Swinburne University of Technology - Privacy Procedures

PART 1 – OVERVIEW

1. Purpose

The purpose of these Procedures is to provide additional guidance for staff, information for students and the general public, on the University's privacy practices and its management of Personal and Health Information.

In particular, the Procedures address the following areas:

- the type of Personal and Health Information the University holds;
- how the University collects and holds Personal and Health Information;
- the purposes for which the University collects, holds, uses and discloses Personal and Health Information;
- how an individual may access Personal or Health Information held by the University and seek the correction of such information;
- how an individual may complain about a breach of the Australian Privacy Principles and how the University will deal with such complaints;
- if the University is likely to disclose Personal Information to overseas recipients, the countries those recipients are likely to be located in (if practicable).

2. Scope

These Procedures are applicable to all dealings with Personal and Health Information that occur in Australia. As such, they apply to all Australia campuses of the University and all University staff are required to observe them along with the relevant Australian Privacy Laws.

These Procedures apply to all Personal and Health Information collected by the University, regardless of the source of the collection or the purpose for collection.

These Procedures do not apply to information that is:

- collected or held about corporations;
- publicly available;
- 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 and available for public inspection; or
- an archive within the meaning of the *Copyright Act* 1968 (Cth).

3. University documents

The University's privacy guidelines and procedures are publicly available on the Swinburne website here.

Privacy resources for staff are available here (requires login).

4. Applicable Legislation

The University collects, uses and discloses Personal and Health Information in accordance with the following Commonwealth and Victorian legislation:

- *Privacy and Data Protection Act* 2014 (Vic)

- *Health Records Act* 2001 (Vic)
- *Freedom of Information Act* 1982 (Vic)
- *Public Records Act* 1973 (Vic)
- *Privacy Act* 1988 (Cth)
- *Higher Education Support Act* 2003 (Cth)

These Procedures have regard to and comply with this legislative framework. In particular, the focus is on the following privacy principles:

- the Information Privacy Principles set out in the Privacy and Data Protection Act;
- the Health Privacy Principles set out in the Health Records Act; and
- the Australian Privacy Principles set out in the Commonwealth Privacy Act.

Further information on privacy in Australia can be found by contacting:

- The Office of the Victorian Information Commissioner
- The Office of the Commonwealth Information Commissioner

5. Privacy Officer

The University Privacy Officer supports Swinburne in its compliance with the Privacy Legislation and these Procedures across the University. The Privacy Officer is the first point of contact for staff, students and the public who have questions or concerns regarding the University's privacy practices and compliance with legislation.

The University's Privacy Officer is Mr Matthew Smith, contactable via email- infoprivacy@swin.edu.au.

6. Complaints process

Any person who has concerns regarding the University's handling of their Personal or Health Information should contact the University's Privacy Officer. Complaints should be:

- in writing and directed to infoprivacy@swin.edu.au; and
- lodged within 6 months of the complainant first becoming aware of the apparent breach.

The Privacy Officer can assess the complaint and may investigate the complaints lodged in accordance with this section. The scope and method of the investigation may vary depending on the nature of the complaint and the information.

In general, complaints will be reviewed and managed in accordance with the University's Complaints Management Guidelines and the Reviews and Appeals Regulations.

PART 2 – DEFINITIONS

The following key terms are used throughout these Procedures:

Term	Definition
Australian Privacy Principle or APP	Means the Australian Privacy Principles set out in Commonwealth Privacy Act.
Commonwealth Privacy Act	Means the *Privacy Act* 1988 (Cth).
Health Complaints Commissioner Guidelines	Means guidelines issued and approved by the Victorian Health Complaints Commissioner in accordance with section 22 of the Health Records Act.
Health Information	As defined in the Health Records Act 2001 (Vic), means: • 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 – that is also personal information; or • 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 be predictive of the health (at any time) of the individual or of any of his or her descendants – but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act.
Health Privacy Principle or HPP	Means the Health Privacy Principles set out in the Health Records Act.
Health Records Act	Means the *Health Records Act* 2001 (Vic).
Information Privacy Principle or IPP	Means the Information Privacy Principles set out in the Privacy and Data Protection Act.
Law	Means any Australian statutory law or Australian court or tribunal order (if applicable).
Personal Information	As defined in the *Privacy and Data Protection Act* 2014 (Vic), 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, but does not include information of a kind to which the *Health Records Act* applies.

Term	Definition
Privacy and Data Protection Act	Means the *Privacy and Data Protection Act* 2014 (Vic).
Privacy Legislation	Means the various pieces of privacy related legislation which the University follows. See paragraph 4 above, for the full list.
Project	Means a project, system or process implemented by Swinburne that involves Personal, Health or Sensitive Information.
Sensitive Information	As defined in the *Privacy and Data Protection Act* 2014 (Vic), means information or an opinion about an individual's – • racial or ethnic origin; or • political opinions; or • membership of a political association; or • religious beliefs or affiliations; or • philosophical beliefs; or • membership of a professional or trade association; or • membership of a trade union; or • sexual preferences or practices; or • criminal record – that is also Personal Information.

PART 3 – HANDLING OF PERSONAL AND HEALTH INFORMATION

7. Overview

7.1 Scope of this Part

Part 3 of these Procedures sets out the core practices of the University in relation to each privacy principle, as set out in the Privacy Legislation, these are:

- Collection;
- Use and disclosure;
- Anonymity and use of pseudonyms;
- Use of identifiers;
- Security;
- Quality of Information;
- Openness;
- Access;
- Correction; and
- Transborder data flow.

7.2 Personal and Health Information

These Procedures apply only to the collection, use and disclosure of Personal and Health Information as defined in the Privacy Legislation. Generally, these terms are understood as follows:

- **Personal Information** is 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. Personal Information does not include Health Information.
- **Health Information** is information or an opinion (which is also Personal Information) about -
  - the physical, mental or psychological health (at any time) of an individual;
  - a disability (at any time) of an individual;
  - 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.

7.3 Solicited and Unsolicited Information

Information held by the University may be either solicited or unsolicited.

- **Solicited Information** is information that is expressly sought by the University, either from the specific individual or a third party. For example, Personal Information collected on student enrolment forms is solicited information.
- **Unsolicited Information** is information that it provided to the University of a person's own choosing and without a request from the University.

Most of the information held by the University is solicited and the principles around collection set out in section 8 of these Procedures apply. The manner by which the University handles unsolicited information is described in section 8.4.

7.4 Primary and Secondary Purposes

Personal Information is collected, used and disclosed in accordance with a purpose. The Privacy Legislation deals with two categories of purpose:

- **Primary Purpose** is the purpose for which the information is collected, as disclosed to the person whose information it is. This is generally a specific singular purpose.
- **Secondary Purpose** is a subsequent purpose, other than the primary purpose, which may or may not have been disclosed. An organisation may have multiple secondary purposes when collecting information.

For example, a restaurant may collect your name, phone number and email address for the purpose of reserving a table. This is the primary purpose for the collection. Consequently, you may receive emails of specials and events. This is a secondary purpose and may or may not have been disclosed when you provided your information to make the booking.

7.5 Health Service Provider

When handling Health Information, the University seeks to comply with principles set out in the Health Records Act. Under that Act, the principles and requirements that an organisation must adhere to are dependent upon whether or not the organisation is a Health Service Provider.

A **Health Service Provider** is an organisation that provides a health service in Victoria, to the extent that it provides such a service.

This means that the University is considered a Health Service Provider in *some* circumstances. For example, the Medical Service and Counselling Service are Health Service Providers. These areas of the University follow the provisions of the Health Records Act applicable to Health Service Providers. If you are a staff member in these areas, or a person seeking information held by one of these areas, further information may be sought from the Privacy Officer.

In all other circumstances, the University seeks to follow the provisions of the Act applicable to it as an organisation.

8. Collection[1]

8.1 Collection of Personal Information

What information does the University collect?

The University collects both Personal Information and Health Information about those it engages with. This includes, for example; prospective and current students, parents and guardians, alumni, prospective and current staff members, volunteers, benefactors, research participants and external contractors.

The University may collect Information from the individual concerned or a third party.

Whilst the University collects a broad spectrum of information depending on the relevant purpose, generally the kind of information collected includes:

- names;

- student identification numbers;
- addresses;
- emergency contacts;
- photographic identification; and
- other related personal information required for the effective management of the University.

Why does the University collect information?

The University collects:

- **Personal Information** where the information is necessary for (or directly related to) one or more of the University's functions or activities.
- **Health Information** when necessary for one or more of its functions or activities. Health Information is collected with consent or under a valid exception (see section 8.3).

In all circumstances the University collects Personal and Health information by legal and fair means and is not unreasonably intrusive.

Who does the University collect information from?

Generally, the University will collect information from the individual concerned. However, in some cases it is unreasonable or impractical to do so. In such cases, information may be collected from a third party.

For example, the University collects Personal Information from important authoritative sources, such as:

- schools;
- the Victorian Tertiary Admissions Centre (VTAC) and equivalent interstate and overseas bodies;
- other tertiary institutions, including private providers and recruitment agencies;
- previous employers and referees nominated by prospective and current staff members;
- academic assessors; and
- external and internal medical and rehabilitation providers.

When does the University inform a person that their information is being collected?

Unless an exception applies, the University will notify the individual concerned of the collection of his or her Personal or Health Information, in writing. Where possible, the notification will be given at or before the time of collection. In all other cases, it will be given as soon as practicable thereafter.

The University will not provide such a notification, if it believes:

- making the individual aware of the collection would pose a serious threat to the life or health of any individual; or
- in the case of Health Information – the notification would involve disclosure of information given in confidence (see section 8.3).

The notification may include the following information:

- the identity of the University and how to contact it;
- how the individual may access the information collected and seek to correct it;
- the purposes for which the information is being collected (primary purpose);

- the persons to whom the University usually discloses information of the kind being collected;
- any law that requires the particular information to be collected;
- the main consequences (if any) for the individual if all or part of the information is not collected;
- where the individual can find information on how to make a complaint about a breach of privacy laws and how the complaint will be dealt with;
- whether the information is likely to be disclosed to overseas recipients and if so, the countries in which those recipients are likely to be located (if practicable); and
- information on how to access the University's privacy guidelines.

8.2 Collection of Sensitive Information

What is sensitive information?

Some of the information the University collects is Sensitive Information.

Sensitive Information is Personal Information or an opinion about an individual's:

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

When will the University collect Sensitive Information?

The University may collect Sensitive Information about an individual where:

- the individual has consented;
- the collection is required by Law;
- 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 is physically or legally incapable of giving consent to the collection or physically unable to communicate consent to the collection;
- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;
- 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.

8.3 Collection of Health Information

When does the University collect Health Information?

The University may collect Heath Information about an individual where it is necessary for its functions or activities and at least one of the following circumstances applies:

- the individual has consented;
- the collection is permitted by law;
- the information is necessary to provide a health service to an individual who is incapable of giving consent,[2] and it is not reasonably practicable to obtain the consent of an authorised representative of the individual[3];
- the information is disclosed to the University in accordance with specific Health Principles;
- the collection is –
  - necessary for research, or the compilation or analysis of statistics, in the public interest; and
  - that purpose cannot be achieved by the collection of de-identified information; and
  - it is impracticable for the University to seek the individual's consent to the collection;
- the information is collected in accordance with the Health Complaints Commissioner Guidelines;
- the collection is necessary to prevent or lessen –
  - a serious and imminent threat to the life, health, safety or welfare of any individual; or
  - a serious threat to public health, safety or welfare; and
  - the information is collected in accordance with the Health Complaints Commissioner Guidelines;
- the collection is by a law enforcement agency and necessary for a law enforcement function; or
- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

How does the University deal with Health Information Collected in Confidence?

When the University is acting in its capacity as a Health Service Provider, it may collect Health Information which is necessary to provide a health service to an individual. In some cases, the individual may be incapable of giving consent[4] and it is not reasonably practicable to obtain the consent of an authorised representative.

In such circumstances (and others), Personal Information may be given in confidence to the University by another person. The provision of information may come with a request that the information not be communicated to the individual to whom it relates. In such cases, the University will:

- confirm with the person providing the information that it is to remain confidential;
- record the information only if it is relevant to the provision of health services to, or the care of, the individual;
- take reasonable steps to ensure that the information is accurate and not misleading; and
- take reasonable steps to record that the information is given in confidence and is to remain confidential.

8.4 Unsolicited information

In most cases, information held by the University is solicited. That is, it is expressly sought by the University, either from the specific individual or a third party.

At times however, the University is provided with unsolicited information. This occurs when a person provides information to the University at their own accord and without a request from the University.

When the University receives unsolicited Personal Information, it will follow the process set out below.

- The University will access the information to determine whether or not it could have collected the information if it had requested it, in accordance with these Procedures.
- In doing so, the University may use or disclose the unsolicited information.
- Where the University determines that –
  - it **could not** have collected the Personal Information - the University will, as soon as practicable, destroy the information or ensure that the information is de-identified (provided it is lawful and reasonable to do so); or
  - it **could** have collected the personal information - the University will treat the information as if it were solicited information and as such these Procedures will apply.

9. Use and disclosure

9.1 Use and disclosure of Personal Information

When collecting Personal Information, the University will disclose to the individual the primary purpose for the collection. This is the main purpose for which the information is collected. Subsequently, the University will also use and disclose Personal Information, in accordance with this primary purpose.

In some cases, the University may seek to use or disclose the information for another purpose (that is, a secondary purpose). The University will only do this where one of the following circumstances applies:

- the individual has consented to the use or disclosure of the information for the secondary purpose;
- the individual would reasonably expect the University to use or disclose the information for the secondary purpose and the secondary purpose is:
  - directly related to the primary purpose (in the case of sensitive information); or
  - related to the primary purpose (in all other cases);
- 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
  - it is impracticable for the University to seek the individual's consent before the use or disclosure; and
  - in the case of disclosure, the University reasonably believes the recipient of the information will not disclose it;
- the University reasonably believes that the use or disclosure is necessary to lessen or prevent a –
  - serious and imminent threat an individual's life, health, safety or welfare; or

  - serious threat to public health, safety or welfare;
- the University has reason to suspect unlawful activity may be occurring, and it uses or discloses the information as a necessary part of its investigation or to report its concerns to relevant persons or authorities;
- the use or disclosure is required or authorised by Law; or
- the University reasonably believes that the use or disclosure is necessary for a law enforcement agency to perform a law enforcement function or activity.[5]

9.2 Direct marketing

What is direct marketing?

Direct marketing involves the use and/or the disclosure of Personal Information to communicate directly with an individual to promote goods and services.

When will the University use Personal Information for direct marketing?

The University may seek to use or disclose Personal Information for the purpose of direct marketing, if one of the below situations applies:

- The University has collected Personal Information from an individual who would reasonably expect the University to use or disclose the information for direct marketing purposes.
- The University has collected the Personal Information –
  - from an individual who would not reasonably expect the University to use or disclose the information for direct marketing purposes or from someone other than the individual ; and
  - the individual has consented to the use or disclosure for direct marketing purposes or it is impracticable to obtain that consent.
- The University has collected Sensitive Information for direct marketing purposes and obtained consent to the use or disclosure for information for that purpose.
- The University is a contracted service provider for a government contract and the collection, use and disclosure of Personal Information for direct marketing purposes is required to meet the obligations of the contract.

Individual may request not to receive direct marketing communications

Where the University uses or discloses Personal Information for direct marketing purposes, it will provide a simple means for the individual concerned to request that they no longer receive such communications.

Where such a request is made, the University will cease all direct marketing communications (and ensure third parties do likewise), within a reasonable period after the request is made.

9.3 Use and disclosure of Health Information

Use and disclosure of Health Information

The University seeks to use and disclose Health Information, in accordance with the primary purpose for which it was collected. However, in some cases, the University may seek to use or disclose the information for another purpose (that is, a secondary purpose).

In all circumstances, the University will seek to comply with any applicable Health Complaints Commissioner Guidelines.

The University may use Health Information for a secondary purpose where one of the following situations applies:

- the individual has consented to the use or disclosure of the information for the secondary purpose;
- the individual would reasonably expect the University to use or disclose the information for the secondary purpose, which is directly related to the primary purpose;
- the use or disclosure is required or authorised by Law;
- the use or disclosure is for the purpose of funding, management, planning, monitoring, improvement or evaluation of health services or training provided by a health service provider to employees, and –
  - the purpose cannot be achieved by the use or disclosure of de-identified information and it is impracticable to seek the individual's consent to the use or disclosure; or
  - reasonable steps are taken to de-identify the information.
- the use or disclosure is –
  - necessary for research, or the compilation or analysis of statistics, in the public interest;
  - it is impracticable for the University to seek the individual's consent before the use or disclosure;
  - the purpose cannot be achieved by the use or disclosure of de-identified information; and
  - in the case of disclosure, the University reasonably believes that the recipient of the information will not disclose it and any publication will be in a form that de-identifies particular individuals.;
- the University reasonably believes that the use or disclosure is necessary to lessen or prevent a –
  - serious and imminent threat an individual's life, health, safety or welfare; or
  - serious threat to public health, safety or welfare;
- the University has reason to suspect unlawful activity may be occurring, and it uses or discloses the information as a necessary part of its investigation or to report its concerns to relevant persons or authorities;
- the University reasonably believes that the use or disclosure is necessary for a law enforcement agency to perform a law enforcement function or activity; or
- the use or disclosure is necessary for the establishment, exercise or defence of a legal or equitable claim.

Use and disclosure in serious circumstances

In circumstances where an individual is dead, missing or been involved in an accident and is incapable of consenting to the use or disclosure, the University may use or disclose Health Information it holds. The University will do so for the purpose of assisting to identify the individual and/or family members, so that they may be contacted by the authorities.

Where an individual is missing or has been involved in an accident, the University will not use or disclose Health Information as described above, if it is contrary to any wish expressed by the individual.

Acting as a Health Service Provider

When acting in its capacity as a Health Service Provider, the University may use or disclose Health Information for a secondary purpose, where one of the following applies:

- The University is providing a health service to an individual and the use or disclosure is necessary for the provision of that health service, however the individual is incapable of giving consent and it is not reasonably practicable to obtain the consent of an authorised representative.
- The University is providing a health service to an individual and the use is for the purpose of providing further health services safely and effectively.

Disclosure to family members

The University may disclose Health Information to an immediate family member of an individual if –

- the disclosure is necessary to provide appropriate health services to or care of the individual or the disclosure is made for compassionate reasons;
- the disclosure is limited to the information that is reasonable and necessary for the above purpose;
- the individual is incapable of giving consent to the disclosure;
- the disclosure is not contrary to any wish expressed by the individual before the individual became incapable of giving consent; and
- in the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, that person has sufficient maturity to receive the information.

No obligation to disclose

Nothing in the Health Privacy Principles requires the University to disclose Health Information about an individual. Notwithstanding these Procedures, the University maintains its right to refuse to disclose Health Information in the absence of a legal obligation to do so.

9.4 De-identification

In the following circumstances, the University will take reasonable steps to ensure the Health Information it holds is de-identified, before it is disclosed.

- The collection is necessary for any of the following purposes:
  - research relevant to public health or safety;
  - the compilation or analysis of statistics relevant to public health or safety;
  - the management, funding or monitoring of a health service; and
- the purpose cannot be achieved by the collection of information about the individual that is de-identified; and
- it is impracticable for the University to obtain the individual's consent to the collection; and
- the collection is required under Australian law (other than the Privacy Act) or other rules or guidelines which bind the University.

9.5 Providing information to other Health Service Providers

Where the University holds Health Information in its capacity as a Health Service Provider, an individual may request that the University disclose that information to another health service provider. Such a request may be made by the second health service provider on the individual's behalf. In such cases, the University will disclose the information as soon as practicable.

The University may charge a fee for the disclosure of such information.

10. Anonymity and use of pseudonyms

In some interactions with the University, an individual may wish to remain anonymous or use a pseudonym. Where possible, the University may seek to accommodate this. However, the University will not agree to anonymity or the use of pseudonyms where –

- the University is required or authorised by Law to deal with an individual who has identified themselves; or
- it is impracticable for the University to deal with an individual without knowing their identity.

For example, prospective students will be required to disclose their identity when seeking to enrol at the University, as will prospective employees when seeking employment.

11. Unique identifiers

11.1 Use of unique identifiers

A **unique identifier** is a reference (usually a number) assigned to a person, to uniquely identify them. A unique identifier is never duplicated and is therefore distinct from a person's name, which may not be unique. Common examples include driver licence numbers, passport numbers and tax file numbers.

The University may assign unique identifiers to individuals where it is necessary to enable the University to carry out any of its functions efficiently. For example, the University assigns staff numbers to staff and student numbers to students.

11.2 Adopting the unique identifiers of other organisations

Unique identifiers are used by many organisations, most notably government entities. The University will rarely adopt and use a unique identifier of another organisation. The exceptions to this, are as follows:

- the University may adopt a unique identifier of another organisation as its own, if:
  - it is necessary to enable the University to carry out any of its functions efficiently;
  - the University has obtained the consent of the individual; or
  - the identifier relates to the performance of a government contract;
- the University may adopt a government related identifier as its own if authorised or required by Law.

11.3 Adopting unique identifiers of other organisations

Where an individual has been assigned a unique identifier by another organisation, the University may use or disclose that unique identifier where:

- the use or disclosure is necessary for the University to fulfil its obligations to the other organisation;
- the use or disclosure is reasonably necessary for the University to verify the identity of the individual;
- the University has obtained the consent of the individual;

- the University reasonably believes that the use or disclosure is necessary to lessen or prevent a –
  - serious and imminent threat to an individual's life, health, safety or welfare; or
  - serious threat to public health, safety, or welfare;
- the University has reason to suspect unlawful activity may be occurring, and it uses or discloses the information as a necessary part of its investigation or to report its concerns to relevant persons or authorities;
- the use or disclosure is required or authorised by Law; or
- the University reasonably believes that the use or disclosure is necessary for a law enforcement agency to perform a law enforcement function or activity.

12. Security of Personal Information

12.1 Protection of information

The University takes reasonable steps to protect Personal and Health Information it holds, from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

12.2 Deletion and de-identification

In some circumstances, the University may take steps to destroy or permanently de-identify Personal or Health Information. In all cases, the University seeks to ensure such measures comply with the terms of the *Public Records Act* (Vic) 1973.

Personal Information

The University will take reasonable steps to destroy or permanently de-identified Personal Information held by it, if all of the following circumstances apply:

- the University no longer needs the information for any purpose for which it may be used or disclosed;
- the information is not contained in a government record; and
- the University is not required by Law to retain the information.

Health Information

The University will take reasonable steps to destroy or permanently de-identified Health Information, if the University no longer needs it for any purpose for which it was collected or any other purpose authorised by Law.

Where the University holds Health Information in its capacity as a Health Service Provider, the University seeks to comply with the Health Records Act regarding when and how information may be deleted or transferred. For further guidance, please contact the Privacy Officer.

13. Quality of information

The University takes reasonable steps to ensure the Personal and Health Information it collects, uses and discloses is:

- accurate, complete and up to date; and

- relevant to its functions and activities.

The *steps* taken by the University may vary depending on the type of type of information, specific circumstances and the purpose for which the relevant information is to be collected, used or disclosed.

To assist the University in retaining accurate records, it requires individuals to provide it with accurate and complete information, and to update that information when changes occur.

14. Openness

The University seeks to ensure it is open and transparent in its dealings with individuals, and its handling of Personal and Health Information. At any time, an individual may make enquiries regarding the Personal or Health Information the University holds. On receiving such a request, the University will take reasonable steps to inform the individual of –

- the nature of the information it holds;
- the purposes for which the information is used; and
- how the University collects, holds, uses and discloses the information.

If the request relates to Health Information, the University will also seek to:

- confirm whether the University holds Health Information relating to the specific individual; and
- advise the steps the individual can take to obtain access to the information, if desired.

15. Access to Personal Information

15.1 Seeking access to Personal Information

When can a person access their information?

At any time, an individual may request access to their Personal or Health Information held by the University, by contacting the Privacy Officer. The University will only provide access to an individual about their own Personal or Health Information and not that of another person.

The University will usually provide an individual with access to their Personal or Health Information, however, such access may be denied if any of the below exemptions apply.

Exemptions

The University may not provide access to Personal or Health Information if:

- providing access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;[6]
- providing access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to legal proceedings between the University and the individual, and the information would not be accessible by the process of discovery or subpoena;
- providing access would reveal the intentions of the University in relation to negotiations with the individual, in such a way as to prejudice those negotiations;
- providing access would be unlawful;
- the University being required to deny access is required by Law;
- providing access may prejudice an investigation of possible unlawful activity, or enforcement related activities conducted by a law enforcement agency;

- the University suspects[7] that unlawful activity or serious misconduct relating to the University's functions or activities is (or has been) engaged in, and giving access may prejudice the taking of appropriate action; or
- providing access would reveal the University's evaluative information regarding commercially sensitive decision-making process.

Specific requirements for Health Information

The University provides access to Health Information in accordance with the Health Records Act and the Health Complaints Commissioner Guidelines. Where a request for access is made, University staff should consult with the Privacy Officer.

Generally, the University will provide a person with access to their own Health Information, unless one of the exemptions applies. In addition, the University may deny access where -

- the Information is subject to confidentiality under the Health Records Act;[8]
- a law enforcement agency performing a security function requests that the University not provide access as it may cause damage to the security of Australia;
- the request is similar to one which has been unsuccessfully on at least one previous occasion, and there is no reasonable ground for making the request again; or
- the individual has been provided with access in accordance with Part 5 of the Health Records Act and is making an unreasonable repeated request for access to the same information in the same way.[9]

15.2 Process for accessing information[10]

How does the University deal with requests for access to information?

Upon receiving a request for access to Personal or Health Information, the University will review the request determine whether it will provide access.

The University will –

- seek to respond to requests for access to Personal Information within 45 days of the request being made;[11]
- provide reasons, if there is any delay in providing access; and
- give access to the information in the manner requested by the individual, if reasonable and practicable to do so. Where access by the requested means is not be possible, the University takes reasonable steps to give access in a way that meets the needs of the University and the individual.

If the University refuses the request for access or provides access in a manner other than that requested by the individual, the University will advise the individual (by written notice) of -

- the reasons for the refusal of access, unless it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal of access.[12]

What is the cost? [13]

The University may set a fee for access to Information. Such a fee will not be excessive and will only apply when access to information is provided. The University will not charge a fee for making a request for access.

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

16. Correction of information[14]

16.1 Correction of Personal Information[15]

When will the University correct Personal Information?

The University seeks to ensure that all Personal Information it holds is accurate, complete, up to date, relevant and not misleading. Where it is identified that this is not the case, the University takes reasonable steps to correct the information.

Generally, corrections will take place where -

- the University is satisfied, having regard to a purpose for which the information is held, that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or
- an individual requests the University to correct the information and the University approves the request.

The University is not bound to correct information upon request and will refuse to do so, if it believes that the information it holds is accurate, complete, up to date, relevant and not misleading.

What is the process for requesting a correction?[16]

At any time, an individual may request that the University correct Personal Information held about that person.

Upon receiving a request for a correction, the University will -

- consider the request to determine whether the information appears inaccurate, out-of-date, incomplete, irrelevant or misleading; and
- seek to respond to the request within 45 days of the request being made.[17]

If the University refuses to correct the Personal Information as requested, the University will advise the individual (by written notice) of -

- the reasons for the refusal, unless it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal.[18]

Where the University corrects Personal Information which it has previously disclosed to a third party, the University will attempt to notify those parties of the correction, unless it is impracticable or unlawful to do so. Such notification will only occur when requested by the individual.[19]

Request to associate a statement[20]

Where the University refuses to correct the Personal Information as requested, the individual may subsequently request that the University associate with the information, a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.

Where such a request is made, the University will take reasonable steps to associate the statement in such a way that will make the statement apparent to users of the information.

What is the cost?

The University will not charge an individual for requesting a correction, for making the correction or for associating the statement with the personal information (as the case may be).

16.2 Correction of Health Information[21]

When will the University correct Health Information?

Where an individual can establish that Health Information held by the University about that individual is inaccurate, out-of-date, incomplete or misleading, the University will take reasonable steps to correct the information.

What is the process for requesting a correction?

At any time, an individual may request that the University correct Health Information held about that person. The individual is required to show that the Health Information is inaccurate, out-of-date, incomplete or misleading.

Upon receiving a request for a correction, the University will -

- consider the request to determine whether the information is inaccurate, out-of-date, incomplete, or misleading;
- seek to respond to the request within 30 days of the request being made; and
- where the request for a correction is refused, provide reasons for the refusal.[22]

Correcting health records[23]

The University recognises the importance of maintaining complete health records and as such, any correction will be made following the Health Records Act principles. For example, in some circumstances, the University will maintain a record of the incorrect information which is not generally accessible.

Where the University corrects the Health Information it will seek to -

- record with the correction, the name of the person who made the correction and the date on which it was made; and
- notify any health service providers to whom the University disclosed the Health Information before its correction, who may reasonably be expected to rely upon the information.

If the University deletes the information it will do so in accordance with the Health Privacy Principles and the Health Records Act. Advice should be sought from the Privacy Officer in these circumstances.

Request to associate a statement[24]

Where the University refuses to correct the Health Information as requested, the individual may give the University a written statement concerning the requested correction. The University will take reasonable steps to associate the statement with the information.

17. Transborder data flow[25]

17.1 Transfer of information outside of Victoria[26]

Personal or Health Information held by the University may be transferred outside of Victoria (either interstate or overseas), where it is necessary for the University to perform its functions or carry out its activities. Such a transfer may be for the benefit of, or at the request of, the relevant individual. For example, a student seeking to study overseas. In such circumstances, the University seeks to comply with Privacy Legislation governing transborder data flow.

The University may transfer Personal or Health Information to someone (other than the University itself or the individual concerned) who is outside Victoria if –

- the University reasonably believes the recipient of the information is bound by privacy principles substantially similar to the IPPs or HPPs (as applicable);
- the individual consents to the transfer;
- the transfer is necessary for the performance of a contract between the individual and the University;
- the transfer is necessary for the performance of a contract for the benefit of the individual, between the University and a third party;
- 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 the transfer; and
  - if it were practicable to obtain that consent, the individual would be likely to give it;
- the University has taken reasonable steps to ensure the information will not be held, used or disclosed by the recipient inconsistently with the HPPs or IPPs; or
- the transfer is authorised or required by Law.

17.2 Application of the Australian Privacy Principles[27]

Before the University discloses Personal Information to a person outside of Australia, the University will take reasonable steps to ensure the recipient does not breach the Australian Privacy Principles.

This requirement will not apply where:

- The University reasonably believes:
  - the recipient of the information is subject to a law that protects the information in a way that is substantially similar (at least) to Australian Privacy Legislation; and
  - there are mechanisms the individual can access to enforce the protection of that law.
- The individual consents to the disclosure of the information after being expressly informed by the University that their consent will mean the above requirement will not apply.
- The disclosure of the information is authorised or required by Law.

18. Procurement, Contracts and Projects

It is the responsibility of the Head of Management Unit to ensure a Project includes safeguard to protect Personal, Health and Sensitive Information relating to individuals.

Before a new Project is commenced, or prior to a Project being changed, staff must consider the Privacy resources available here (login required), this may include completing a Threshold Privacy Assessment and/or Privacy Impact Assessment (Privacy Impact Assessment Procedure under review).

Advice from the Privacy Officer must be sought when a Project involves Personal, Health and Sensitive Information being transferred outside of Australia.

Where a Project involves Records or IT systems, staff should consult that relevant area to seek advice as required.

Endnotes (Notes from the Privacy Officer):

General Comments

Whilst the IPPs, APPs and HPPs are largely consistent in the principles themselves, there is some deviation in the specific language used. The Procedures are written in such a way to ensure compliance with all pieces of legislation, however if an issue were to arise (or a question of a breach), specific reference should be made to the relevant Acts.

REFERENCES

[1] Relevant Principles - IPP 1 and 10, HPP 1 and APP 3-5.

[2] Consent within the meaning of the Health Records Act, section 85(3).

[3] See Health Records Act, section 85, for definition of an authorised representative. This also applies if the individual does not have an authorised representative.

[4] Health Records Act, section 85(3).

[5] Refer to IPP 2.1 for a full list of the law enforcement functions and activities. Also refer to requests by ASIO or ASIS.

[6] If the Information is Health Information - Division 3 of Part 5 includes a procedure to be followed where access is denied on the grounds that it would pose a serious threat to the life or health of the individual (see HPP 6.3).

[7] The University must have "reason" to suspect.

[8] Refer to section 27 of the Act for the full procedure. Note, information will be subject to confidentiality where it is given in confidence to the person who recorded it by a third person, with a request that it not be communicated to the individual.

[9] Access to Health Records must be provided in accordance with Part 5 of the Act and Guidelines issued under section 22 (HPP 6.1).

[10] Refer to IPP 6.3 and APP12.4-12.6.

[11] The APPs state that requests must be responded to within a "reasonable time". The 45-day limit is specified in the IPPs, hence the wording "seek to respond" in the Procedures.

[12] Refer to APP 12.9.

[13] Refer to IPP 6.4 and APP 12.8. The *Health Records Regulations* 2012 (Vic) specify maximum fees applicable to the granting of access to Health Information.

[14] Relevant Principles - IPP 6, HPP 6 and APP 13.

[15] Refer to IPP 6.5 and APP 13.1.

[16] Refer to IPP 6.8 and APP 13.5.

[17] The APPs state that requests must be responded to within a "reasonable time". The 45-day limit is specified in the IPPs, hence the wording "seek to respond" in the Procedures.

[18] Refer to IPP 6.8, HPP 6 and APP 13.3.

[19] Refer to APP 13.2.

[20] Refer to IPP 6.6 and APP 13.4.

[21] Refer to HPP 6.5.

[22] Refer to HPP 6.5.

[23] Refer to HPP 6.7-6.8.

[24] Refer to HPP 6.5. There is no requirement to associate a statement where a decision or recommendation to the effect that the information should be corrected is pending or has been made under the Act or other law.

[25] Relevant Principles - IPP 9, APP 8 and HPP 9.

[26] Refer to IPP 9 and HPP 9.

[27] Refer to APP 8.1-8.2.