Records, Data and Information Management and Security Policy

Supporting plans, policies and procedures	• Academic Assessment and Moderation Policy and Procedure • Academic Progress and Student At-Risk Policy and Procedure • Code of Conduct • Critical Incidents and Business Continuity Policy and Procedure • Critical Incidents and Business Continuity Plan • Conferral of Awards and Graduation and Academic Documentation Policy • Equity, Diversity and Aboriginal and Torres Strait Islander Peoples Framework and Policy • Facilities, ICT Infrastructure and Resources Policy • Freedom of Intellectual Enquiry Policy • ICT/Infrastructure Plan • Marketing and Student Recruitment Policy • Privacy Policy • Risk Management Policy • Risk Register
Related legislation and references	• Australian Privacy Principles • Higher Education Standards Framework (Threshold Standards) 2021 • Public Records Office, *Victoria Retention and Disposal Authority for Records of Higher and Further Education Functions (https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1607-higher-and-further-education-functions)* • Tertiary Education Quality and Standards Agency (TEQSA) Act 2011
Version	3.1
Approved by	Board of Directors and Academic Board
Date approved	AB: 28/10/2024 BoD: 23 May 2024
Approval reference	ABMO# 17 BoD MO#33
Document Review	This document is to be reviewed at least every three years

Version	Review Date and Person/Body	Notes
0.1	Draft prepared by CEO and approved at 7 January 2020 Board of Directors meeting	
1.0	Reviewed by Learning and Teaching Committee (LTC) on 4 February 2020	
1.1	Presented to Academic Board on 18 February 2020 for review and approval	The Academic Board requested reference to the Privacy Principles and definitions of who's accountable for different data be added
1.2	Presented to Academic Board on 21 April 2020 for review and approval	Included items requested by the Academic Board on 18 February 2020
2.0	Approved by the Academic Board on 21 April 2020	Included items requested by the Academic Board on 21 April 2020
2.1	Reviewed and approved at 20 October 2020 Academic Board meeting	Minor amendments following comments from external reviewers
	Reviewed and approved at 28 October 2020 Board of Directors meeting	

3.0	Reviewed and approved by the Board of Directors and Academic Board via email circulation on 23 July 2021	Updates made following the response to the TEQSA Request for Information 23 July 2021
3.1	Reviewed and approved by the Board of Directors on 28 Oct. 2024 and Academic Board on 23 May 2024	Revisions pursuant to scheduled review including in relation to data retention.

Background and Scope

This policy outlines how MIHE will manage records to meet business, legislative and regulatory requirements. Accordingly, this policy specifies how MIHE manages records/data collection, security, retention, and the destruction of records.

This policy binds all directors, committee members, staff, students, contractors, and visitors (hereafter referred to as stakeholders).

This policy applies to all records, data and information created or received in any format as part of or in conjunction with MIHE operations. Also, refer to the *Privacy Policy* which was developed in alignment with the Australian Privacy Principles.(https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/).

Definitions

Data	Data means information, resources, and other records that fit into one of the following categories: • Public Access: data that is publicly available and is unlimited in access to all students, staff, and the general public such as the MIHE's public website • Internal Data: data used and accessed only MIHE staff and not to be used by external sources without prior approval • Internal Protected Data: data that is only accessible by the staff members that are required to use it to complete their assigned duties at MIHE • Internal Restricted Data: secure data that is to be kept confidential with specialised authorisation that must be given to anyone wishing to access this type of data

Also refer to Glossary of Terms.

Policy

Policy Principles

This policy and procedure will meet the following principles:

1. Recordkeeping responsibilities will be assigned to and implemented by staff.
2. Full and accurate records will be made, managed, and preserved for as long as they are required for business and legislative requirements.
3. Records will be disposed of in a safe and secure manner.

4. Approved information systems will ensure the systematic, comprehensive, reliable, timely and accurate retrieval of records.
5. Students will be able to access their own records upon request through an appropriate process.
6. Records management systems and practices will be regularly monitored, audited, and evaluated for accountability, compliance, and continued improvement.
7. Security provisions will be implemented to maintain the integrity of records and authenticity by preventing unauthorised access, damage, alteration, fraud or misuse.

MIHE is the sole owner of all records created in the process of conducting its operations and governance. Control of any category of MIHE data will always be vested in more than staff member. All MIHE staff will perform the essential role of record keeping.

Data Leader

A Data Leader at MIHE will be in charge of ensuring that there is appropriate data quality and security, and that this policy is being adhered to. The Data Leader in charge of any category of data is responsible for allowing the access and distribution of that data in accordance with MIHE's policies and procedures.

The Data Leader also has the following responsibilities:

- Determining whether or not any individual should be granted access to a piece of data that is otherwise considered to be protected or restricted. When the Data Leader does not have the ability to grant access alone, they must work together with their supervisor or other authorised staff before permission can be given to access the data.
- Consider and assess the reason for the data access request along with what the data will be used for after access has been granted (see Data Access, Retention and Disposal below for details).
- Ensure all appropriate steps below are completed to ensure that data/records are as accurate and complete as possible:
    - Plan, design, and develop data/records collection.
    - Organise, store and protect data/records.
    - Monitor, review, improve and/or dispose of data/records.

In addition to the Data Leaders, all data users are responsible for making sure that the appropriate steps and guidelines are followed when accessing data to ensure the accuracy and reliability of the data/records remain intact and in a useable form. Data Leaders and all data users must also adhere to all MIHE's policies and procedures, including the *Privacy Policy*.

With the exception of public data, no data can be collected, used or shared without prior approval by the Data Leader or Chief Executive Officer.

Where the data is to be collected used or shared for academic purposes, approval may be given by the Data Leader Data must never be accessed or used for personal purposes.

Electronic safeguards must be in place for all data stored electronically. Any hardcopies of records or data must also be stored securely so that it cannot be accessed by unauthorised individuals. Hardcopies must not be altered and all care must be taken to prevent them from damage. The *Critical Incidents and Business Continuity Policy and Procedure* outlines the process for managing potential loss of records.

All data should be disposed of properly and securely if required. Hard copies and electronic sources (such as hard drives and flash drives) must be disposed of securely. All Student Data is to be retained permanently as prescribed below.

Data Access, Retention, and Disposal

Staff may have access to those records necessary to fulfil their duties at MIHE; however, access to designated confidential records may be restricted. All organisational data will be stored on secure electronic servers consistent with the requirements of the *Critical Incidents and Business Continuity Plan*. External parties will not have access to records unless authorised by the Data Leader or as required by the law.

The following table outlines the key data categories, including registers, that MIHE manages, including, data type, data form/system, and Data Leader position.

Data Category	Data Type	Systems	Data Leader
Student enrolment, progression, completion, qualification and award data	Internal Restricted	Student management system	Dean, Administration Manager
Student feedback and survey information			
Course delivery material: unit outlines, study guides, reading guides Course guides: course descriptions, requirements, content, outcomes Assessments, examination questions		Hardcopies, Electronic copies stored on secure network server, Learning Management System	Dean, Course Director
Corporate Documents (policies, plans, insurance policies, etc.)	Public Access, Internal, Internal Protected, Internal Restricted	Hardcopies, Electronic copies stored on secure network server	CEO, Dean, Administration Manager
Complaints Register			

Academic Misconduct Register	Internal Restricted	Electronic copies stored on secure network server	CEO, Dean, Administration Manager
Non-Academic Misconduct Register			
Critical Incident Register			
Conflict of Interest Register			
BoD and AB Resolutions Register			
Policies and Procedures	Public Access, Internal, Internal Protected, Internal Restricted	Electronic copies stored on secure network server	

The retention and disposal requirements of all data must occur in accordance with the requirements of the *Retention and Disposal Authority for Records of Higher and Further Education Functions* (2019) as amended from time to time (https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1607-higher-and-further-education-functions). In the event of a conflict between these requirements and this policy, the former shall prevail to the extent of any inconsistency.

Auditing

Records, data and information management activities and practices will be audited regularly to ensure security and compliance with the Audit and Risk Committee providing oversight. Auditing will ensure accuracy and fairness of MIHE's records, data and information management systems.

Penalties

Breach or failure to comply with this policy may result in disciplinary action in accordance with the *Code of Conduct*.