# Data Management Procedure

## 1 Purpose and Objective

1.1 This procedure outlines the process for the management of IIBITEG's corporate, master and personal data to assure its quality, integrity and its proper management and protection.

## 2 Scope

2.1 This procedure applies to all IIBITEG staff and its corporate, master and personal data in all formats, of IIBITEG entities located in Australia.

2.2 Data included in this procedure includes:

a) Corporate data: facts as text, numbers, graphics, images, sound or video captured as an outcome of IIBITEG's day-to-day operations. It can include, but is not restricted to: staff data, student data, financial data, facilities data, curriculum data, etc.

b) Master data: data about IIBITEG entities that provide context for business transactions.

c) Personal data: data where a person's identity is apparent, or can reasonably be ascertained.

## 3 Data Requirements

3.1 Data should only be collected where it serves a known and documented use, as per clause 3.15 of the Data and Records Management Policy.

3.2 IIBITEG has an obligation to fulfil its data capture and reporting requirements to external agencies, as outlined below.

| SYSTEM | DATA REQUIREMENT | FUNCTIONAL OWNER |
|---|---|---|
| HEIMS | • HE Student Data Collection<br>• HE Staff Data Collection<br>• VET Data Collection (VET Student Loans, VET FEE-HELP) | • Department of Student Administration |
| ASQA | • Total VET Activity Reporting<br>• Quality Indicator Reports | • Department of Student Administration |
| NEAS | • Student Data Collection by staff | • Department of Student Administration |
| QILT | • Student Experience Survey<br>• Course Experience Questionnaire<br>• Graduate Outcomes Survey<br>• Employer Satisfaction Survey | • Department of Student Administration |

| SYSTEM | DATA REQUIREMENT | FUNCTIONAL OWNER |
|---|---|---|
| PRISMS | • Annual international student numbers and income<br>• Student Data Collection<br>• Student Deferral Data<br>• Medical Records<br>• Banking Details | • Department of Student Administration |
| Work Ready | • Medical Records<br>• Student Data Collection<br>• Student ID Checks (i.e. Qualifications and Personal Details – USI {Unique Student Identifier}<br>• Language Literacy & Numeracy Data Testing (LLN)<br>• Academic Records/Performance of Students | • Department of Student Administration |
| Smart and Skilled | • Medical Records<br>• Student Data Collection<br>• Student ID Checks (i.e. Qualifications and Personal Details – USI {Unique Student Identifier}<br>• Language Literacy & Numeracy Data Testing (LLN)<br>• Academic Records/Performance of Students | • Department of Student Administration |

3.3 The Senior General Manager (Operations) has overarching responsibility for ensuring that all data is captured and reported in accordance with external regulatory and contractual requirements.

3.4 IIBITEG also has additional data capture and reporting requirements that support internal processes such as: strategic planning, performance monitoring and review; budgeting and financial reporting; asset registers; transactions; continuous improvement activities, review of services, organisational units and facilities and human resource services.

3.5 Data requirements should be frequently reviewed and updated as required based on the compliance requirement changes by regulatory bodies and also changes to internal data and reporting processes.

3.6 The Information Technology and Facilities Manager is responsible for ensuring that data requirements are reviewed on a periodic basis as outlined in clause 3.5.

3.7 The Operations Committee will be advised of any data requirement changes as they arise to ensure an organisational perspective of all data requirements is maintained.

3.8 The Department of Information Technology and Facilities Management maintains a register of endorsed systems and data stored in them.

## 4 Data Capture, Processing, Initial Verification and Quality

4.1 Effective data capture relies on knowledgeable staff, well-designed forms, databases and interfaces to ensure that all required data is collected in a form that meets the organisational and reporting needs and ensures the production of high quality and targeted data.

4.2 Wherever possible data capture, processing and verification should be automated to maximise data quality.

4.3 Effective processes must be in place for the capture, maintenance and dissemination of high quality data with all data required to confirm to the requirements of each field.

4.4 Data processing must be processed lawfully, fairly and in a transparent manner.

4.5 Initial verification of data must be undertaken by staff who enrol students at the initial stage i.e. the Admission Staff would bear an onus for the initial verification of data.

4.6 It is the responsibility of the relevant department manager to appoint a Data Stewards for each unit. Data Stewards are responsible for:

a) checks in relation to the accuracy and integrity of data produced by their organisational unit;
b) frequent review, update and reporting of new or revised data requirements;
c) day-to-day management and oversight of quality of data produced by their unit;
d) overseeing and undertaking data quality audits and contributing to the resolution of identified issues in their unit; and
e) being the key point of contact within each organisational unit to assist with the effective implementation of the Data and Records Management Policy and this Procedure.

4.7 It is the responsibility of the relevant department manager to undertake additional periodic quality checks in relation to adherence to business process and data entry ensure high quality data capture.

4.8 Staff members who identify data quality issues relating to accuracy, completeness, duplication and/or currency of data, or changes to business processes impacting on data collection and recording are required to report issues to the Senior General Manager (Operations). The Senior General Manager (Operations) will convene an ad hoc Data Management Working Group to facilitate an appropriate organisational response to the issue raised.

4.9 Issues with the possibility of negatively impacting on ongoing compliance or contractual arrangements are to be reported to the IIBITEG Audit and Risk Committee by the Senior General Manager (Operations).

## 5 Data Storage, Retention and Disposal

5.1 Storage media used for the archiving of data must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary or internal formats are involved.

5.2 Data storage systems are to be approved by the Information Technology and Facilities Manager and reported to the Operations Committee.

5.1 Corporate, Master and Personal Data, whether physical or digital must be stored in endorsed systems.

5.2 When permanently disposing of equipment containing storage media, all Confidential Data and licensed software must be irretrievably deleted before the equipment is moved off-site.

5.3 Data must be stored in an accessible form in accordance with the provision and minimum retention periods specified by the associated regulatory guidelines.

5.4 The timely destruction of data is essential for effective management. Electronic and physical data are destroyed by the authorised person after fulfilling the minimum retention period prescribed in Records Retention and Disposal Authority.

## 6 Data Accessibility and Security

6.1 Data sharing is encouraged and data must be readily available to staff with a legitimate business need, except where the nature of the data requires restriction.

6.2 Access to data within IBITEG is restricted to authorized staff with the relevant business process requirement. All staff need to be authorised to access data as per authorization approval process.

6.3 Extraction, manipulation and reporting of data internally should inform IIBITEG's teaching, management and governance requirements only.

6.4 Even where data is to be used as outlined in clause 6.3 where the data is related to any aspect of the student experience from first contact through to alumni it must be used ethically, particularly in instances where IIBITEG seeks to use such data to influence student behaviour either directly or indirectly. Any use outside that proscribed in the Offer Letter must be authorised by the IIBITEG Audit and Risk Committee.

6.5 Personal use of institutional data, including derived data for personal research, in any format and at any location, is prohibited.

6.6 Requests to use such data for personal research or scholarship should be managed via the Human Research Ethics Procedure regardless of the sector in which they teach.

6.7 Where appropriate, before any data (other than publicly available data) is used or shared outside the IIBITEG, verification from the Senior General Manager (Operations) is required to ensure the quality, integrity and security of data will not be compromised.

6.8 Third parties who are provided with access to IIBITEG data are required to sign a non-disclosure agreement.

6.9 Suitable controls are implemented for safeguarding sensitive data in IIBITEG systems, including strong authentication for all access and encrypting data during transmission over public networks.

6.10 High security firewalls are used to control access to services or ports on servers that contain IIBITEG data.

## 7 Metadata Management

7.1 Metadata management is undertaken by the Department Information Technology and Facilities Management.

## 8 Roles and Responsibilities

8.1 The IIBITEG Board of Governance is responsible for:

a) oversight of this procedure;
b) approval of any request to dispose of data.

8.2 The Senior General Manager (Operations) is responsible for:

a) implementation of this procedure ensuring compliance with this procedure;
b) ensuring that staff are adequately notified of the existence of this procedure;
c) benchmarking IIBITEG policy and standards with those adopted elsewhere in the tertiary sector; and
d) the monitoring of information available from the review of records relating to the implementation of this procedure.

8.3 The Information Technology and Facilities Manager is responsible for:

a) approving new and major changes to existing official data management systems;
b) changes to the structure of official data management systems;
c) changes to security levels within official data management systems; and
d) reporting to the Operations Committee regarding a) to c).

8.4 Managers of Organisational Units are responsible for:

a) nominating a Data Steward for the unit. The Data Steward does not necessarily have to be solely dedicated to data management, although this responsibility for oversight of data management for the unit should form part of their duty statement;
b) ensuring effective processes are in place for the capture, maintenance and dissemination of high quality data by their unit; and

c) ensuring all staff in the organisational unit are aware of their responsibilities and the key role they play in producing high quality data.

8.5 Data Stewards are responsible for:

a) accuracy and integrity of data produced by their organisational unit;
b) frequent review, update and reporting of new or revised data requirements;
c) day-to-day management and oversight of quality of data produced by their unit;
d) overseeing and undertaking data quality audits and contributing to the resolution of identified issues in their unit; and
e) being the key point of contact within each organisational unit to assist with the effective implementation of the Data and Records Management Policy and this Procedure.

8.6 Staff with the responsibility for data entry are responsible for the capture and maintenance of accurate data and ensuring data entered confirms to the requirements of each field.

8.7 Data Users are responsible for:

a) the accurate presentation and interpretation of data; and
b) releasing data only on the authority of the Manager of their organisational unit or higher.

8.8 It is the responsibility of all staff to understand their role in data capture, processing, verification to ensure the integrity and quality of all IIBITEG corporate, master and personal data.

## 9 Definitions

| | |
|---|---|
| ADMINISTRATIVE METADATA | means data that provides information to help manage a resource, such as when and how it was created, file type and other technical information, and who can access it |
| CORPORATE DATA | means facts as text, numbers, graphics, images, sound or video captured as an outcome of IIBITEG's day-to-day operation. It can include, but is not restricted to: staff data, student data, financial data, facilities data, curriculum data, etc |
| DATA ADMINISTRATOR | means the person responsible for the administration of the data and monitoring of the quality of data capture |
| DATA STEWARD | means the person responsible for the accuracy and integrity, of data |
| DESCRIPTIVE METADATA | means the description of a resource for purposes such as discovery and identification. It can include elements such as title, abstract, author, and keywords. |

| | |
|---|---|
| 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 |
| PERSONAL DATA | means data where a person's identity is apparent, or can reasonably be ascertained. |
| QUANTITATIVE DATA | means data that can be counted (discrete data) or measured (continuous data) |
| QUALITATIVE DATA | means non-numerical, categorical data that be arranged or coded into categories |
| STRUCTURAL METADATA | means the data that describes the internal structure or representation of a data asset |

## 10 Associated Information

| | |
|---|---|
| **Related Documents** | • Data and Records Management Policy<br>• Records Retention and Disposal Authority<br>• Qualifications Issuance and Graduation Policy<br>• Student Well-Being and Support Policy<br>• Academic Policy<br>• Student Appeals Procedures<br>• Student Complaints and Grievances Procedure<br>• Academic Integrity and Academic Misconduct Procedure |
| **Related Legislation** | • TEQSA Act 2011<br>• ESOS Act 2000<br>• Higher Education Standards Framework 2015<br>• National Code of Practice for Providers of Education and Training to Overseas Students 2018<br>• AQF Qualifications Issuance Policy<br>• Guidelines for the presentation of Australian Higher Education Graduation Statements |
| **Date Approved** | 23 March 2018 |
| **Date of Effect** | 1 April 2018 |
| **Date of Review** | March 2023 |
| **Approval Authority** | IIBITEG Board of Governance |
| **Document Administrator** | Senior General Manager (Operations) |
| **PinPoint DocID** | 369 |

## 11 Change History

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