Information Privacy Procedure

Policy code:	OG1893
Policy owner:	Head of Legal
Approval authority:	Chief Operating Officer
Approval date:	15 November 2023
Next review date:	21 June 2026

Table of Contents

Purpose

This document describes the University's compliances regarding the personal information of University staff, students, prospective students, and other individuals associated with the University (both past and present, including:

- The kinds of personal information that the University collects and holds;
- How the University collects and holds information;
- The purposes for which the University collects, holds, uses and discloses personal information;
- How an individual may access personal information that is held by the University and seek the correction of that information;
- How an individual may complain about a breach of the Information Privacy Principles, or a registered privacy code (if any) that binds the University, and how the University will deal with such a complaint;
- The likelihood of disclosure of personal information to recipients outside Victoria, and the circumstances in which this will occur.

Scope

This procedure applies to personal and health information collected by the University concerning staff, students and other individuals associated with the University. It does not apply to information about corporations.

This procedure does not apply to personal information that is:

- In a publication that is available to the public;
- Kept in a library, art gallery or museum for reference, study or exhibition purposes;
- A public record under the control of the Keeper of Public Records that is available for public inspection; or
- An archive within the meaning of the Commonwealth *Copyright Act 1968*.

Definitions

Term	Definition
Controlled entity	means a corporation or body, of which the University has control of its financial and operating policies within the meaning of section 50AA of the *Corporations Act 2001* (Cth).
Health information	means: 1. Personal information about: 2. i. The physical, mental or psychological health (at any time) of an individual; or ii. A disability (at any time) of an individual; or iii. An individual's expressed wishes about the future provision of health services to them; or iv. A health service provided, or to be provided, or an individual; or 3. Other personal information collected to provide, or in providing, a health service; or 4. Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances; or 5. Other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or any of their descendants.
Personal information	means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Sensitive information	means personal information about an individual's: 1. Racial or ethnic origin; 2. Political opinions; 3. Membership of a political association; 4. Religious beliefs or affiliations; 5. Philosophical beliefs; 6. Membership of a professional or trade association;

	7. Membership of a trade union; 8. Sexual preferences or practices; or 9. Criminal record; that is also personal information.

Procedure Statement

It is University procedure that:

- The collection and use of personal and health information must relate directly to the legitimate purposes of the University.
- Individuals must be aware of, or informed of, the purposes for which personal and health information is obtained.
- The University will take all reasonable steps to ensure that the personal and health information it receives and holds is up to date. However, it is the responsibility of each student and staff member to ensure that up to date and accurate information is provided to the University.
- The University will take all reasonable measures to store personal and health information securely.
- Individuals are entitled to have access to their own records, unless prevented by law.
- Third party access to personal and health information will only be granted if permitted or required by Australian law, and in accordance with University policies and procedures.
- The University will amend records shown to be incorrect.
- The University will observe and comply with all relevant privacy legislation.

The relevant privacy legislation includes the *Privacy and Data Protection Act 2014* (Vic) and the Health Records Act 2001 (Vic). The University's controlled entities are required to comply with the *Privacy Act 1988 (Cth)*. These laws regulate the handling of personal information, with respect to collection, use and disclosure, storage, accessibility and disposal. The *Privacy and Data Protection Act 2014* sets out 10 information privacy principles (IPPs) and the *Health Records Act 2001* (Vic) sets out 11 Privacy Principles (HPPs). The Privacy Act 1988 (Cth) sets out 13 Australian Privacy Principles. The manner in which the University addresses these principles is set out in this procedure and the Information Privacy Procedure.

The University endeavours to comply with the Information Privacy Principles at all times. However, these principles will not apply to a use or disclosure of personal information that is subject to a public interest determination, an approved information usage arrangement or a current certificate issued by the Commissioner for Privacy and Data Protection within the meaning of the *Privacy and Data Protection Act 2014*.

The *Privacy and Data Protection Act 2014* and *Privacy Act 1988* do not apply to personal information of a person who is deceased. The Health Records Act 2001 continues to apply to health information of a deceased person for 30 years after their death.

Nothing in this procedure applies to a document containing information which would be subject to the provisions of the *Freedom of Information Act 1982* ("FOI Act"). If a person requires access to such a document, the person must make a Freedom of Information request through the University's Legal Office. Staff members may have access to their personnel files on request, without the need for an FOI application.

1. Collection of personal information

The University collects personal information (including sensitive information) about prospective and current students, parents, guardians, care providers, prospective and current staff members, volunteers and contractors. The purposes of collecting this information are to:

- Enable the University to deliver education services; and
- Meet the wider functional needs of the University, including financial management, legal accountability, and national reporting requirements; and
- Meet the requirements of legislation or external government agencies.

The University will only collect personal information using lawful and fair means, and not in an unreasonably intrusive way.

The University will collect health information only if the information is necessary for one or more of its functions or activities and with consent, or pursuant to an exception specified in the *Health Records Act 2001*.

Sensitive information

The University will not collect sensitive information about an individual unless:

- The individual consents to the collection of this information; and
- The collection is reasonably necessary for, or directly related to, any of the purposes outlined above.

Method of collection

The University takes all reasonable steps to ensure that information collected:

- is necessary for the University's purposes; and
- is relevant to the purpose of collection; and
- is collected in a fair way, with consent where reasonably possible and without unreasonable intrusion; and
- is as up to date and complete as reasonably possible.

Where the University collects personal and health information about an individual directly from that individual, it will take reasonable steps to ensure that the individual is aware of:

- the identity of the University and how to contact it; and
- the fact that they are able to gain access to the information; and
- the purposes for which the information is collected ("the primary purposes"); and
- to whom (or the types of individuals or organisations to which) the University usually discloses information of that kind; and
- any law that requires the particular information to be collected; and
- the main consequences (if any) for the individual if all or part of the information is not collected.

The University's preferred source of information is the individual concerned. However, there are other important sources of personal information, which may include the following:

Students

- Schools, Victorian Tertiary Admissions Centre VTAC, its successors and equivalent interstate and overseas bodies; and
- Other tertiary institutions, including private providers and recruitment agencies.

Staff

- Previous employers and referees nominated by prospective and current staff members;
- Academic assessors;
- External and internal medical and rehabilitation providers; and

- Promotion and performance review assessments.

The University will not collect personal information about an individual from any party other than those outlined above, or the individual themselves, unless:

- the individual consents; or
- the University is required or authorised by Australian law, or by a court or tribunal order, to collect the information from someone other than the individual; or
- it is unreasonable or impractical to obtain the individual's consent.

Subject to the exceptions specified in section 11 of the *Surveillance Devices Act 1999* (Vic), it is unlawful to knowingly communicate or publish a record or report of a private conversation or private activity that has been made as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device.

Notification

The University will take all reasonable steps to ensure an individual is aware that personal information has been collected about them, and the circumstances of collection if:

- the information has been collected from a person or entity other than the individual; and
- the individual could not reasonably be expected to know that the information has been collected about them.

This notification will include:

- the reason for collection;
- the purpose of collection;
- the consequences for the individual if the information is not collected;
- the bodies and organisations (if any) to which the information may be disclosed; and
- information on how to access this procedure.

2. Use and disclosure of personal information

The University will not without the prior consent of an individual use or disclose personal or health information about that individual for a purpose ("the secondary purpose") other than the primary purpose of collection except in any of the following situations:

1. The individual has consented to the use or disclosure of the information; or
2. The individual would reasonably expect the University to use or disclose the information for the secondary purpose and the secondary purpose is:
    a. if the information is sensitive information – directly related to the primary purpose; or
    b. if the information is not sensitive information – related to the primary purpose; or
3. The use or disclosure of the information is required or authorised by or under an Australian law or a court/ tribunal order; or
4. For personal information, if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual; and
    a. it is impracticable for the University to seek the individual's consent before the use or disclosure; and
    b. in the case of disclosure – the University reasonably believes that the recipient will not disclose the information; or
5. For health information, if the use or disclosure is necessary for research, or the compilation or analysis, in the public interest as contained in the Statutory Guidelines on Research 2002 under the *Health Records Act 2001* (Vic); or

6. The University reasonably believes that the use or disclosure is necessary to lessen or prevent either:
   a. a serious and imminent threat to an individual's life, health, safety or welfare; or
   b. a serious threat to public health, public safety or public welfare; or
7. The University has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
8. The University reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

In ordinary circumstances, any disclosure under scenarios 3, 4, 5, 6, 7 & 8 should only be made by the Vice Chancellor or the University's Privacy Officer.

In some circumstances, the University may use personal information obtained from an individual for purposes other than the original purpose for which it was collected ("a secondary purpose"). Where this occurs, the secondary purpose should be related to the University's activities and functions. The individual may request that their personal information is not used for a specific secondary purpose, and where such a request is made, reasonable steps will be taken to ensure that the information is not used for the secondary purpose.

In addition, the University may release students' personal information in the following instances:

- factual data (name, address, etc.) to the University studentassociation and student bodies to enable them to manage their membership;
- academic progress information to another tertiary institution or related body as required in the course of a student's transfer to a new institution;
- personal and enrolment information, including academic results, of students undertaking cross-institutional study to the relevant institution as required to confirm the student's enrolment or qualification;
- personal information to relevant organisations engaged by the University to provide debt recovery services;
- personal and enrolment information, including academic results, of students undertaking apprenticeship training to their employer;

Direct Marketing

The term "direct marketing "includes direct marketing communications with one or more individuals and it also applies to communications directed to improving the University's marketing practices. The University may de-identify an individual's personal information and use the de-identified personal information for direct marketing purposes, for example to our marketing service providers and partners.

The University will not use or disclose personal information about an individual for the purposes of direct marketing, unless:

- the University collected the information from the individual; and
- the individual would reasonably expect the University to use or disclose the information for that purpose.

Individuals may request the University not to send them direct marketing communications by contacting the University's Privacy Officer.

Despite the above, the University reserves the right to use or disclose personal information about an individual for the purposes of direct marketing if:

1. the University has collected the information from:
   a. the individual and the individual would not reasonably expect the University to use or disclose the information for that purpose; or

   b. someone other than the individual; and
2. either:
   a. the individual has consented to the use or disclosure of the information for that purpose; or
   b. it is impractical to obtain that consent; and
3. the University has advised the individual that they can request not to receive direct marketing communications by contacting the University's Privacy Officer; and
4. in each direct marketing communication with the individual, the University has provided a prominent statement advising that the individual may make such a request; or otherwise drawn the individual's attention to this right, and the University has not received such a request from the individual.

The University will not use sensitive information for the purpose of direct marketing without the individual's consent.

3. Quality of personal information

The University will take reasonable steps to make sure that the personal and health information it collects, uses or discloses is accurate, complete and up to date. If the University is to ensure quality and accuracy of personal information, this places an obligation upon the individual to provide relevant and accurate information to the University.

Unsolicited personal information

If the University receives personal information about an individual that it did not solicit, the University will determine within 15 working days whether the University could have collected the information under the Information Privacy Principle 3, as contained in the Victorian *Privacy and Data Protection Act 2014*.

The University reserves the right to use or disclose the unsolicited information for the purposes of making this determination.

If the University determines that it could not have collected the information under the Victorian *Privacy and Data Protection Act 2014*, the University will destroy or de-identify the information as soon as practicable, provided it is lawful and reasonable to do so.

4. Security of personal information

The University will take all reasonable steps to ensure that the personal and health information it holds is protected from misuse, loss, or unauthorised access, modification or disclosure.

The University will also take all reasonable steps to destroy or permanently de-identify personal and health information if it is no longer needed for any purpose. Under the *Public Records Act 1973* (Vic) the University is required to keep full and accurate records and implement a record disposal program. Destruction of personal and health information will be carried out according to the University's disposal schedules.

Storage of Information

An individual's personal information will primarily be stored in the University's ICT systems. Some information may be retained in hard copy.

The security of personal information is governed by the Information Security Policy. All staff are required to familiarise themselves and comply with the requirements of this procedure. In some circumstances, personal information obtained by the University may be stored in cloud storage, which may involve some storage of

information in offshore servers. The University will not knowingly transmit personal information to a location that does not provide privacy protections substantially similar to those in Victoria.

In circumstances where information is transmitted to an offshore partner provider or agent, the partner provider or agent will be subject to binding contractual obligations to ensure compliance with the University's policies and procedures relating to privacy and information security.

All information relating to administrative and academic matters should be stored securely.

Privacy or Data Breach

In the event of a suspected privacy or data breach involving personal information (whether accidental or otherwise), a staff member must as matter of urgency, actively and quickly communicate with the Privacy Officer.

A staff member involved in the identification of a privacy or data breach must keep written records of the events as they happen.

Rectification steps should not be taken without first consulting with Privacy Officer. The Manager, IT Security & Risk, should also be notified for security related issues. Any remedial actions involving information technology must be approved by the Director ITS prior to implementation.

The Privacy Officer will take steps to manage the breach following the University's privacy breach quick reference guide.

Further to the processes detailed in the guide, the Privacy Officer is responsible for managing the breach response process including:

- receiving all notifications of privacy or data breaches;
- commencing investigations into the breach;
- engaging appropriate stakeholders to assist with investigation and remediation of the breach;
- reporting to the Office of the Victorian Information Commissioner (as required) or other relevant regulators;
- notifying affected individuals (as required) including notification of the right to complain to Office of the Victorian Information Commission at www.ovic.vic.gov.au; and
- conducting reviews to understand how and why the breach occurred and to enhance controls to prevent recurrence.

5. Openness

The University will make this Privacy Policy and related documents available on its website.

On request by a person to the Privacy Officer, the University will take reasonable steps to let the person know, generally, what sort of personal and health information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. Access to and correction of personal information

Access

If the University holds personal or health information about an individual, it will provide the individual with access to the information on request by the individual, except to the extent that:

1. The University reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
2. Giving access would have an unreasonable impact on the privacy of other individuals; or
3. The request for access is frivolous or vexatious; or
4. The information relates to existing or anticipated legal proceedings between the University and individual, and would not be accessible by the process of discovery in those proceedings; or
5. Giving access would reveal the intentions of the University in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
6. Giving access would be unlawful; or
7. Denying access is required or authorised by or under an Australian law or a court/tribunal order; or
8. Both of the following apply:
    a. The University has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the University's functions or activities has been, is being or may be engaged in; and
    b. Giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
9. Giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
10. Giving access would reveal evaluative information generated within the University in connection with a commercially sensitive decision-making process.

The University will respond to a request for access to personal information within a reasonable period, and give access to the information in the manner requested by the individual, if the University considers that it is reasonable and practicable to do so. If the University has refused access, it will provide reasons for the refusal.

If the University refuses to give access to the personal information, or access in the manner requested by the individual, the University will take all reasonable steps in the circumstances to give access in a way that meets the needs of the individual and the University. This may be through the use of a mutually agreed intermediary.

Access charges

The University reserves the right to charge an individual for access to personal information. Details of relevant fees will be provided to the individual on receipt of a request for access, but no charges will apply to the actual making of the request.

The University may refuse to provide access until the fee is paid.

Correction

If the University holds personal information about an individual and either:

- the University is satisfied that, considering the purposes for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
- the individual requests the University to correct the information;

The University will take such steps (if any) as reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading, within a reasonable time frame.

If changes have been made to information that has previously been disclosed to a third party, and the individual requests that the third party be notified of the correction, the University will take all reasonable steps to give that notification, unless it is impracticable or unlawful to do so.

Refusal to correct personal information

If the University determines that it will not alter the personal information as requested by the individual, it will provide written notice of this decision, including the reasons for a refusal and the mechanisms available to complain about the refusal.

Request to associate a statement

If the University refuses to correct personal information as requested by the individual, the individual may request that the University associates a statement with the information to the effect that the information may be inaccurate, out of date, incomplete, irrelevant or misleading. The University will take all reasonable steps to ensure that this statement is apparent to users of the information.

Costs

The University will not charge an individual for making a request for correction of personal information, for correction of the personal information, or for associating a statement with the personal information.

7. Unique identifiers

The University will not assign unique identifiers to individuals except for a Staff Number to identify a staff member and a Student Number to identify a student. Staff Numbers and Student Numbers are necessary for the University to carry out its function efficiently.

The University will not adopt a unique identifier of an individual that has been assigned by another organisation. However, the University may collect and store unique identifiers used by other organisations. These may be included in reports to relevant Commonwealth and Victorian departments and agencies.

The University will not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

8. Anonymity and pseudonymity

An individual may, in some circumstances, be able to request and receive information from the University anonymously, or using a pseudonym. This may be done by making a request to the University's Legal Office.

Anonymity and pseudonymity will not be available if:

- the University is required or authorised by Australian law, or by a court or tribunal order, to deal with individuals who have identified themselves; or
- it is impractical for the University to deal with individuals who have not identified themselves or who have used a pseudonym.

9. Transborder data flow

The University will only transfer personal or health information about an individual to someone (other than the University or the individual) who is outside Victoria if:

- the University reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles or the Health Privacy Principles set out in this Procedure; or

- the individual consents to the transfer; or
- the transfer is necessary for the performance of a contract between the individual and the University, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- the transfer is necessary for the performance of a contract in the interest of the individual between the University and a third party; or
- all of the following apply:
  - the transfer is for the benefit of the individual;
  - it is impracticable to obtain the consent of the individual to that transfer;
  - if it were practicable to obtain that consent, the individual would be likely to give it; or
  - the University has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles or Health Privacy Principles set out in this Procedure.

10. Sensitive information

The University will not collect sensitive information about an individual unless:

- the individual has consented; or
- the collection is required under law; or
- the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

Despite the above, the University may collect sensitive information about an individual if the collection:

- is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
- is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
- there is no reasonably practicable alternative to collecting the information for that purpose; and
- it is impractical for the University to seek the individual's consent to the collection.

The personal information of persons under the age of 18 should not be collected without the permission of a parent or guardian. The University takes its obligations for protection of persons under the age of 18 seriously, and extra care should be taken during the collection, use, disclosure and disposal of their personal information.

Legislative Context

- *Freedom of Information Act 1982* (Cth)
- *Health Records Act 2001* (Vic)
- *Privacy Act 1988* (Cth)
- *Privacy and Data Protection Act 2014* (Vic)
- *Privacy Regulations 2013* (Cth)
- *Public Records Act 1973* (Vic)
- *Surveillance Devices Act 1999* (Vic)

Associated documents

- Corporate Governance Policy

- Operations Governance Policy
- Records Management Procedure
- Information Technology Services Operations Manual- Use of Computing and Communication Facilities and, Information Security
- Information Technology Services Operations Manual- Master Data Management, Data Classification and Usage, and Data Storage

Responsibilities

The Chief Operating Officer will be responsible for control and maintenance of the Information Privacy Procedure.

The University shall appoint a Privacy Officer who will be responsible for the administration of this Procedure. Specifically, the Privacy Officer will:

- keep records which are required to be kept under this Procedure;
- investigate complaints concerning a breach of the Information Privacy Principles and Health Privacy Principles;
- receiving notifications of a suspected privacy or data breach;
- managing the privacy breach response process in accordance with the University's crisis management framework;
- conduct an ongoing review of the University's practices and procedures to ensure that they comply with this Procedure, current legislation and best practice; and
- inform and assist staff with respect to privacy issues.