



Records Management

Policy

Australian Institute of Business (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 appropriately and in accordance with all Commonwealth and State legislation.

Definitions:

The following definitions apply for the purpose of this policy.

Records includes

staff records, student electronic 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. 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.

Staff records means

Personnel files maintained in hard copy in a locked cabinet. These files include:

- Curriculum Vitae
- Contract of Employment;
- Transcripts of Qualifications;
- Employment Declaration; and
- Annual and sick leave taken.

Student electronic records means

The electronic database for student records, for items such as:

- Student personal details;
- Course enrolled;
- Fees paid;
- Attendance;
- Assessments;

- Issuance of qualifications;
- Other courses undertaken

Student Records means

- Examination scripts
- Application Forms
- Consents
- Assignments in hard copy

Financial Records means (whether in hard copy or electronic form)

- AIB Financial records showing income and expenditure, budgets, projections
- AIB Bank statements
- AIB Receipts, purchase and procurement documentation

Security Measures

All records are stored securely by the respective Departments, for example

- student files are kept in locked cabinets by Student Support Services;
- financial records are kept in locked cabinets by the Finance Officer; and
- Staff files and parchment forms are kept under lock and key by the Registrar.

Computer Protection

- All computers are adequately password-protected.
- The AIB server is backed up on a daily basis and the back up is securely stored off site.

Archival Information

- All archival information is stored in the strong room and appropriately marked for easy access.
- A list of archived boxes and the files contained is stored in paper copy as well as in soft copy.
- The student results are retained in soft and hard copy and will be retained for a period of 30 years from graduation.

Privacy

Only relevant staff is allowed access to student records. At their induction and at regular intervals, they are reminded of the need to maintain the confidentiality of the student information and never to discuss their work with anyone outside their team.

Client Access

- Clients may have access to their own records on request
- Client records will not be released to a third party unless written authorisation is received from the client.

Version Control

When new policies, procedures, documents and VET training packages are introduced, the relevant Master file is updated with these new documents and the superseded documents are removed. Electronically, the newest version is labeled with the relevant

version number and the superseded document is transferred into the superseded file. That way, only the current version is available readily. The appropriate staff is advised and the new versions are used.

Insurance

Insurance policies are held for:

- Contents (fire, theft, etc.) and Public Liability
- Motor Vehicles
- Professional Indemnity
- Tax Probe (in the event of an audit by the Tax Department) and Legal Expense (in the event a legal action is brought against Gibaran).

The type and amount of cover is reviewed annually to make sure that we are correctly insured.

Related Forms:

Nil

Responsibility:

Student Support Services
Finance Officer
Registrar

Related Policies:

Confidentiality
Student Personal Information

Current Status	Version 2
Approved By:	Board of Directors
Date of Approval:	1 July 2011
Previous version:	27 October 2008