RECORDS MANAGEMENT PROCEDURE

Approving authority	Executive Management Team
Purpose	The purpose of this procedure is to define policy and procedures for records management.
Responsible Officer	Executive Director
Next scheduled review	September 2023
Document Location	http://www.ozford.edu.au/higher-education/life-at-ozford/
Associated documents	Admissions Policy & Procedure Assessment Policy & Procedure Academic Progress Policy & Procedure Academic Integrity Policy & Procedure Credit Transfer and Articulation Policy Conferral of Academic Qualification Policy & Procedure

1. PRINCIPLES

The Institute of Higher Education (herein referred to as the "Institute") will ensure that all required information relating to students will be stored appropriately with controls over access; that this data is accurate, complete and current with appropriate back-up arrangements in place.

2. SCOPE

This procedure applies to all data collecting from students.

3. DEFINITIONS

Records: records information in any form including data in computer systems, created or retrieved and maintained by the Institute and kept as evidence of activities.

Archives: Records relocated to long-term storage for preservation beyond their immediate business function, including permanent records.

Disposal: Destroy or abandon the record.

4. PROCEDURES

4.1 Financial Records

4.1.1 The financial records are archived at the end of each financial year. The data is placed into archive boxes, clearly labelled and stored for 7 years. At the end of this period the documents are shredded.

4.1.2 The Institute will maintain up to date records of financial information including fees paid and refunds given.

4.2 On-Line Records

4.2.1 Any on-line documentation regarding the quality system is updated as required on- line. Printed out-of-date documentation is to be destroyed by relevant staff members securely as soon as they have been notified of any amendments to documents. Out-of-date documents are to be placed into the locked security bins or shredded in-house.

4.2.2 On-line information is stored in appropriate folders on the computer by the Head of Departments or responsible staff member.

4.3 Student Records upon Acceptance

4.3.1 The Institute must keep a record of each accepted student who is enrolled or who has paid any tuition fees for a course provided by the Institute.

4.3.2 Accepted student means a student (whether within or outside Australia) who is accepted for enrolment, or enrolled, in a course provided by the Institute.

4.3.3 The records must consist of the following details for each accepted student:

a) the student's enrolment records including signed acceptance agreement, payment record,
b) the student's personal details including residential address, mobile phone number, email, address and passport number;
c) credit transfers or exemptions granted;
d) any other details prescribed by the ESOS regulations (applicable to international students on student visa only).

4.3.4 The record will be entered onto Student Administration systems and scanned in secured network drive. Student files will be maintained for two years after the student ceases to be an accepted student in a secure network drive after which time they will be deleted.

4.3.5 If the Institute grants RPL or course credit to an overseas student, the Institute will give a written record of the decision to the overseas student to accept and retain the written record of acceptance for two years after the overseas student ceases to be an accepted students.

4.4 Student Records upon Commencement

4.4.1 The Institute must keep and maintain a record of each student upon student commencing enrolment at the Institute.

4.4.2 The records must consist of the following details for each student upon commencement:

a) the student's personal information including name, date of birth, and medical condition;
b) the student's contact information including Australia residential address, mobile phone number, email address, and emergency contact details.

4.4.3 The record will be entered onto Student Administration systems and scanned in secured network drive.

4.4.4 Student personal and contact information will be maintained for two years after the student ceases to be an accepted student in a secure network drive after which time they will be disposed.

4.5 Assessment Records

4.5.1 Assessment records will be maintained for every enrolled student and will include all assessment tasks for each unit within an enrolled course.

4.5.2 Assessment records for each enrolled student will include grades assigned on the completion of individual units. This also includes the administration, recording and reporting requirements, and may address a cluster of assessment tasks as applicable for holistic assessment.

4.5.3 Completed student assessment items are the actual piece(s) of work completed by a student or evidence of that work, including evidence collected for Recognition of Prior Learning (RPL) process. An assessor's completed marking guide, criteria, and observation checklist for each student may be sufficient where it is not possible to retain the student's actual work. However, the retained evidence must have enough detail to demonstrate the assessor's judgement of the student's performance against the standard required.

4.5.4 The Institute will securely retain all completed student assessment items for each student, as per the definition above, for a period of six months from the date on which the assessment of the final unit grade for the student was made.

4.6 Student Progression Records

4.6.1 The Institute must keep and maintain a record of each student progression during their enrolment at the Institute.

4.6.2 The progression records must consist of the following details for each student:

a) the student's enrolled units and unit outcome (student transcripts);

b) if student is identified as at risk of course progress: letters issued to student to inform progress and intervention meeting record.

4.6.3 Student progression will be maintained for two years after the student ceases to be an accepted student in a secure network drive after which time they will be deleted.

4.7 Student Incident Records

4.7.1 Incidents that the Institute must keep and maintain a record include:

a) formal complaint by students;

b) allegation of student misconduct;

c) breaches of academic integrity;

d) student critical incidents (refer to Critical Incident Policy and Procedures).

4.7.2 The records must consist of the following details for each incident:

a) details of incident including date and summary of incident;

b) management and outcome of the incident;

c) evaluation of the incident (if available).

4.7.3 The record will be entered onto Student Administration system and scanned in secured network drive.

4.7.4 Student incident record will be maintained for two years after the student ceases to be an accepted student in a secure network drive after which time they will be deleted.

4.8 Student Completion and Award of Qualification Records

4.8.1 The Institute must keep and maintain a record of each student upon student completion of enrolment at the Institute.

4.8.2 The records must consist of the following details for each student upon completion:

a) student full academic record (statement of result);

b) award of qualification issued (Refer to Conferral of Academic Qualifications Policy and Procedures).

4.8.3 The Institute's student completion and award of qualification records will be maintained for a period of 30 years.

4.9 Information Privacy

4.9.1 The Institute implements the Information Privacy Principles specified in the *Information Privacy Act* 2000 (Vic).

4.9.2 The collection and use of personal and health information must relate directly to the legitimate purposes of the Institute.

4.9.3 Individuals must be aware of, or informed of, the purposes for which personal and health information is obtained.

4.9.4 The Institute will take all reasonable measures to ensure that the personal information it receives and holds is up to date.

4.9.5 The Institute will take all reasonable measures to store personal information securely.

4.9.6 Individuals are entitled to have access to their own records, unless prevented by law.

4.9.7 Third party access to personal and health information may only be granted in accordance with the privacy principles and Institute policy and procedures.

4.9.8 The Institute will amend records shown to be incorrect.

4.9.9 The Institute will safeguard the confidentially of information obtained on its behalf and will ensure that except as required under the Standards for registration as a Higher Education Provider or by law, information about a client is not disclosed to a third party without written consent of the client.

4.10 Staff Competencies

4.10.1 The Vice President, Academic Dean, academic staff and relevant administrative staff are responsible for maintaining up to date records of the verified academic qualifications and experience of all staff and persons working on behalf of the Institute. These documents are kept secured in the Accounts office.

4.11 Other Documentation

4.11.1 All other hard-copy documentation is archived as required by staff and management. All archive boxes are to be clearly labelled and stored for 7 years. At the end of this period the documents are shredded.

4.12 Computer Data Back-up Procedure

4.12.1 The IT Department ensures the back-up on a nightly basis. Contents of the shared drives are backed up to local backup server and tapes. The tapes are stored securely offsite with a tape management company.

4.12.2 Back up for network drive that contains students' records of attainments of units of competence and qualification are retained for a period of 30 years.

4.12.3 Back up for network drive that contains students' records of attainments of units of competence and qualification are retained for a period of 30 years.

4.13 Access and Security of the Records

Access to the Institute records is only permitted by authorised staff.

Personal information held on corporate records must only be used for the purpose with which it was collected and must only be disclosed to authorised persons. Records containing personal information must be captured, stored, accessed, and disposed of in line with the requirements of relevant legislation (including, but not limited to the Information Privacy Act, Freedom of Information Act and Public Records Act).

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

All staff must ensure their username and password for the Institute systems are kept secure at all times and are not shared with anyone else under any circumstances.

All records kept at the Institute, including records of breaches to academic integrity (by staff or student), allegations of academic misconduct, and assessment results, student records, student progression and student completion, can only be accessed by the Executive Director, Academic dean, Head of Department and Head of Student Services and Administration or their delegate. Other record accessibility is available in appendix 1.

5. QUALITY ASSURANCE

To ensure that this procedure is fit for purpose and meet the requirements of the HES Threshold Standards the procedure will be:

5.1 internally approved by the Executive Management Team on development or review;

5.2 externally reviewed as part of any independent review of the HES Threshold Standards approved by the Governing Board;

5.3 internally reviewed by the Responsible Officer every three years from the date of approval (if not earlier);

5.4 referenced to the applicable HES threshold Standard and/or other legislation/regulation.

6. FEEDBACK

Feedback or comments on this procedure is welcomed by the listed Responsible officers of the Institute.

7. ACKNOWLEDGEMENTS

This policy was initially developed with reference to the following institution's policy: Ozford College of Business, Records Management Policy, January 2016.

Australian Catholic University, Record and Archive Management Policy, August 2018

8. VERSION CONTROL

Version	Date approved	Description	Approved by
3.0	September 2018	Initial Issue	EMT
4.0	May 2019	Internal Review	EMT
4.1	November 2019	Classification of student records	EMT
5.0	October 2020	Internal Review	EMT
Related legislation/ regulation/standard	HES Threshold Standards 2015 Domain 7 ESOS National Code 2018		

Appendix 1 : Record Accessibility

	Record Categories	Description	Accessible by
1	Student Personal information	a person's name, address, date of birth, student identification card, and other personal characteristics.	? Executive Director ? Account Manager ? Head of Student Services and Administration ? or their delegate
2	Staff Personal Information	a person's name, address, date of birth, identification card and other personal characteristics	? Executive Director ? Human Resources Manager ? Account Manager ? or their delegate
3	Student Assessment Records including Academic Integrity matters	marked assessment papers and academic misconduct register	? Academic Dean ? Head of Student Services and Administration ? or their delegate
4	Financial information	tuition fee payments, tax file numbers, bank account or credit card details.	? Account Manager ? or their delegate
5	Health related information	counselling notes or medical information.	? Head of Student Services and Administration ? or their delegate
6	Legally privileged documents		? Executive Director ? or their delegate