Records Management Procedure

1 Purpose & Objective

1.1 This procedure outlines the process for the capture, storage, use, sharing, archiving and disposal of official records of IIBITEG.

2 Scope

2.1 This procedure applies to all IIBITEG entities located in Australia.

2.2 Records in the scope of this procedure include all documents that provide objective evidence of activities performed, events occurred, decisions made, results achieved, or statements made in relation to individual students, cohorts of students, or corporate business and governance activities. Records include but are not limited to legal contracts and agreements, electronic communication, letters, forms, teaching materials including content delivered via the Learning Management System, memos, drawings, letters, podcasts, videos, photographs and transcripts of verbal communication.

3 Procedure: Records Structure and Systems

3.1 All IIBITEG records, as defined in clause 2.2, must be created, collected, classified, and organised in a manner that ensures their integrity, quality and security.

3.2 There are five broad categories of records.

a) *Corporate*: for all corporate functions. All staff have access to these.
b) *Student*: for all student related records. Access to student records is limited.
c) *Personnel*: for Human Resources related records. Access to human resource records is limited.
d) *Executive*: for briefings, correspondence and other records pertaining to senior management. Access to executive records is limited.
e) *Governance*: for briefings, correspondence and other records pertaining to governance committees and boards. Access to governance records is limited.

3.3 An approved system must, at a minimum, meet basic records management criteria. These criteria include the functionality to:

a) manage electronic records, scanned images, voice files, video clips, digital plans, databases and information from other applications;
b) integrate with applications used for transaction of business (office utilities, e-mail, websites, database applications, workflow, etc.);
c) capture records by assigning them unique identities and attributing brief descriptive information to them, such as a title and date;
d) arrange records into categories based on the business activities they document, as a means of facilitating record control, retrieval, disposal and access;

e) assign and implement rights or restrictions that protect records against unauthorised or inappropriate use or access;
f) establish access points to facilitate record retrieval;
g) monitor record use to ensure no inappropriate use occurs and an auditable record of use is maintained;
h) link disposal periods to records;
i) make records available as corporate information resources;
j) identify and present records in response to user search requests and, where appropriate, enable records to be printed on request.

3.4 It is the responsibility of the Information Technology and Facilities Manager to assess all records management systems for compliance with clauses 3.3 before they are implemented or before records are migrated to or from the system.

3.5 A major change to an existing system must also be assessed for compliance prior to implementation by the Information Technology and Facilities Manager.

3.6 To maintain the integrity of the records management system, changes to the structure (folders, cabinets etc.) of the system must be approved and facilitated by the Information Technology and Facilities Manager.

3.7 To maintain the security of the records management system changes to the security settings on folders, cabinets or specific documents must be approved and facilitated by the Information Technology and Facilities Manager.

4 Procedure: Records Capture and Storage

4.1 It is the responsibility of all staff to capture records where the document provides objective evidence of activities performed, events occurred, decisions made, results achieved, or statements made in relation to individual students, cohorts of students, or corporate business and governance activities relevant to their position.

4.2 All records must be captured in an approved records management system.

4.3 Records that are created by an approved records management system must be stored in that system.

4.4 Records, including emails that are not created and/or stored in an approved business system, must be stored in the corporate records management system, PinPoint.

4.5 It is the responsibility of the staff member capturing the record to ensure sufficient metadata is included to enable other staff to easily understand when, how, where, why and on whose authority actions took place and decisions were made.

4.6 Corporate records must not be stored or maintained in email folders, shared drives, personal drives or external storage media.

5 Procedure: Records Use and Share

5.1 Access to records is only permitted by authorised members of staff or external members of governance boards and committees who require access for official business.

5.2 Under no circumstances are records to be accessed or used for non-IIBITEG related business.

5.3 Personal information held on records must only be used for the purpose for which it was collected and must only be disclosed to authorised persons.

5.4 Records containing personal information must be captured, stored, accessed, and disposed of in line with the requirements of relevant legislation.

5.5 Hard copy records stored within business areas must be secured to avoid possible theft, misuse or inappropriate access.

5.6 Staff leaving IIBITEG or moving roles within the organisation are responsible for ensuring records in their custody are made available intact and in their entirety to authorised staff. This includes transferring the custody of hard copy records and ensuring records stored in Outlook and / or network drives have been registered in PinPoint.

6 Procedure: Records Archiving and Disposal

Archiving

6.1 Details pertaining to the retention and disposal of records is outlined in the Records Retention and Disposal Authority.

6.2 Hard copy records no longer required for daily business activity that have not met the requirements for disposal should be transferred to IIBITEG's approved offsite archive facility.

6.3 Storage at other offsite storage facilities is not permitted.

6.4 Authority to transfer hardcopy documents must be obtained from the Information Technology and Facilities Manager.

6.5 Records must be boxed in C1 archive boxes.

6.6 Where multiple record types exist, records are to be placed with similar records of the same class, or retention period.

6.7 Records containing sensitive or personal information are to be stored separately to records of a general nature.

6.8 Records are required to be removed from lever arch files, bull-dog clips and plastic inserts prior to being boxed. Rubber bands or other methods of bundling are also prohibited to be used on records being prepared for archiving. Manilla folders can be used to separate records. Staples are permitted.

6.9 An Archives Lodgement Form is to be completed and a copy placed inside the top of each box.

Disposal of Hardcopy Records

6.10 The following steps are to be followed in to the destruction of hardcopy records that are time-expired:

a) order a destruction bin from the Department of Information Technology and Facilities Management;
b) complete a Records Destruction List;
c) ensure the Records Destruction List is signed by the member of staff with the authority to dispose of the record as specified in the Records Retention and Disposal Authority AND the Information Technology and Facilities Manager;
d) scan the signed Records Destruction List and save electronically in PinPoint;
e) place the records in the destruction bin;
f) arrange collection of the bin from the Department of Information Technology and Facilities Management.

6.11 The Department of Information Technology and Facilities Management arranges for disposal of the records via secure records and information disposal service.

Electronic Records

6.12 The Department of Information Technology and Facilities Management run reports periodically to identify records that are eligible for destruction based on disposal class (see Data and Records Management Policy).

6.13 The Department of Information Technology and Facilities Management contacts the member of staff with the authority to dispose of the record as specified in the Records Retention and Disposal Authority AND the Information Technology and Facilities Manager for authorisation to destroy time-expired records.

6.14 The member of staff with the authority to dispose of the record as specified in the Records Retention and Disposal Authority AND the Information Technology and Facilities Manager authorise destruction of the records.

6.15 Destruction of the records CANNOT proceed without authorisation from both the member of staff with the authority to dispose of the record as specified in the Records Retention and Disposal Authority AND the Information Technology and Facilities Manager.

6.16 The Department of Information Technology and Facilities Management destroys the authorised records and information (metadata) about the destroyed records is kept in PinPoint.

7 Responsibilities

7.1 The IIBITEG Board of Governance is responsible for the oversight of this procedure.

7.2 The Senior General Manager (Operations) is responsible for:
a) implementation of this procedure;
b) ensuring compliance with this procedure;
c) ensuring that staff are adequately notified of the existence of this procedures;
d) benchmarking IIBITEG policy and standards with those adopted elsewhere in the tertiary sector; and
e) the monitoring of information available from the review of records relating to the implementation of this procedure.

7.3 The Information Technology and Facilities Manager is responsible for:
a) approving new and major changes to existing official records management systems;
b) changes to the structure of official records management systems;
c) changes to security levels within official records management systems;
d) approving the destruction of hard copy and electronic records.

7.4 The member of staff with the authority to dispose of the record as specified in the Records Retention and Disposal Authority is responsible for approving the destruction of hard copy and electronic records.

7.5 It is the responsibility of all staff to capture records where the document provides objective evidence of activities performed, events occurred, decisions made, results achieved, or statements made in relation to individual students, cohorts of students, or corporate business and governance activities relevant to their position.

8 Definitions

MASTER DATA

means data about IIBITEG entities that provide context for business transactions

METADATA

means data that provides information about other data. IIBITEG references three distinct types of metadata: descriptive metadata, structural metadata, and administrative metadata

RECORDS

means documents that provide objective evidence of activities performed, events occurred, decisions made, results achieved, or statements made in relation to individual students, cohorts of students, or corporate business and governance activities. Records include but are not limited to legal contracts and agreements, electronic communication, letters, forms, teaching materials including content delivered via the Learning Management System, memos, drawings, letters, podcasts, videos, photographs and transcripts of verbal communication

9 Associated Information

Related Documents	- Records and Data Management Policy - Records Retention and Disposal Authority - Campus and Information Technology Asset Management Policy
Related Legislation	- TEQSA Act 2011 - ESOS Act 2000 - Higher Education Standards Framework 2015 - National Code of Practice for Providers of Education and Training to Overseas Students 2018 - Information Privacy Act - Freedom of Information Act
Date Approved	23 March 2018
Date of Effect	26 March 2018
Date of Review	March 2023
Approval Authority	IIBITEG Board of Governance
Document Administrator	Senior General Manager (Operations)
PinPoint DocID	361

10 Change History

Version Control	Version 1.1	
Change Summary	V1.1 2-May-19	Update responsibility from SGMAC to SGMO and administrative updates