

(iii) are designed to cause harm to organisations with which AIB has commercial relationships

(iv) are, or contain, chain letters

(v) contain unsolicited personal opinions on social, political, religious or other non-AIB related matters, where sending such opinions is not a legitimate part of study.

(b) use, or attempt to use, another person's username, password or mailbox without authorisation

(c) forge emails or any other type of electronic correspondence

(d) use another's identity or conceal or misrepresent their name or affiliation or address

(e) use AIB facilities to make personal profit from commercial activities or to buy or sell goods or services

(f) install software on any AIB IT facility

(g) seek access to data not required as part of their study
(h) save passwords electronically within applications
(i) attempt to circumvent system security provisions
(j) visit, download, store or transmit materials that are pornographic, profane or offensive.

2. Copyright

2.1 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.

3. Privacy

3.1. Privacy is limited in the following ways:
(a) use of computers, email and the internet as well as data on AIB 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. For further information refer to the AIB Privacy Policy.

4. Freedom of Information

4.1 Email and other electronic messages created in the course of studying may be official records covered by the State Records Act (1997) and the Freedom of Information Act (1991). The content of these messages remains the property of AIB and may be subject to release in accordance with the FOI Act.

5. Alleged Misuse

5.1. Where an alleged misuse has been reported, the Chief Financial Officer may:
(a) act immediately to prevent any continuation of the alleged misuse pending an investigation
(b) promptly notify other authorities
(c) advise the student of the Acceptable Use of IT Facilities policy and direct the student to discontinue the alleged misuse immediately.

5.2. If an investigation of alleged misuse requires a student's use of IT facilities to be examined or monitored they will not necessarily be notified.

5.3. Allegations that constitute 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; and
(b) data which may be limited by contractual obligation including copyrighted software and software that is patented or which contains trade secrets.

6. Monitoring

6.1. Routine monitoring of the use of IT facilities is conducted to monitor the costs and acceptable use of AIB resources.

6.2. In normal circumstances, AIB and third party staff supporting IT services will not monitor the contents of electronic mail messages or other communications or files they access as a result of their work (e.g. auditing operations). However, AIB and third party staff supporting IT services

will inspect, copy, store and disclose the contents of email when appropriate to prevent or correct improper use, satisfy a legal obligation, or to ensure proper operation of IT facilities.