

## **Internet Policies**

### **Purpose:**

To ensure that users of the Australian Institute of Business (AIB) internet system and IT provided to staff, faculty and students are aware of their responsibilities in the appropriate use of those facilities in compliance with general law and normal standards of good behaviour.

### **Scope:**

This policy applies to all users of AIB Internet resources, whether on campus or from remote locations.

### **Detail:**

The IT resources of AIB are provided for, and intended to be used for, AIB purposes, not for personal or non- AIB-related activities or purposes. Users are expected to use them accordingly.

‘AIB purposes’ are those purposes in furtherance of the AIB's teaching and learning, research, community engagement and commercial activities, and the technical and administrative activities which support them.

Users of the AIB IT resources must comply with all Commonwealth and State government civil and criminal laws; all AIB policies; and all relevant contracts and licences. Examples of such laws, rules, policies, contracts, and licences include, but are not limited to:

- Commonwealth and State laws covering defamation, privacy, freedom of information, censorship, copyright, trademark, offensive material, pornography and spam;
- Commonwealth and State IT-specific criminal laws, which prohibit hacking, spreading viruses, unauthorised use and a range of other IT-related activities;
- the AIB's policies on academic integrity, sexual harassment, racism, bullying and equal opportunity;
- the AIB's policy on access to Student Personal Information;
- the AIB's policy on Media Statements; and
- all applicable software licences.

Users of the AIB IT resources must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected; and not divulge confidential data except where required by the law or AIB policies.

Ability to access other persons' accounts does not, by itself, imply authorisation to do so. Users are responsible for ascertaining what authorisations are necessary and for obtaining them before proceeding.

Users of The AIB IT resources must respect the finite capacity and cost of IT resources and avoid consuming an unreasonable amount of those resources or interfering unreasonably with the activity of other users.

Communications made by means of the AIB IT resources are deemed official documents that are subject to the same laws as any other form of correspondence.

Email sent from AIB IT resources is, like the more traditional letterhead, readily identifiable as being from AIB. Please view the separate policy on emails.

Webpages are also an important tool supporting the AIB's core activities of education and research. Consistency of design and structure is important in enhancing AIB's reputation, and so users involved in producing AIB webpages are expected to follow approved standards of formatting and design as set out in the AIB Marketing and Community Relations Policies.

Users breaching this policy may be warned or have their access to AIB IT resources denied or restricted by the Compliance Officer. Before taking such action, the Compliance Officer must make such inquiries as they see fit to be satisfied that a breach has occurred, and must give the user the opportunity to be heard.

Breaches which are persistent (as defined by a third or subsequent breach) or deemed by the Compliance Officer to be serious (eg to have the potential to impact on the rights or safety of other users, or on the integrity, security or functionality of the AIB IT resources) will normally be handled through the relevant disciplinary procedures for staff and students.

In addition to imposing any penalty or disciplinary action, AIB may take action to recover from an individual the costs associated with any damage to or loss of IT resources or data caused by that individual through the deliberate breach of this policy.

AIB may remove material from websites or computers, or suspend or block access to an account, or take other forms of action, at any time when it reasonably appears necessary to do so in order to protect the rights and safety of others, or to protect the integrity, security, or functionality of the AIB or other IT resources, or to protect AIB from liability.

Authority to exercise this power resides with the Chief Executive and their delegate.

Users should be aware that their uses of AIB IT resources are not completely private. While individual usage of AIB IT resources is not routinely monitored, the normal operation and maintenance of IT resources may require:

- system backups, which may access all files in an individual's account
- software upgrades which may require editing startup files in an account
- diagnostic and troubleshooting activities
- the backup and caching of data and communications
- the logging of activity
- the monitoring of general usage patterns
- the scanning of systems and network ports for anomalies and vulnerabilities, and
- other such activities that are necessary to provide IT services.

**Related Forms:**

Nil

**Responsibility:**

Compliance Officer

**Related Policies:**

Student Personal Information

**Current Status**

**version 2**

Approved By:

Board of Directors

Date of Approval:

1 July 2011

Previous version:

27 October 2008