QAF055 RECORDS MANAGEMENT AND SECURITY PROCEDURES

1. Overview

Senior management of the Higher Education Leadership Institute ("the Institute") have a legal responsibility to protect the organisation's physical and electronic records and the information the Institute holds.

The creating, securing and retention of records is part of the Institute's overall knowledge management system.

The Institute keeps records to:

- provide an historical record of the Institute's operations, activities and decision making;
- provide evidence of business transactions and decisions, for purposes of accountability;
- enable the Institute to find the right information easily and comprehensively;
- enable the Institute to meet its legal and regulatory requirements for data management and reporting.

2. Types of records

2.1 Student records

A "student record" is created for each student in the Student Management System (MeshedHE).

The Registrar maintains student records.

The student record contains as a minimum:

- the completed *Application for Admission Form [FRM010];*
- evidence that the student meets the course entry requirements;
- the *Letter of Offer and Student Agreement [FRM011]*;
- any information relating to request for, and granting of, credit for prior learning;
- results for each assessment task in a subject;
- the final mark and grade for each subject;
- details of payments and refunds;
- copies of testamurs and records of results issued;
- any notes made by the academic / administrative staff about the student (including any disciplinary matters).

The entire student record is maintained for a period of at least 2 years from graduation (or when the student otherwise ceases to be a student).

Financial records relating to a student are kept for a minimum of 7 years.

Student results for each subject are retained indefinitely to enable the re-issue of an award and record of results if required.

In the event of the Institute's closure, student records will be transferred to the relevant higher education regulator, or as otherwise prescribed by regulation.

Students may access information on their files as per the *Privacy and Personal Information Procedures [QAF050]*. Third party access to personal information is only permitted when required by law or with the express permission of the student as outlined in the *Privacy and Personal Information Procedures [QAF050]*.

2.2 Staff records

The Registrar maintains staff records.

Each staff member has an electronic file created and maintained for the purpose of archiving:

- recruitment documentation;
- employment conditions / letter of offer / employment agreement;
- evidence of the "right to work" in Australia;
- role description;
- certified copies of qualifications claimed;
- verification of experience;
- professional development and scholarly activity.

Original documentation must be sighted to verify the authenticity of qualifications. Copies on file must indicate the date sighted and by whom (refer *Staff Appointment, Development and Appraisal Policy & Procedure [QAF065]*, section 2.4).

Disciplinary action or details of grievances in which the staff member is a complainant or respondent will also be noted in the staff file.

Staff may access information on their files on request to the Registrar.

Third party access to staff records is only permitted when required by law or with the express permission of the relevant staff member.

2.3 Financial records

The Finance Manager maintains financial records.

Financial records are created, secured, archived and retained consistent with contractual and legal requirements (Refer *Financial Management Procedures [QAF040]*).

Financial and contractual records are kept for a minimum of 7 years.

3. Records security and access

The Institute takes seriously its obligations under privacy legislation to safeguard all confidential information. The Institute will also ensure that anyone acting on its behalf maintains appropriate confidentiality. As such, it is a requirement that records are held in a secure environment and safeguarded against loss, damage or unauthorised access. Only authorised staff will be granted access to student and staff records.

3.1 Electronic records

The Institute maintains a secure computer system that comprises a series of integrated network services. Each user has their own password(s) which allows them access to appropriate functions, data and files within the system.

The Technology Infrastructure Manager is responsible for the restriction of access to and security of electronic records.

3.2 Physical records

Physical records (where they exist) are kept in secure areas or locked filing cabinets and access is only available to authorised personnel.

4. Version management

In the interests of effective knowledge management, the Institute has implemented a system for managing the versions of certain documents - refer section 4.4 of the *Quality Framework [QAF001]* and the *Version Control Register [QAF000].*

5. Record retention and disposal

Records will be retained and secured according to the following retention periods:

- General business records (including financial records): 7 years.
- Student records: 2 years after the student ceases to be a student except for enough data to re-issue an award or record of results to be kept in perpetuity.
- Staff records: 5 years after the staff member ceases to be a staff member.

6. Security of electronic data

The breakdown of key ICT infrastructure and loss of externally hosted services, either by mechanical means or human intervention, can become a critical incident if proper safeguards are not put in place to ameliorate the impact of such a breakdown.

Refer *HELI ICT Disaster Recovery / Business Continuity Plan [PLN036].*

6.1 Preventions against data loss

As the Institute relies primarily on external providers for the provision of ICT infrastructure, it is reliant on each provider to protect against data loss. In the event of data loss, the Institute would contact the relevant provider for assistance.

Where possible, the Institute will take and securely store independent backups of all data at regular intervals to facilitate recovery in the event of provider failure, or a data loss event that falls outside the scope of service level agreements.

6.2 Security safeguards

6.2.1 Protection against in-house intrusions:

i) All administrative accounts and network-level services are to be secured and configured in accordance with industry best practice.

ii) Details of administrative accounts are to be held only by the Technology Infrastructure Manager and CEO.

iii) If deemed practical and necessary by the CEO, some or all administrative account usernames and / or passwords are to be changed if the Technology Infrastructure Manager or other personnel cease to be employed by the Institute.

6.2.2 Protection against external intrusions

i) As the Institute relies primarily on external providers for the provision of IT infrastructure, it is reliant on these providers to secure their networks and services. All providers are to be evaluated in this regard prior to engagement, and relevant service level agreements are to be put in place.

ii) All Institute staff are to ensure that personal devices used to conduct Institute business have up-to-date security patches, firewall and anti-virus software installed.

iii) Student data should not be stored on devices belonging to Institute staff for longer than necessary and should be deleted as soon as possible.

iv) All computers used in conducting business for the Institute should be protected with a "logon" password to protect against casual theft, however it should be noted that data can be easily extracted from the hard disk of a stolen computer unless encrypted.

6.2.3 In the case that data is compromised:

The Technology Infrastructure Manager will evaluate the situation and report the extent of the damage and a proposed course of action to the CEO as soon as is practical and no later than within 12 hours of the compromise being detected.

7. Related documents

QAF000 Version Control Register

QAF001 Quality Framework

QAF040 Financial Management Procedures

QAF050 Privacy and Personal Information Procedures

QAF065 Staff Appointment, Development and Appraisal Policy and Procedure

PLN035 HELI Technology Development and Management Plan

PLN036 HELI ICT Disaster Recovery/Business Continuity Plan

8. Version history

Version	Approved by	Approval Date	Sections modified
1.0	Executive Management Committee	8 July 2016	Document creation and initial approval
1.1	Executive Management Committee	6 July 2018	Scheduled review
2.0	Executive Management Committee	17 February 2020	Scheduled review Minor consequential changes
2.1	CEO	7 July 2023	CEO reviewed the policy and extended the review date to 7 July 2024.
2.2	CEO	30 January 2025	CEO reviewed the policy and extended the review date to 7 December 2025

Document owner: Registrar