Records Management, Security, Retention and Disposal Policy and Procedure

CONTENTS

1 PURPOSE

1.1 The purpose of this policy and procedure is to ensure that all records retained by Polytechnic Institute Australia ('PIA') reflect the regulatory requirements, privacy principles, and legal responsibility to protect, retain and discard the organisation's physical and electronic records (including IT infrastructure) and the information PIA holds.

2 SCOPE

2.1 This policy and procedure applies to all members of staff at PIA.

3 POLICY STATEMENT

3.1 This policy and procedure upholds the principles of best practice with respect to all facets of records management, acknowledges the legal and ethical obligations of PIA, and supports its commitment to complying with those obligations.

Records Management, Security, Retention and Disposal Policy and Procedure

4 PROCEDURES

Student Records Management

4.1 A separate paper-based file is created for each student and an electronic record is also created in the student database, Student Management System (RTOM).

4.2 The paper and electronic student files combined are known as the 'student record'.

4.3 Student records are maintained by the Registrar.

4.4 The student record contains, as a minimum:

- the completed Application Form;
- Confirmation of Enrolment (CoE) for international students;
- supporting enrolment documentation;
- enrolment details;
- any agreement with the student;
- any information relating to a request for, and granting of, Advanced Standing;
- completed Student Induction checklist;
- signed Student Code of Conduct;
- confirmation of unit enrolment;
- personal details;
- student requests;
- Special Consideration forms;
- results for each assessment event in a unit of study;
- the final mark and grade for each unit of study;
- details of payments and refunds;
- copies of testamurs and records of results issued;
- any Student Intervention activity or actions; and
- any notes made by the academic/administrative staff about the student (including any disciplinary matters). Some items may be retained in the e-files.

4.5 In the event a third party wishes to gain access to the Student Record, written permission must be provided by the student, unless the request is made under subpoena.

Records Management, Security, Retention and Disposal Policy and Procedure

Staff Records Management

4.6 The Human Resource Officer maintains staff records.

4.7 Each staff member has a file created and maintained for the purpose of employment, which includes:

- recruitment paperwork;
- employment conditions / letter of offer / employment agreement;
- evidence of the 'right to work' in Australia;
- position description;
- evidence of participation in the staff induction process;
- certified copies of qualifications;
- verification of experience; and
- professional development and scholarly activity details.

4.8 Copies of original documentation, including qualifications, kept on file must be sighted to verify authenticity, and indicate the date sighted and by whom (refer *Staff Qualifications, Recruitment and Appointment Policy and Procedure*).

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

4.10 Staff may access information on their files on request to the Human Resource Officer.

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

Financial Records Management

4.12 Financial records are created, secured, retained and archived in compliance with contractual and legal requirements.

Security

4.13 PIA takes seriously its obligations under privacy legislation to safeguard all confidential information. PIA will also ensure that anyone acting on its behalf maintains appropriate confidentiality.

4.14 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.

4.15 PIA maintains a secure computer network. Each user has their own password which allows them access to specific functions and files within the system, as appropriate.

4.16 Physical records are kept in secure areas or locked filing cabinets and access is only available to authorised personnel.

4.17 IT infrastructure is protected and secured in the following ways:

- backups (including software as well as all data information) are sent off-site on a monthly basis to facilitate recovery;
- a remote backup facility is utilised to minimise data loss;
- surge protectors are employed to minimise the effect of power surges on electronic equipment;
- servers and essential equipment are protected with an Uninterruptible Power Supply (UPS) and/or backup generator;
- an effective alarm system and accessible fire extinguishers are installed in the case of a fire;
- anti-virus software, firewalls and other security measures are employed;
- electronic records are backed up each night;
- backups are rotated daily;
- the computer network is maintained by a programmed regimen of maintenance along with ad hoc support as and when required;
- Group Policy limited access and Symantec malware provide protection against in-house intrusions;
- cloud-based security for both RTO Manager and Moodle are used to protect against external intrusions; and
- the remote backup is tested at least twice a year to ensure it is working.

Notifiable Data Breaches

4.18 In the event of the data breach, PIA has adopted the Notifiable Data Breach scheme (NDBs). For further information, refer to the Data Breach Response Procedure.

4.19 The Office of the Australian Information Commissioner (OIAC) has identified Notifiable Data Breaches as follows:

4.19.1 An eligible data breach occurs when three criteria are met:

i. There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;
ii. This is likely to result in serious harm to one or more individuals; and
iii. The entity has not been able to prevent the likely risk of serious harm with remedial action.

4.19.2 ‘Serious harm’ can be psychological, emotional, physical, reputational, or other forms of harm. Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach.

4.20 Where PIA suspects a data breach, it will establish if the breach is 'likely to result in serious harm'. If serious harm is deemed likely, the following will occur.

4.20.1 an assessment will be undertaken within thirty (30) days of the breach becoming apparent; and

4.20.2 the OIAC, together with any and all individuals likely to be at risk of serious harm as a consequence of the breach, will be notified as soon as practicable.

4.21 The OAIC will be notified in a statement which includes the following:

- the identity and contact details of PIA;
- a description of the eligible data breach;
- the kind or kinds of information involved in the eligible data breach; and
- the steps PIA recommends in response to the eligible data breach.

4.22 Depending on the nature, severity and extent of the breach, the notification may be made publicly available in order to alert a wider audience.

Retention

4.23 All documents are retained as per Schedule 1 of this document. ~~the PROS/ 16/07 Retention and Disposal Authority for Records of the Higher and Further Education Functions 19/12/2016.~~

4.24 Refer to Schedule 1 accompanying this policy for details on the Retention Schedule for all documents.

Disposal

4.25 Records will be disposed of in accordance with the Australian Privacy Principles Guidelines for information held by an organisation.

4.26 Where personal information is no longer required for any legitimate and sanctioned purpose, PIA will take reasonable steps to destroy and/or de-identify the information, together with any copies of the information, including archived records and back-ups.

4.27 All records are disposed of by secure means, including internal shredders to shred documents that contain personal or financial information. Professional shredding companies may be contracted to bulk-shred archive items as they approach their date of destruction.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The Administration Manager is responsible for ensuring that this policy is adhered to by all staff.

5.2 This policy is managed and reviewed by the Executive Management Committee and ratified by the Board of Directors.

Reporting

5.3 Items within sections 4.18 – 4.22 of this policy must be reported to the OIAC and affected parties.

Records management

5.4 Staff must maintain all records relevant to administering this policy and procedure in a recognised PIA recordkeeping system.

5.5 All records are maintained as prescribed in Schedule 1 of this policy.

6 DEFINITIONS

6.1 Terms not defined in this document may be in the PIA glossary.

7 RELATED LEGISLATION AND DOCUMENTS

Documents

IT Usage Policy and Procedure
Records Management, Security, Retention and Disposal Schedule
Staff Qualifications, Recruitment and Appointment Policy and Procedure

PROS/ 16/07 Retention and Disposal Authority for Records of the Higher and Further Education Functions 19/12/2016
The Privacy Act 1988

Higher Education Standards Framework

7.1 This policy and procedure complies with the Higher Education Standards Framework (Threshold Standards) 2015, Standard 7.3, which states:

1. *Information systems and records are maintained, securely and confidentially as necessary to:*

   b. *prevent unauthorised or fraudulent access to private or sensitive information, including information where unauthorised access may compromise academic or research integrity.*

7.2 Education Services for Overseas Students Act 2000

This policy and procedure complies with Section 21 of the ESOS Act:

Records Management, Security, Retention and Disposal Policy and Procedure

21 Record keeping

Records of students' details

(1) A registered provider must keep records of each accepted student who is enrolled with the provider or who has paid any tuition fees for a course provided by the provider.

(2) The records must consist of the following details for each accepted student:

(a) the student's current residential address;

(b) the student's mobile phone number (if any);

(c) the student's email address (if any);

(d) any other details prescribed by the regulations.

(2A) A registered provider must have a procedure to ensure that, at least every 6 months, while the student remains an accepted student of the provider:

(a) the provider confirms, in writing, the details referred to in subsection (2) with the student; and

(b) the records are updated accordingly.

xRecords of assessment

(2B) If:

(a) an accepted student of a registered provider completes a unit of study for a course; and

(b) the student's progress in that unit is assessed;

the provider must record the outcome of the student's assessment for the unit.

(2C) A record under subsection (2B) must be:

(a) kept in accordance with any requirements prescribed by the regulations; and

(b) kept up-to-date.

Retention of records

(3) The provider must retain records kept under this section for at least 2 years after the person ceases to be an accepted student. However, the records do not need to be kept up-to-date after the cessation.

8 FEEDBACK

8.1 PIA staff and students may provide feedback about this document by emailing policy@pia.edu.au.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Executive Management Committee
Administrator	CEO

Records Management, Security, Retention and Disposal Policy and Procedure