OZFORD
Institute of Higher Education

PRIVACY POLICY

Approving authority	Governing Board
Purpose	This policy outlines how the Institute collects, uses, discloses and otherwise manages personal information.
Responsible Officer	President and CEO
Next scheduled review	September 2026
Document Location	http://www.ozford.edu.au/higher-education/policies-and-procedures/
Associated documents	Human Resources Policy and Procedure (Manual) Student Grievances and Appeals Policy and Procedure Records Management Policy and Procedure Privacy Procedure

1. PRINCIPLES

Ozford Institute of Higher Education's (hereafter referred to as 'the Institute') role as a provider of higher education requires it to collect, store, use and disclose personal information relating to its staff and students.

The Institute is committed to protecting the privacy of personal information while honouring its obligations under the *Privacy Act 1988 (Cth)* (Privacy Act), the *Australian Privacy Principles* (APPs) and the *Health Privacy Principles* which are contained in the *Health Records Act 2001 (Vic)* (Health Records Act).

This Privacy Policy is based on the APPs and explains how the Institute collects, uses, manages, discloses and otherwise handles personal information. It explains how information might be accessed or corrected and how a suspected privacy breach might be investigated.

2. SCOPE

This policy applies all staff and contractors involved in in Institute services that involve collecting, using, managing, disclosing and otherwise handling personal information.

3. DEFINITIONS

APPs

The Australian Privacy Principles (APPs) means the set of 13 principles in the *Privacy Act 1988* (Cth) governing the collection, use, disclosure, management and transfer of personal information by Commonwealth government agencies and private entities with an annual turnover of more than $3 million or with contracts with the Australian Government. The APPs regulate the manner in which personal information is handled throughout its life cycle, from collection, to use and disclosure, storage, access and disposal.

Consent

Consent means express consent or implied consent. The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the Institute.

Data breach

A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

De-identified information

Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'. De-identified information is not 'personal information'

European Union's (EU's) General Data Protection Regulation (GDPR)

Australian businesses may need to comply with the European Union's (EU's) General Data Protection Regulation (GDPR) if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.

Health information

Health information has the meaning given to it in section 3 of the *Health Records Act 2001* (Vic).

Health Privacy Principles

Health Privacy Principles means the set of 11 principles in the *Health Records Act 2001* (Vic) governing the collection, management, use, disclosure and transfer of health information by organisations such as the Institute.

Information Privacy Principles

Information Privacy Principles means the set of 10 principles in the *Privacy and Data Protection Act 2014* (Vic) governing the collection, use, disclosure, management and transfer of personal information by organisations such as the Institute.

Notifiable Data Breaches (NDB) scheme

The NDB scheme in the Privacy Act requires entities to notify affected individuals and the Australian Information Commissioner (the Commissioner) of certain data breaches. The NDB scheme requires entities to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.

- The entity has been unable to prevent the likely risk of serious harm with remedial action.
- Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

Personal information
Personal information has the meaning given to it by Privacy legislation.

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

Sensitive information
Sensitive information is a subset of personal information that is generally afforded a higher level of privacy protection. Sensitive information is information or opinion about an individual's:

- membership of a political association;
- racial or ethnic origin;
- health or disability;
- membership of a professional or trade association or membership of a trade union;
- political opinions;
- religious beliefs, affiliations or philosophical beliefs;
- criminal record; or
- sexual preferences or practices.

Sensitive information can only be used and disclosed only for the purpose for which it was provided or for a directly related secondary purpose, unless the information provider agreed otherwise, or the use or disclosure of the sensitive information is allowed by law.

Staff
All references to staff refer to any person appointed, contracted or engaged by the Institute that works in Institute services that involve collecting, using, managing, disclosing and otherwise handling personal information.

4. POLICY

4.1 The Institute respects the privacy of anyone who interacts with it and is committed to protecting and managing personal and health information in an open and transparent way. This commitment arises not only from a wish to comply with its legal obligations but also in recognition of and commitment to information privacy as one of the foundations of human dignity.

4.2 The Institute complies with the *Privacy and Data Protection Act 2014* (Vic), the *Health Records Act 2001* (Vic) and the *Privacy Act 1988* (Cth), where required by contract or legislation. In circumstances where the GDPR applies to the Institute's activities, the Institute will act in accordance with its requirements.

4.3 As part of operating the Institute, the Institute collects information for various purposes, including for:

- the provision of education and related activities; and

- the employment of staff and engagement of contractors and other persons to deliver services.

4.4 The Institute collects personal information from a variety of sources including:

- prospective staff.
- individuals who are customers of the organisation or party in question.
- clients.
- business partners.
- suppliers.
- contractors.
- shareholders.
- Students:
  - when a course enquiry is made;
  - when a person applies for admission to the Institute;
  - when a person enrols for a course or unit offered by the Institute; and
  - when a person applies for a job in the Institute;
- other people who may come into contact with the Institute.

4.5 All staff and contractors must in performing the duties of their employment, appointment or engagement:

- be proactive in its approach to privacy protection by anticipating and preventing invasive events before they occur.
- embed privacy considerations into the design and architecture of information technology systems and business processes.
- respect the privacy of Personal and Health Information that they collect, use or disclose; and
- comply with the requirements of all applicable personal data protection laws, this ***Privacy Policy*** and the related ***Privacy Procedure***.

Collection of Information

4.6 Personal and Health Information must be collected only:

- where necessary and relevant to the Institute's functions and activities and where there is a specific and immediate need to do so; and
- in a lawful, fair and not unreasonably intrusive way.

4.7 Where lawful and practicable, individuals may choose not to identify themselves when transacting with the Institute. However, the Institute may consequently be unable to provide services in these circumstances.

4.8 Sensitive information must only be collected where the individual has provided consent, or where the collection:

- is required by law; or
- is otherwise authorised under the *Privacy and Data Protection Act 2014 (Vic)* or the *Health Records Act 2001 (Vic)*.

4.9 When collecting Personal and Health Information directly from an individual, whether by verbal, written or electronic means, all reasonable steps must be taken to ensure that the individual providing

such information is made aware of how their information will be used and with whom it might be shared or communicated in an appropriate collection statement.

4.10 Personal or Health Information must not be collected from individuals if it is reasonable and practicable to transact with them without collecting this type of information.

4.11 The collection statement must include:

- the purpose for which the information is being collected (the proposed use) and to whom it might be disclosed.
- the area collecting the information and how to contact it.
- that the individual is able to gain access to the information
- any law that requires the particular information to be collected
- the main consequence (if any) for the individual if all or part of the information is not provided to the Institute.

4.1 The Institute collects personal information from its students and staff through a variety of lawful and fair means including:

- on printed forms.
- through email exchange.
- over the phone.
- through written correspondence.
- in person.

4.2 The type of information the Institute collects and holds is set out in Appendix 1.

4.12 The Institute handles student records as set out in the ***Records Management Policy and Procedure.***

4.13 The Institute handles staff health records in accordance with the Health Privacy Principles as set out in the ***Human Resources Policy and Procedure (Manual).***

Use and Disclosure

4.14 Personal and Health Information collected in the course of the Institute's activities must be used only for the primary purpose of collection, a related secondary use reasonably anticipated by the individual, where an individual has consented, or where authorised by law.

4.15 Staff must only access Personal or Health Information to the extent necessary to perform their work. The particular purpose for which personal information is collected by the Institute is specified or reasonably apparent at the time the information is collected.

4.16 The Institute only discloses personal information for the purpose which was either specified or reasonably apparent at the time when the information was collected. All staff must seek advice from the Head of Department prior to any use or disclosure that is not for the primary purpose of collection or a related secondary use that would be reasonably anticipated by the individual.

4.17 Staff must refer all requests that require disclosure by law to the Privacy Officer, the CEO and President.

4.18 The reference in privacy law to personal information being 'recorded in any form' does not diminish the obligation of staff to hold in confidence all information of a personal nature obtained in any manner, including verbally, in the course of their employment, appointment or engagement.

4.19 Staff must take reasonable steps to ensure that Personal and Health Information collected, used or disclosed is accurate, complete and up to date.

4.20 The Institute also obtains personal information about volunteers who assist the Institute in its functions or conduct associated activities, such as alumni associations, to enable the Institute and the volunteers to work together.

Marketing and the Institute Website

4.21 The Institute will only publish personal information on its website if that information has been collected for this purpose, and only with the knowledge and consent of the individual concerned.

4.22 The Institute may use personal information to send information about the Institute's services and in enrolment reminders, study suggestions, and invitations to participate in forums or surveys.

4.23 Parents, staff, contractors and other members of the wider community may from time to time receive marketing and fundraising information. Institute publications, such as newsletters and magazines, which include personal information, may be used for marketing purposes.

Use of Unique Identifiers

4.24 The Institute will not assign unique identifiers unless it is necessary to carry out its functions efficiently. Staff and student identification numbers are considered necessary for this reason.

4.25 The Institute will not adopt as its own a unique identifier assigned to an individual by another organisation (eg. tax file number, driver's licence number).

4.26 The use or disclosure of a unique identifier (ie. Tax File Numbers) assigned to an individual by another organisation will comply with all legislative requirements.

Data security and disposal

4.27 The Institute will take reasonable steps to ensure that the information it handles is protected from misuse, loss, unauthorised access, modification and disclosure.

4.28 The Institute will take reasonable steps to destroy or permanently de-identify personal or sensitive information if it is no longer legally required to be held. The Institute's requirements in relation to the destruction of documents are governed by the ***Records Management Policy and Procedure***.

4.29 The Institute will only destroy or permanently de-identify health information in accordance with the Health Records Act 2001 (Vic).

Access to and Correction

4.30 The Institute takes all reasonable steps to ensure that any personal information it collects, uses and discloses is accurate, up to date, complete and (in the case of use or disclosure) relevant.

4.31 Individuals are required to keep personal information accurate and up to date, advising the Institute in writing of any changes required.

4.32 Any person may request access to own personal information held by the Institute and to request its correction if the information held is inaccurate, incomplete or outdated.

4.33 The request for access or any requested changes will be dealt with in a reasonable manner and time.

Data Subject Rights of European Economic Area/United Kingdom Residents

4.34 In addition to the rights of access and correction above and subject to any conditions and exemptions in the GDPR, the Institute will respect the rights of residents of the European Economic Area and the United Kingdom to:

- object to processing of their personal information.
- request suspension of processing of their personal information
- transfer their personal information held in electronic form to them or a third party in a structured, commonly used, machine-readable form;
- withdraw their consent to processing where Deakin's right to process is based only on their consent.

Transferring Personal Information

4.35 The Institute does not transfer personal information unless it is authorised by law to do so or consent has been gained as part of the services it provides.

4.36 The Institute will only send information outside of Victoria:

- if the recipient is subject to principles for fair handling of information that are substantially similar to Victoria's.
- with the individual's consent, or if it is impracticable to obtain their consent if the transfer is for their benefit and they would be likely to consent if they could.
- if contracting with the individual, or with a third party for the individual's benefit (such as education agents); or
- in accordance with the applicable legislation.

4.37 The Institute will use online or 'cloud' service providers to store personal information and to provide services that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information will be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

4.38 If the Institute engages a third-party contractor to perform services which involves handling personal information, the Institute will ensure that the contractor will be subject to the same privacy obligations as the Institute to protect personal information. The Institute will also take reasonable steps to prohibit the contractor from using personal information, except for the purposes for which it was supplied.

Complaints

4.39 If a person believes that the Institute has failed to handle their personal information in accordance with this ***Privacy Policy***, a formal complaint should be made as follows:

- complaints must be made within six (6) months of the time the complainant first became aware of the alleged breach
- where the complainant is a student, any complaint will be dealt with under the ***Student Grievance and Appeals Policy and Procedure*** which is located on the Institute website.
- where the complainant is a staff member, any complaint will be dealt with asset out in the ***Human Resources Policy and Procedure (Manual)***.
- where the complainant is neither a currently enrolled student nor a current staff member, complaints must be forwarded in writing to the CEO and President who will be responsible for:
  - appointing an appropriate person to undertake an investigation of the complaint and to provide recommendations to the Privacy Officer as to an appropriate response;
  - determining what actions the Institute will take;
  - providing a written response in respect of the outcome to the complainant, and
  - advising relevant Institute personnel of actions required to remedy the interference with the complainant's privacy (if any).

Responding to a Data Security Breach

4.40 The Institute will take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate any incident as follows:

- Step 1: Contain the data breach to prevent any further compromise of personal information.
- Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
- Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.
- Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

Note: Appendix 2 includes the OAIC Diagram summarising the data breach response process. The Institute's data breach response plan is set out in the Privacy Procedure.

4.41 The Executive Team will be responsible for co-ordinating and managing the data breach response including all communications with external stakeholders.

4.42 The Institute will comply with its obligation to notify affected individuals and the Office of the Australian Information Commissioner when a data breach is likely to result in serious harm to an individual whose personal information is involved. The Institute will also ensure that it complies with any other external reporting obligations.

4.43 The Executive Management Team will report any privacy security breach to the Audit and Risk Committee and the Governing Board.

Review

4.44 The Institute will, from time to time, review and update this ***Privacy Policy*** to take account of new laws and technology, changes to its operations and practices and to make sure it remains appropriate to the changing environment.

4.45 After a privacy security breach, the Institute will evaluate how a data breach occurred, and the success of the response, where necessary make changes to improve data handling and data breach management.

5. QUALITY ASSURANCE

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

5.1 internally endorsed by the Executive Management Team on development or review, prior to approval by Governing Board, or the Academic Board or other delegated authority;

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 policy is welcomed by the listed Responsible officer of the Institute.

7. ACKNOWLEDGEMENT

This policy was developed with reference to the following:

- Office of the Australian Information Commissioner and Privacy Commissioner website resources.
- Deakin University, Privacy Policy, 2022 (https://policy.deakin.edu.au/document/view-current.php?id=139)
- Victoria University, Privacy Policy, 2019 (https://policy.vu.edu.au/document/view.php?id=166)
- University of Melbourne, Privacy Policy, 2022 (https://policy.unimelb.edu.au/MPF1104/)
- Independent Schools Council of Australia and National Catholic Education Commission Privacy Compliance Manual, August 2016

8. VERSION CONTROL

Version	Date approved	Description	Approved by
1.0	February 2014	Initial issue	GB
2.0	September 2017	Internal review	GB
3.0	September 2018	Internal review	GB
4.0	September 2023	Internal Review	GB
Related legislation/ regulation/standard	Tertiary Education Quality and Standards Act 2011 Higher Education Standards Framework (Threshold Standards) 2021 Education Services for Overseas Students Act (ESOS) 2000 Education Services for Overseas Students Regulations 2019 The National Code of Practice for Providers of Education and Training to Overseas Students 2018 Privacy Act 1988 (Cth). Privacy and Data Protection Act 2014 (Vic), Health Records Act 2001 (Vic), Public Records Act 1973 (Vic) Australian Privacy Principles (APPs) Health Privacy Principles Information Privacy Principles European Union General Data Protection Regulation (GDPR)		

GB = Govering Board

Appendix 1: Personal Information collected by the Institute

The Institute collects personal information for the primary purpose of providing students with the courses of study for which they are enrolled and the associated services to individuals. Personal information may be collected for purposes related, or ancillary to, the primary purpose of collection. This includes:

- administering and managing the services provided by the Institute to prospective and current students, including admission and enrolment;
- the delivery of courses including teaching, learning and assessment functions;
- marketing the services of the Institute to prospective, current and past students;
- guiding students in their study options;
- providing student counselling services;
- conducting surveys;
- keeping students informed about matters related to education services, through correspondence, newsletters and magazines; conducting research for service improvement purposes and to compile statistics and analyse trends; and
- the regulation of student visas and Australian immigration laws generally under the Education Services for Overseas Students Act 2000, and the National Code of Practice for Providers of Education and Training to Overseas Students 2018.

In relation to personal information of job applicants and contractors, the primary purpose of collection is to assess and (if successful) to engage the applicant or contractor, as the case may be.

The purposes for which the Institute uses personal information of job applicants and contractors include

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing; and
- satisfying legal obligations.

The type of information the Institute collects and holds includes (but is not limited to) personal information, including health and other sensitive information, about:

- students and families (Parents/legal guardians/carers) before, during and after the course of an enrolment at the Institute, including:
    - name, contact details (including next of kin), date of birth, previous education/school and religion;
    - medical information (e.g. details of disability and/or allergies, absence notes, medical reports and names of doctors);
    - conduct and complaint records, or other behaviour notes, and academic reports;
    - information about referrals to government welfare agencies;
    - counselling reports;
    - health fund details and Medicare number (if applicable);
    - information about the disability support needs of individual students, to assist with special needs and to develop disability access plans where appropriate;
    - health information that may be relevant to an individual student's failure to achieve a satisfactory course outcome. any court orders;
    - volunteering information; and
    - photos and videos at Institute events;

- job applicants, staff members, volunteers and contractors, including:

- name, contact details (including next of kin), date of birth, and religion;
- information on job application;
- professional development history;
- salary and payment information, including superannuation details;
- medical information (e.g. details of disability and/or allergies, and medical certificates);
- complaint records and investigation reports;
- leave details;
- photos and videos at Institute events;
- workplace surveillance information;
- work emails and private emails (when using work email address) and Internet browsing history; and

- other people who come into contact with the Institute, including name and contact details and any other information necessary for the particular contact with the Institute.

The Institute will generally collect personal information held about an individual by way of forms filled out by students (or their parents/legal guardians), face-to-face meetings and interviews, emails and telephone calls. On occasions people other than students (or their parents/legal guardians) such as education agents provide personal information.

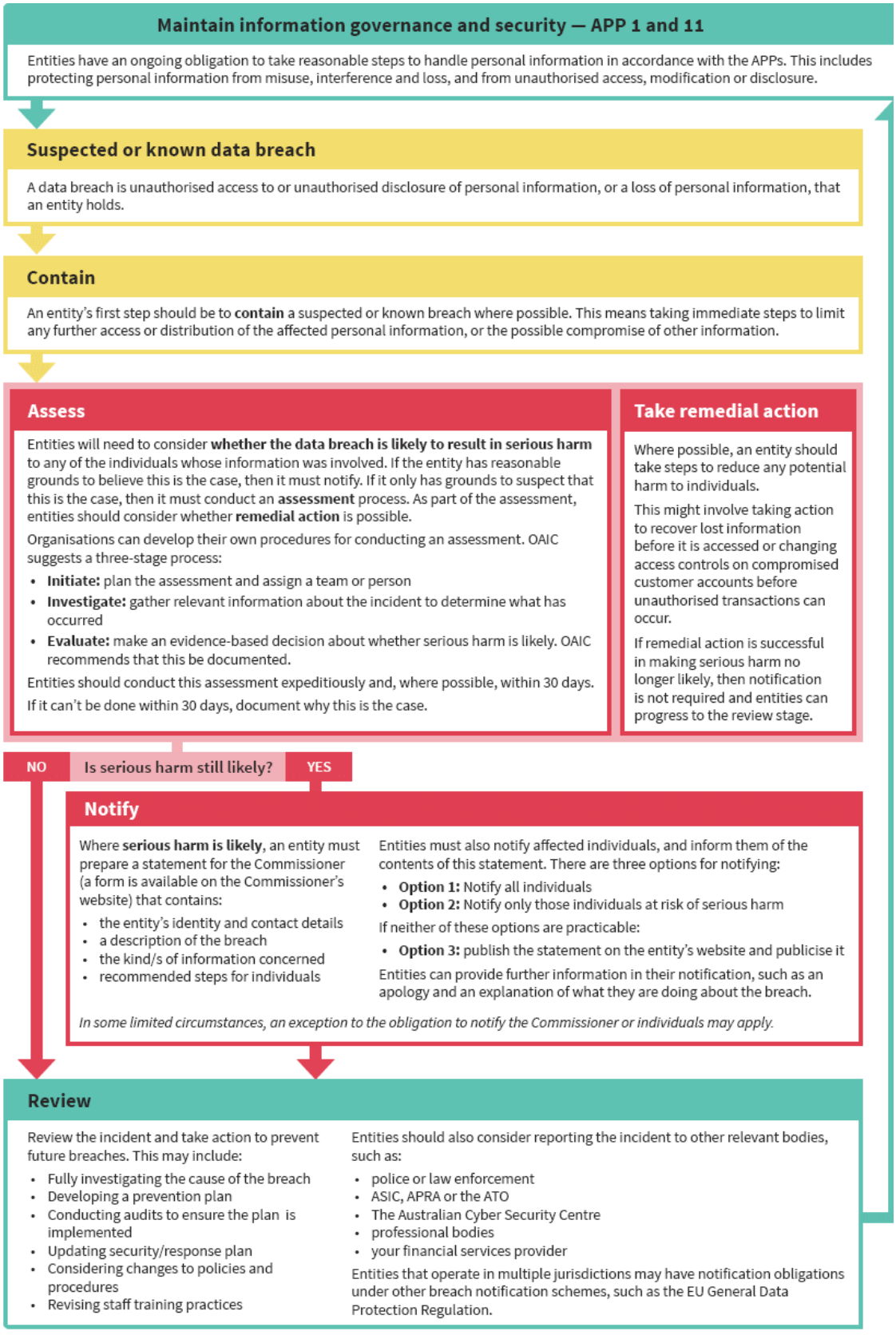
In some circumstances the Institute may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another education provider.

On occasions, the Institute may collect personal information about students from:

- Commonwealth and State agencies;
- Education agents who may be based in Australia or overseas;
- a company for whom you work;
- other individuals and/or organisations with whom you have any dealings;
- an employment recruitment agent or agency;
- a student related recruitment agent or agency;

Staff may use online or 'cloud' service providers to store personal information and to provide services that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

Appendix 2 OAIC Diagram summarising the data breach response process



Source : Part 3: Responding to data breaches – four key steps | OAIC