OZFORD
Institute of Higher Education

PRIVACY PROCEDURE

Approving authority	Governing Board
Purpose	This Procedure outlines how the Institute collects, uses, discloses and otherwise manages personal information.
Responsible Officer	President and CEO
Next scheduled review	August 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 Policy

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 Procedure explains how the Institute collects, uses, manages, discloses, and otherwise handles the personal information. It explains how information might be accessed or corrected and how a suspected privacy breach might be investigated.

2. SCOPE

This procedure applies all staff and contractors involved 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 (Privacy)

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 in section 3 of *the Privacy and Data Protection Act 2014* (Vic).

Record
A record is a document or an electronic or other device.

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;
- 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. PROCEDURE

4.1 The overall responsibility for protecting the privacy of all personal information held by the Institute resides with the President and CEO. The President and CEO is the Privacy Officer and the first point of contact for privacy queries. The Executive Management team members can also assist with privacy matters or if there is data breach.

4.2 All staff have responsibility for protecting and managing personal and health information in an open and transparent way and ensuring that all personal information is handled throughout its life cycle, from collection, to use and disclosure, storage, access and disposal in compliance with the Privacy Policy.

Collection of Personal Information

4.3 When collecting information about an individual, staff must:

- only collect information if it is needed (i.e. only collect information if it is necessary for one or more of Institute's functions and activities);
- Wherever possible, collect the information directly from the individual concerned;

- ensure that the information is collected lawfully, securely and fairly;
- ensure the collection is not unreasonably intrusive; and
- tell people that their information is being collected, why it is being collected and how it is to be used.

4.4 Before or at the time of collecting information, staff must take reasonable steps to ensure that the person who is providing the information is aware of the following:

- the identity of the organisation collecting the information and how it can be contacted;
- The purpose(s) for which the information is being collected (e.g. student enrolment, research, marketing etc.);
- How the information being collected will generally be used and to whom it is usually disclosed;
- The fact that the individual is able to gain access to the information;
- Whether the collection of the information is required by law;
- Any consequences of not providing the information (e.g. the Institute may not be able to provide a particular service); and
- The fact that the Institute has a Privacy Policy, which is available on the website, and a Privacy Officer who can be contacted with queries or concerns.

4.5 If information about an individual is to be collected from someone other than that individual (for example another institution or a parent), staff must ensure that the Institute has the individual's written permission.

4.6 If information is collected about an individual from someone other than the individual, staff must take reasonable steps must be taken to ensure that the individual is made aware of the matters listed above.

4.7 Staff must handle staff health records in accordance with the *Health Privacy Principles*. The collection of health information is subject to very stringent legislative requirements, and it must only be collected if it is essential. Health information is very broadly defined and includes information or an opinion about the physical, mental or psychological health of an individual or a disability or a health service provided to an individual.

Use and Disclosure

4.8 Staff must use personal information for the purpose specified or reasonably apparent at the time the information is collected and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which it was consented.

4.9 Staff can share personal (but not sensitive) information with other Ozford entities engaged to deliver Institute services. This allows the Institute to transfer information between Ozford College Pty Ltd, Ozford English Language Centre Pty Ltd and Ozford Business College Pty Ltd.

4.10 All reasonable steps must be taken by staff to destroy hard copies of personal information that are obsolete or no longer required by the Institute. Destruction of personal information is undertaken by secured means authorised by the Head of Marketing and Student Experience.

4.11 In some cases where personal information is requested about an individual, if the information is not obtained, staff may not be able to continue the activity. For example, for a student, the enrolment may not be offered or the student may not be permitted to take part in a particular activity.

4.12 Staff may only disclose a personal information for the purpose which was either specified or reasonably apparent at the time when the information was collected.

4.13 Staff may disclose personal information to:

- the related entities, Ozford College Pty Ltd and Ozford English Language Centre Pty Ltd and Ozford Business College Pty Ltd;
- State and Commonwealth Government departments including the Department of Education and Training, the Department of Home Affairs and the Tuition Protection Service in compliance with the ESOS legislative requirements and their successors;
- the regulator, the Tertiary Education Quality and Standards Agency, and its successors;
- anyone that a student or employee has authorised for disclosure information; and
- any other person with a lawful entitlement to obtain the information.

4.14 In certain exceptional circumstances, a formal authority may not be required. Staff may disclose personal information where consent is given to the Institute to do so or the Institute believes that disclosure is necessary to lessen or prevent a serious threat to life, health, or safety or the disclosure is necessary to assist in locating a person who has been reported as missing or the disclosure is required by law, regulation or a court/tribunal body.

Marketing and the Institute Website

4.15 Staff can 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.

- Students are asked to consent to use of personal information as part of the admission and enrolment processes.
- Staff are asked to consent to use of personal information as part of the recruitment and induction processes.

4.16 When giving such consent, staff should ensure that the individual is made aware that information published on the Institute's website is accessible to millions of users from all over the world, that it will be indexed by search engines and that it may be copied and used by any web user. This means that once the information is published on the Institute website, the Institute will have no control over its subsequent use and disclosure.

4.17 Where authority is held, staff can use personal information collected about students and staff in marketing about the Institute's services, enrolment reminders, study suggestions, and invitations to participate in forums or surveys.

4.18 Staff can also use Institute publications, such as newsletters and magazines, which include personal information, for marketing purposes.

Use of Unique Identifiers

4.19 Staff 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.

4.20 Staff must not adopt as its own a unique identifier assigned to an individual by another organisation (eg. tax file number, driver's licence number).

4.21 Staff must ensure that the use or disclosure of a unique identifier (ie. Tax File Numbers) assigned to an individual by another organisation complies with applicable legislation.

Transferring Personal Information

4.22 Staff sending information outside of Victoria as part of the Institute's functions and activities (e.g. overseas for its international students) must only do so:

- if the recipient is subject to privacy principles for fair handling of information that are substantially similar to Victoria's; or
- 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; or
- 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.

4.23 Staff should not send any health information outside of Victoria. The Executive Management team should be consulted if there is a reason to do so and all staff must comply with the additional requirements of the Health Records Act 2001 (Vic) when sending health information outside of Victoria.

4.24 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.

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

Data security and disposal

4.26 Staff are required to respect the confidentiality of personal information and the privacy of individuals. All staff and each operational area must take reasonable steps to ensure that:

- information is secure and protected from unauthorised use, access, disclosure, modification or loss, whether deliberate or inadvertent.
- practices, procedures and systems (including electronic and physical) are in place to ensure that the information is stored (and if necessary, moved) safely and securely;
- the information has not been changed or been tampered with;
- all records containing personal, sensitive and health information are kept in a secure location and cannot be accessed by unauthorised persons;
- authentication processes (for identification) are adhered to, in that a person accessing or providing information are who they claim to be; and

- requirements around retention of information are complied with, according to the ***Records Management Policy and Procedure*** and the ***ICT Acceptable Use Policies and Procedures (Staff and Students)***.
- subject to the Institute's obligations under legislation, destroyed or permanently de-identified when it is no longer needed by the Institute. The Institute's requirements in relation to the destruction of documents are governed by the ***Records Management Policy and Procedure***;
- health information is managed in accordance with the Health Records Act 2001 (Vic).

4.27 If staff are seeking to develop or implement new ICT systems which are likely to involve the collection, storage and/or disclosure of individuals' information, they must ensure the system is compliant with this Privacy, ICT and Records Management requirements.

Access to and Correction

4.28 Staff should ensure that any personal information is accurate, up to date, complete and (in the case of use or disclosure) relevant.

4.29 Individuals, including all staff and students, must keep their personal information accurate and up to date, advising the Institute in writing of changes required.

4.30 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.

- Students can make a request to access or to update any personal information, the person can contact Student Experience team by telephone or in writing using the contact information on the website; and
- Staff can make a request to their supervisor;
- Contractors can make a request to their contract manager.

4.31 If a staff member receives a request from a student or staff member to access or obtain their own information:

- the identity of the individual should be verified before any information is provided.
- the information required should be specified and staff should assess the cost of collating this information;
- staff should assess whether a fee should be charged to cover the cost of verifying an application and locating, retrieving, reviewing and copying any material requested. If so, the individual should be advised about the cost and pay it prior to the work to collate the information commencing.

4.32 Staff must deal with any request for access or any requested changes within a reasonable manner and time.

4.33 There may be occasions where a request from an individual will need to be carefully considered before a determination can be made about whether the information can be disclosed. Where a request for access is denied, the Executive Management team should be consulted and the reasons must be provided. For example:

- The information may not be able to be disclosed where the information was given in confidence, or where disclosure may have an unreasonable impact on another person's privacy; or

- If the person will not accept the cost of collating information.

4.34 The age at which a person's privacy rights come into effect is not specified. The general principle is that a child or young person may exercise their rights independently (of a parent or legal guardian) if they have sufficient understanding and intelligence to give valid consent or to make their own decisions. The Institute will consider that its students are sufficiently mature and intelligent to make their own decisions in relation to the distribution of their personal information, even if that student is less than 18 years of age. Student personal information should not be provided to parents or to other family members in the absence of the express consent of the student. There may be exceptions to this rule — for example, if a student has an intellectual disability or is subject to a Guardianship Order.

4.35 Staff should act to correct personal information:

- if satisfied, independently of any request, that personal information it holds, is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which the information is held.
- where an individual is able to satisfactorily demonstrate that it is inaccurate.

4.36 If an individual and staff disagree about whether their information is inaccurate, the individual may request that the Institute associate with the information a statement setting out that the individual believes the information to be inaccurate. Staff must take reasonable steps to accommodate such a request.

4.37 Where a request for a correction is denied, staff must ensure that the reasons are provided in writing by email or a letter.

Data Subject Rights of European Economic Area/United Kingdom Residents

4.38 Staff should ensure that the rights of residents of the European Economic Area and the United Kingdom are respected including their right 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

4.39 Staff must 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.

4.40 Staff sending information outside of Victoria as part of the Institute's functions and activities must only do so:

- 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; or
- in accordance with the applicable legislation.

4.41 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.

4.42 If staff engage a third-party contractor to perform services which involves handling personal information, staff must ensure that the contractor is subject to the same privacy obligations as the Institute to protect personal information. Staff must also prohibit the contractor from using personal information, except for the purposes for which it was supplied.

Complaints

4.43 If a student believes that the Institute has failed to handle the personal information in accordance with this Privacy Procedure, a formal grievance can be made. Staff will check that the complaint is within six (6) months of the time the complainant first became aware of the alleged breach. The Institute will investigate any complaint and will notify in writing of a decision in relation to the complaint as soon as is practicable after it has been made.

4.44 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. Alternatively, a copy may be requested from the Student Experience team who can discuss the concern with students, provide information about the complaints process and advocate for students.

4.45 Where the complainant is a staff member, any complaint will be dealt with asset out in the ***Human Resources Policy and Procedure (Manual).***

4.46 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:

- appoint an appropriate person to undertake an investigation of the complaint and to provide recommendations as to an appropriate response;
- determine what actions the Institute will take;
- provide a written response in respect of the outcome to the complainant, and
- advise relevant Institute personnel of actions required to remedy the interference with the complainant's privacy (if any).

Data breach response plan

4.47 There is no single way the Institute will respond to a privacy security breach if one occurs, as privacy security breaches can be caused or exacerbated by a number of factors. Each breach will be dealt with by the Institute on a case-by-case basis, with the Institute undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

4.48 There are four key steps to be followed when responding to a privacy security breach or suspected privacy security breach:

- 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.

Appendix 1 provides the OAIC diagram setting out this process.

Step 1: Contain the Breach

4.49 If any person within the Institute discovers, suspects or is made aware of a privacy security breach, that person should escalate the matter immediately to the CEO and President or a member of the Executive Management Team so that the Institute can take necessary and practicable steps to address and contain the breach.

4.50 What steps are necessary to contain the data breach will depend on the nature of the breach but may include:

- recovery of any records containing personal information;
- shutting down any electronic system that has been interfered with;
- revoking or changing access privileges; and/or
- addressing weaknesses in physical or electronic security.

Step 2: Evaluate the Risks Associated with the Breach

4.51 The Institute will assess the risks associated with the data breach. In doing so, it may consider the following factors:

- The type(s) of personal information involved
  - Some types of personal information are more likely to cause individual harm if compromised (for example, an individual's academic information, financial information, or health or other sensitive information), whether that harm is physical, financial or psychological.
- The context of the affected information and the breach
  - What parties may have gained unauthorised access to the affected information? Did the breach involve disclosure to an unknown party or to a party where there is a potential risk of misuse, or to a trusted, known entity or person that would reasonably be expected to return or destroy the information without disclosing or using it?
  - Have there been other breaches that could have a cumulative effect? A number of small, seemingly insignificant, breaches may have a cumulative effect. Separate breaches that might not, by themselves, be assessed as representing a real risk of serious harm to an affected individual, may meet this threshold when the cumulative effect of the breaches is considered.
  - How could personal information be used? Could the information be used for fraudulent or otherwise harmful purposes, such as to cause financial loss to the affected individual or to cause significant embarrassment to the affected individual? Could the compromised

information be easily combined either with other compromised information or with publicly available information to create a greater risk of harm to the individual?

- Establish the cause and extent of the breach
  - Is there a risk of ongoing breaches or further exposure of the personal information? What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or online?
  - Is there evidence of theft? Is there evidence that suggests theft, and was the personal information the target? For example, where a laptop is stolen, can it be determined whether the thief specifically wanted the information on the laptop?
  - Is the personal information adequately encrypted, anonymised or otherwise not easily accessible? Is the information rendered unreadable by security measures that protect the stored personal information? Is the personal information displayed or stored in such a way so that it cannot be used if breached?
  - What was the source of the breach? For example, did it involve external or internal malicious behaviour, or was it an internal processing error? Does personal information seem to have been lost or misplaced? The risk of harm to the individual may be less where the breach is unintentional or accidental, rather than intentional or malicious.
  - Has the personal information been recovered? For example, has a lost laptop been found or returned? If the personal information has been recovered, are there any signs that it has been accessed, copied or otherwise tampered with?
  - What steps have already been taken to mitigate the harm? Has the Institute adequately and effectively contained the breach? Have compromised security measures such as passwords been replaced? Has the full extent of the breach been assessed? Are further steps required?
  - How many individuals are affected by the breach? If the breach is a result of a systemic problem, there may be more people affected than first anticipated. Even where the breach involves accidental and unintentional misuse of information, if the breach affects many individuals, the scale of the breach may create greater risks that the information will be misused. The Institute's response to the breach will be proportionate to the scale.
- Assess the risk of harm to the affected individuals. Examples of the types of harm to individuals that could result from a privacy security breach include:
  - identity theft;
  - financial loss;
  - the threat to physical safety;
  - the threat to emotional wellbeing;
  - loss of academic, business or employment opportunities; and/or
  - humiliation, damage to reputation or relationships.
- Assess the risk of other harms - Other possible harms associated with a breach of privacy security, including to the Institute include:
  - the loss of public trust in the Institute;
  - reputational damage;
  - loss of assets (eg. stolen computers or storage devices);
  - financial exposure (eg. if bank account details are compromised or if financial compensation is paid by the Institute); and/or
  - legal proceedings (eg. formal complaint).

Step 3: Consider whether Notification is Appropriate and, if so, undertake a Notification Process

4.52 If the Institute suspects an eligible data breach has occurred, the Institute must make an assessment of the suspected eligible data breach under step 2 of this procedure with 30 days.

4.53 The Institute should take any remedial action during the assessment period that is appropriate given the circumstances of the suspected eligible data breach.

4.54 The Institute will consider the particular circumstances of a privacy security breach and decide whether to notify affected individuals; and, if so consider:

- when and how the notification should occur, who should make the notification, and who should be notified;
- what information should be included in the notification; and
- who else (other than the affected individuals) should be notified.

4.55 Notification may be an important mitigation strategy following a privacy security breach, however, the notification will not always be an appropriate response to a breach. Each incident will be considered on a case-by-case basis to determine whether breach notification is appropriate.

Deciding whether to notify affected individuals

4.56 The key consideration the Institute will adopt is whether notification is necessary to avoid or mitigate serious harm to an affected individual. The Institute may consider the following factors when deciding whether notification is required:

- What is the risk of serious harm to the individual as determined by Step 2?
- What is the ability of the individual to avoid or mitigate possible harm if notified of a breach (in addition to steps taken by the Institute)?
- Even if the individual would not be able to take steps to improve the situation, is the information that has been compromised sensitive, or likely to cause financial damage or humiliation or embarrassment for the individual?

Notification process

4.57 If the Institute determines that notification is appropriate, the Institute will endeavour to notify affected individuals directly - by phone, letter, email or in person. The Institute will generally only adopt indirect notification methods, such as by website information, posted notices, media etc, where direct notification could cause further harm, is cost-prohibitive, or the contact information for affected individuals is not known.

What will be included in the notification?

4.58 If the Institute determines that notification is appropriate, the content of the notification will depend on the particular breach and the notification method. Notification may include the following types of information:

- incident description;
- type(s) of personal information involved;
- the response is taken by the Institute to the breach to control or reduce the harm, and proposed future steps that are planned;

- assistance offered to affected individuals and steps the individual can take to avoid or reduce the risk of harm or to further protect themselves;
- other information sources designed to assist individuals in protecting against identity theft or interferences with privacy; and/or
- contact information for persons that can answer questions, provide further information or address specific privacy concerns.

Who else should be notified?

4.59 If the Institute determines that notification is appropriate, the Institute may also consider that there are third parties who should also be notified about the breach. Such third parties may include:

- Office of the Australian Information Commissioner (OAIC): Where the Institute forms the opinion that an eligible data breach has occurred the Institute is required to notify the OAIC and affected individuals.
- Victorian Information Commissioner (Commissioner): In some circumstances, it may be appropriate to notify the Commissioner. The Institute may consider the following factors when deciding whether to report a breach to the Commissioner:
  - any applicable legislation that may require notification;
  - the type(s) of personal information involved and whether there is a real risk of serious harm arising from the breach, including monetary and non-monetary losses;
  - whether a large number of people were affected by the breach;
  - whether the information was fully recovered without further disclosure;
  - whether the affected individuals have been notified; and/or
  - if there is a reasonable expectation that the Commissioner may receive complaints or inquiries about the breach.
- Police: If theft or other crime is suspected.
- Insurers or others: If required by contractual obligations.
- Professional or other regulatory bodies: If professional or regulatory standards require the Institute to notify such a breach.

Step 4: Prevent Future Breaches

4.60 In addition to the above three steps, the Institute will conduct a post incident evaluation to assess whether any further steps are required to prevent future privacy security breaches, including:

- undertaking a privacy security audit to ensure a similar breach does not occur again;
- making appropriate changes to any relevant protocols or work practices;
- reviewing the Institute policies and procedures relevant to the data breach;
- reviewing and, if necessary, revising staff training practices.

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 endorsed 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 officer of the Institute.

7. ACKNOWLEDGEMENT

This procedure was developed with reference to the following:

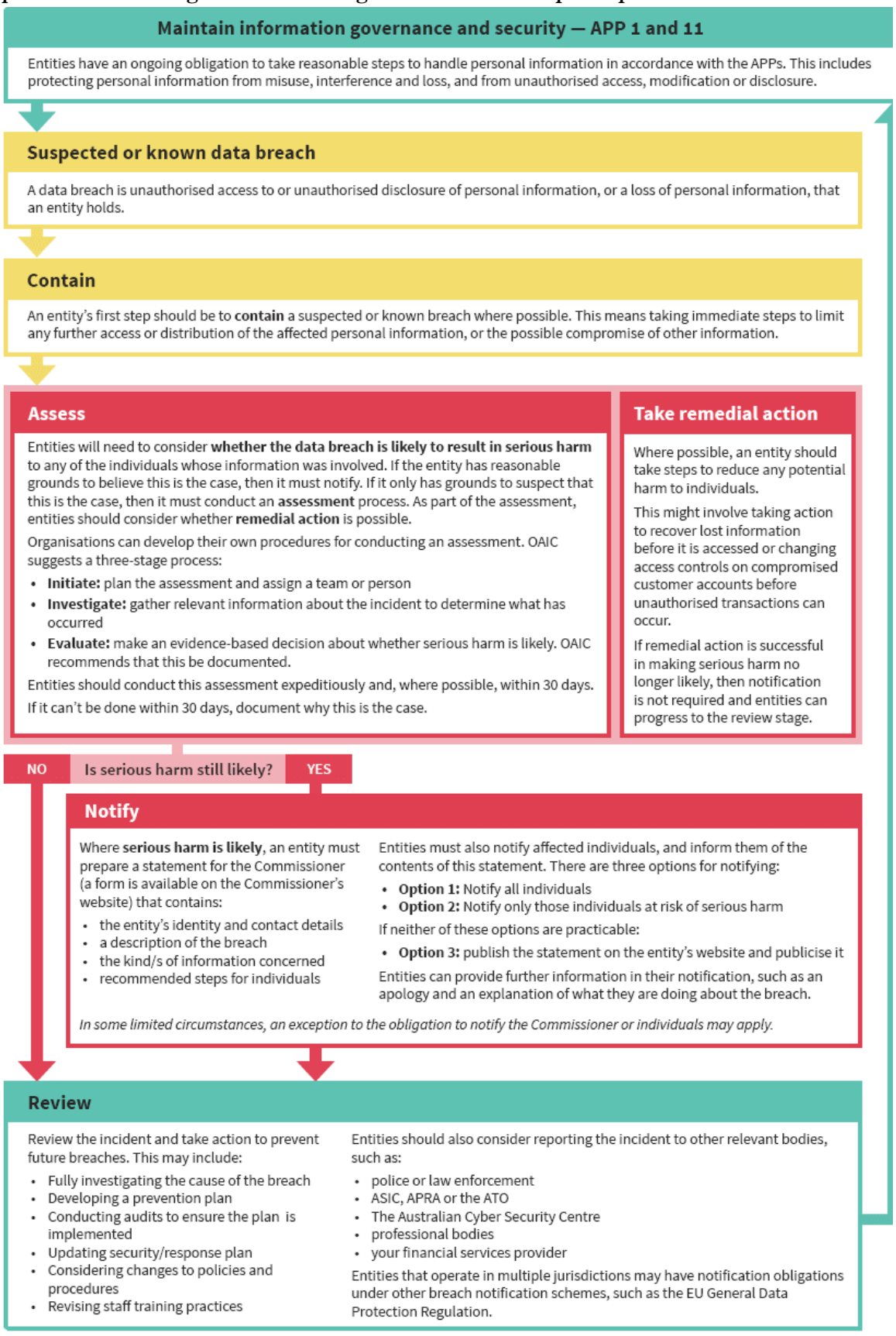
- Office of the Australian Information Commissioner and Privacy Commissioner website resources.
- Deakin University, Privacy Policy, 2022 (https://policy.deakin.edu.au/document/view-current.php?id=139)
- Victoria University, Privacy Policy, 2019 (https://policy.vu.edu.au/document/view.php?id=166)
- University 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
3.0	September 2018	Initial issue	EMT
4.0	August 2023	Internal Review	EMT
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		

Note: EMT = Executive Management team

Appendix 1 OAIC Diagram summarising the data breach response process



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