

Records Management Procedure

Governing Policy

Records Management Policy

Purpose

This procedure provides guidance on how AIB creates, accesses and maintains the Records.

Definitions

Unless otherwise defined in this document, all capitalised terms are defined in the [glossary](#).

Procedure

1. Recordkeeping systems

- 1.1. AIB uses the following main record management systems that are fit for specific business purpose including but not limited to:
 - Student Management system;
 - Student Learning system;
 - Financial and payroll system;
 - CRM system;
 - SharePoint;
 - HR system.
- 1.2. Users of each record management system are responsible for creating the Records, maintaining the Records and ensuring accuracy of the information entered in the appropriate system.

2. Creation and capture

- 2.1. Records are created when information in any format is created, received or maintained by an officer or consultant of AIB in the course of performing their duties.
- 2.2. Records must be captured in compliant recordkeeping and appropriate business system. This includes hard and soft copy Records as well as audio and video records.
- 2.3. Records identified as confidential information will be captured and stored in accordance with the Privacy Policy and Policy on Intellectual Property and Confidentiality Policy, 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 to authorised AIB staff.

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

- Student Records;
- Financial Records;
- Employment files; and
- Parchment forms.

2.4. AIB will keep its Records in electronic format unless they are not available or there is a legislative requirement to keep hard copy Records.

3. Accessibility of records

3.1. The sensitivity and value of Records will be assessed at the time of creation or receipt of a record, so that appropriate arrangements are made for their accessibility and security.

3.2. Records will be stored in a way that they are locatable and accessible only to authorised staff.

3.3. Staff and students require a username and a personal password to access AIB's record management systems that are applicable to their functions.

3.4. Access for staff is granted on the basis of the assessment against duties outlined in their job description.

3.5. AIB will maintain an internal schedule outlining staff access to Student Records.

3.6. Current and former students will have access to their own records in accordance with AIB's Privacy Policy.

3.7. Current students will have access to their subject outcomes through the Student Learning Portal, unless they have an administrative encumbrance denying them access.

3.8. Students who contact AIB by a telephone will be required to verify their identity by completing a verbal identification check before their records can be discussed with them.

3.9. Information about a student or a staff member is not disclosed to a third party without the consent of the student or the staff member, unless required or permitted by law. Details of where AIB is required to disclose information about an individual are outlined in the AIB's Privacy Policy.

4. Maintaining records:

4.1. Records must be appropriately maintained, stored and preserved for as long as the record is required to meet business and legislative requirements.

4.2. 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.

- 4.3. Students are responsible for keeping their personal information up to date, including contact details and residential address, to ensure they retain continual access to the systems and AIB communication.
- 4.4. All Records that are to be archived must be archived as follows:
 - (a) 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
 - (b) If it is in an electronic form, it must be archived in enterprise grade computer data storage facility with a physically separate backup.

5. Privacy

- 5.1. Any collection, use, disclosure, handling and storage of and access to the Records must be in accordance with AIB’s Privacy Policy and Intellectual Property Policy.
- 5.2 At their appointment, staff are asked to sign confidentiality agreement (via employment contract or confidentiality deed).

Related Forms:

Schedule –Access to Students Records (internal)

Responsibility:

Chief Operating Officer

Current Status	Version 1
Approved By:	Executive Team
Date of Approval:	29 May 2019
Effective From:	29 May 2019
Previous Versions:	24 November 2016
	1 July 2011
	27 October 2008
Date of Next Review:	29 May 2022