



Records Management

Policy

Australian Institute of Business Pty Ltd (“AIB”) has policies to ensure the integrity of all records and continuously reviews the policies and procedures to improve our systems and procedures.

Purpose:

To ensure that all Records are kept appropriately and in accordance with the applicable laws, in particular the Privacy Act 1988 (Cth), Tertiary Education Quality and Standards Agency Act 2011 (Cth) and Corporations Act 2001 (Cth).

Definitions:

The following definitions apply for the purpose of this policy, unless the context otherwise requires:

- (a) “Records” mean AIB’s written records (both electronic and hardcopy), which include without limitation, Staff Records, Student Records, Financial Records, marketing materials, articulation agreements, minutes of meetings and administrative records created in the conduct of the business of AIB, but does not include working papers or rough drafts of documents unless the sequence of amendment is of importance.
- (b) “Staff Records” mean AIB’s employees’ records and personnel files, such as:
 - (i) Files maintained by HR;
 - (ii) Curricula vitae;
 - (iii) Contracts of employment;
 - (iv) Transcripts of qualifications;
 - (v) Employment declarations; and
 - (vi) Leave entitlements.
- (c) “Student Records” mean AIB’s records of its students, such as:
 - (i) Application documents;
 - (ii) Consents;
 - (iii) Interactions with AIB;
 - (iv) Assessment items; and
 - (v) Student information such as:
 - (A) Student personal information, including sensitive information, as defined under the Privacy Act 1988 (Cth);
 - (B) Course enrollments;
 - (C) Fees paid;
 - (D) Progression;

- (E) Assessments;
- (F) Completions;
- (G) Award of qualifications; and
- (H) Other courses undertaken.

- (d) "Financial Records" mean AIB's:
 - (i) Financial records showing income and expenditure, budgets, projections;
 - (ii) Bank statements;
 - (iii) Receipts, purchase and procurement documentation; and
 - (iv) Insurance policies.

Confidentiality and storage

All Records must be handled in accordance with the [Confidentiality Policy](#) with confidential information stored in a secure manner, as follows:

- (a) if it is in a material form, it must be kept in a locked, secure area; and
- (b) if it is in electronic form, it must be accessible only by password

For example the following Records are to be stored in a secure manner:

- (a) student records;
- (b) financial records;
- (c) employment files; and
- (d) parchment forms.

Documents created or received by an officer or consultant of AIB in the course of performing their duties are official AIB Records and must be incorporated into the AIB records management system.

Archival of Records

- (a) All Records that are to be archived must be archived as follows
 - (i) if it is in a material form, it must be archived in a lockable, vermin free and weathertight room, and appropriately marked for easy retrieval; and
 - (ii) if it is in an electronic form, it must be archived in enterprise grade computer data storage facility with a physically separate backup.
- (b) Records are to be retained for the greater of seven years or statutory or regulatory requirements. Notwithstanding this, Students' official results are to be retained for a minimum of 30 years from their respective graduations.

Privacy

- (a) Any collection, use, disclosure, handling and storage of and access to the Records must be in accordance with AIB's [Privacy Policy](#) and [Confidentiality Policy](#).
- (b) Only relevant staff may access the Records and such access is to be limited to only those Records which are directly relevant to their specific roles.
- (c) At their induction and at regular intervals, staff are to be reminded of the need to maintain the privacy and confidentiality of the student information and never to discuss their work with anyone outside their team.

Version Control

When new policies, procedures, documents and training packages are introduced, the relevant physical or electronic file is to be updated with these new documents and the superseded documents are removed and archived. The appropriate staff are to be informed of the new versions that are to be used.

Related Forms:

Nil

Responsibility:

Chief Information Officer

Related Policies:

Confidentiality

Privacy

Policy Development and Amendment

Current Status

Approved By:

Date of Approval:

Previous version:

Version 3

Board of Directors

24 November 2016

1 July 2011

27 October 2008