Information Privacy Procedure

Policy Code: IM1893

Table of Contents

Responsibility

Definitions

Term	Definition
Business day	means Monday through to Friday but excluding days which are designated as University holidays.
Health information	means: a. Personal information about: 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 him or her; or iv. A health service provided, or to be provided, or an individual; or b. Other personal information collected to provide, or in providing, a health service; or c. Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or Other personal information that is genetic information about an individual in a form which is or could predictive of the health (at any time) of the individual or any of his or her descendants.

Term	Definition
Identification information	Biographic and demographic personal information about an individual that is collected for the purposes of reporting and provision of educational services, including but not limited to: a. Name; b. date of birth; c. citizenship; d. languages; e. ethnicity; f. family background; and g. educational background.
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 or an opinion about an individual's: a. Racial or ethnic origin; b. Political opinions; c. Membership of a political association; d. Religious beliefs or affiliations; e. Philosophical beliefs; f. Membership of a professional or trade association; g. Membership of a trade union; h. Sexual preferences or practices; or i. Criminal record; that is also personal information.

What information can be collected?

The University may collect a variety of information about an individual in order to provide services related to University activities. This information may include, but is not limited to:

- 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;
- Information or an opinion about:
  - The physical, mental or psychological health (at any time) of an individual; or
  - A disability (at any time) of an individual; or
  - An individual's expressed wishes about the future provision of health services to him or her; or
  - A health service provided, or to be provided, to an individual.
- Other personal information collected to provide, or in providing, a health service; or
- Other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- Other personal information that is genetic information about an individual in a form which is or could predictive of the health (at any time) of the individual or any of his or her descendants;

- Identification information;
- Basic information about financial or credit status (eg starting dates) and infringements;
- Information about payments and payment plans;
- Information about academic credit and previous results; and
- Various publicly available information like bankruptcy and credit-related court judgements.

It is important to note that the University will not seek or store any of the above information unnecessarily.

Method of collection

The University will, if possible, collect personal information directly from the individual. In some circumstances, personal information will be collected from outside bodies. If these circumstances arise, the University will take all reasonable steps to obtain the consent of the individual for this collection. Information may be obtained through a variety of methods, including (but not limited to) the completion of online forms, paper-based forms, and verbally.

The University seeks to ensure the security of the campus and members of the University community through the appropriate application of closed circuit television (CCTV) surveillance systems.

The primary security use of CCTV is to discourage and/or detect unlawful behaviour in and around university property thereby enhancing the safety and security of all people and property. Other applications and benefits of CCTV include traffic management and assisting some access control environments. However, the use of CCTV may result in the recording of personal information about an individual. All footage containing personal information will be treated in accordance with the University's Information Privacy Policy and Procedure, including restricting access.

The University will take all reasonable steps to ensure the accuracy and currency of the personal information it holds.

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 policy. 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.

Access to information

Personal information will not be made accessible to University staff unnecessarily.

An individual may wish to review the personal information held by the University about them. Requests to access information should be directed to the University's Privacy Officer at privacyofficer@federation.edu.au.

The University will respond to requests for access to information as soon as reasonably practicable. Access will be provided within 30 days of the receipt of a request and sufficient identification of the applicant, unless unusual circumstances arise. If access cannot be provided within 30 days, the University will notify the applicant of the reason for the delay as soon as reasonably practicable, and seek consent for an extension of time.

Correction of information

You have the right to request the correction of any of your personal information held by the University. Requests to correct information should be directed to the University's Privacy Officer at privacyofficer@federation.edu.au.

The University will respond to requests for correction of information as soon as reasonably practicable. Corrections will be made within 30 days of the receipt of a request and sufficient identification of the applicant, unless unusual circumstances arise. If correction cannot be completed within 30 days, the University will notify the applicant of the reason for the delay as soon as reasonably practicable, and seek consent for an extension of time.

If the University cannot correct personal information, the applicant will be notified in writing within 5 business days. Applicants may be directed to external bodies that may be able to correct the information as requested.

Disposal of information

You have the right to request the disposal of any of your personal information held by the University. Requests for disposal of information should be directed to the University's Privacy Officer at privacyofficer@federation.edu.au.

However, this does not mean that a request will automatically result in the disposal of your personal information. All disposal of personal information will be made in accordance with the University's Records Management Policy and Procedure, this procedure, and the University's obligations under privacy and public records legislation.

Personal information of minors

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.

Complaints

Complaints relating to privacy or personal information are governed by the University's Student Complaints Policy and Procedure and Staff Grievance Policy and Procedure or should be directed to the University's Privacy Officer on 5327 9021 or privacyofficer@federation.edu.au. If you feel your privacy has been breached, you can contact the Student Advisory Service, or the University's Privacy Officer for a discussion.

In the event that a complaint relating to privacy or personal information cannot be resolved under the University's Staff Grievance Policy and Procedure, the complaint may be referred to the Commissioner for Privacy and Data Protection.

Reporting

All staff dealing with personal information are required to accurately document:

- the nature of any personal information disclosed;

- the date of the disclosure;
- the person(s) responsible for the disclosure;
- the person(s) who received the disclosure;
- evidence that the disclosure was permitted or that consent was given;
- any relevant written notices or correspondence;
- details of any subsequent action taken; and
- any other relevant information.

Documentation should be retained for 5 years.

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.

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

- Information Security Policy
- Information Privacy Procedure
- Records Management Policy and Procedure
- Use of Computing and Communications Facilities Policy