

## GUIDELINES TO COMPLY WITH THE UNIVERSITY OF MELBOURNE PRIVACY POLICY

These Privacy Policy guidelines explain how you, as an employee or agent of the University, must deal with personal and health information to ensure that the University complies with privacy laws.

**Relevant legislation:** *Information Privacy Act 2000* (Vic) - effective from 1 September 2002 and *Health Records Act 2001* (Vic)- effective from 1 July 2002.

In some instances the University may be contractually bound to comply with Commonwealth privacy laws. This will be when information is received or collected under a contract between the University and a Commonwealth body or agency.

A reference in these Guidelines to “information” is a reference to personal & health information, except where otherwise indicated. ([See Definitions](#))

The University has appointed a **Privacy Officer** and any queries or concerns you have should be directed to the **Privacy Officer**.

The University takes its privacy obligations very seriously. A breach of these Guidelines may have serious consequences for the University and for staff.

<b>COLLECTION OF INFORMATION</b>	<p>When we collect information we should ensure that:</p> <ul style="list-style-type: none"> <li>• the University needs the information; and</li> <li>• it is being collected fairly; and</li> <li>• the individual is informed of certain things.</li> </ul> <p>Be careful when collecting <u>health and sensitive information</u>! This kind of information should only be collected if:</p> <ul style="list-style-type: none"> <li>• we have consent; or</li> <li>• there are other good reasons for us to collect the information.</li> </ul> <p><b>Contact the Privacy Officer if you wish to collect such information and do not have consent.</b></p> <p><b>[further explanation and examples]</b></p>
<b>USE &amp; DISCLOSURE</b>	<p>We can only use and disclose information if:</p> <ul style="list-style-type: none"> <li>• the information is used for the main purposes for which it was collected; or</li> <li>• we have consent; or</li> <li>• there are other good reasons for us to use or disclose the information.</li> </ul> <p><b>Contact the Privacy Officer if you wish to use or disclose information without consent.</b></p> <p><b>[further explanation and examples]</b></p>
<b>ACCURACY OF INFORMATION</b>	<p>We need to take steps to ensure that information we hold and use is correct.</p> <p><b>[further explanation and examples]</b></p>
<b>SECURITY OF INFORMATION</b>	<p>We need to take steps to ensure that information is held securely.</p> <p><b>[further explanation and examples]</b></p>
<b>OPENNESS</b>	<p>We need to make the University's Privacy Policy available to anyone who asks for it.</p> <p><b>[further explanation and examples]</b></p>

<b>ACCESS</b>	We should comply with Freedom of Information laws in granting access to information. Requests for access to information should be re-directed to the <i>University's FOI officer</i> . <b>[further explanation and examples]</b>
<b>IDENTIFIERS</b>	We must not use an identifying number or code for an individual (like a tax file number) that has been assigned by another organisation unless it is necessary. <b>[further explanation and examples]</b>
<b>ANONYMITY</b>	If possible we must give individuals the option of not identifying themselves when dealing with the University. <b>[further explanation and examples]</b>
<b>TRANSFER OF INFORMATION OUTSIDE VICTORIA</b>	We must not transfer information outside Victoria without consent, unless: <ul style="list-style-type: none"> <li>• we can be confident that the organisation receiving the information will respect the privacy of the individual; or</li> <li>• the transfer is for the benefit of the individual</li> </ul> <b>[further explanation and examples]</b>
<b>TRANSFER OF INFORMATION TO ANOTHER HEALTH SERVICE PROVIDER</b>	The University should transfer information to another health service provider if requested to do so by the individual concerned. <b>[further explanation and examples]</b>

**[Back to Privacy Office Home Page]**

## DEFINITIONS

**'consent'** means free and informed consent. An individual is incapable of giving consent, if he or she is unable to understand the nature & effect of giving consent by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder.

**'personal information'** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include health information.

**'sensitive information'** means information or an opinion about an individual's:

- (i) racial or ethnic origin;
- (ii) political opinions;
- (iii) membership of a political association;
- (iv) religious beliefs or affiliations;
- (v) philosophical beliefs;
- (vi) membership of a professional or trade association;
- (vii) membership of a trade union;
- (viii) sexual preferences or practices; or
- (ix) criminal record.

**'health information'** means:

- (a) information or an opinion about:
  - (i) an individual's disability or physical, mental or psychological health (at any time); ;
  - (ii) an individual's expressed wishes about the future provision of health services to him or her; or
  - (iii) a health service provided, or to be provided, to an individual, that is also personal information; 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
- (d) 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 that is exempt under the Health Records Act 2001 (Vic).

**'information'** means both personal information and health information, unless otherwise indicated.

**'health service'** means:

- (a) an activity or service claimed or intended to
  - (i) assess, maintain or improve health;
  - (ii) diagnose illness, injury or disability; or
  - (iii) treat illness, injury or disability or suspected illness, injury or disability;
- (b) a disability service, palliative care service or aged care service;
- (c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist; or
- (d) a service, or a class of service, provided in conjunction with an activity or service referred to in paragraph (a), (b) or (c) that is prescribed as a health service.

The **'Privacy Officer'** of the University, Ms Janet White can be contacted for privacy related issues.

**'unique identifier'** means an identifier (usually a number) assigned by the University to an individual to identify that individual for the purposes of the operations of the University but does not include an individual's name.

## 1. COLLECTION OF INFORMATION

4.1 The University must not collect information unless the information is necessary for one or more of its functions or activities.

4.1 The University must collect information in a way that is fair and open and without being too intrusive.

**Example:** The University asks students for particular information in order to enrol them. In reality this information is used to determine funding and create a student profile for statistical purposes. This is not a fair and open collection of information.

**Example:** Jane, from student admin, notices a student in the cafeteria who has applied for special consideration. Jane needs further information from the student to assess the application and approaches him in order to collect further sensitive information. In these circumstances, the University is collecting information in a manner that is too intrusive.

1.3 At or before the time (or, if that is not practical, as soon as possible after) the University collects information from an individual, the University must take reasonable steps to ensure that the individual is aware of:

- (a) how to contact the University;
- (b) the fact that he or she is able to gain access to the information via freedom of information mechanisms;
- (c) the purposes for which the information is collected;
- (d) to whom (or the types of individuals or organisations to which) the University usually discloses information of that kind and if possible identify these;
- (e) any law that requires the particular information to be collected; and
- (f) any consequences for the individual if all or part of the information is not provided.

**Note:** This information will be included on all forms, applications, etc where information is collected by the University.

**Example:** All Forms and questionnaires should state briefly;

- the purpose for which the information is collected
- whether all fields of the form are compulsory or some are optional
- how we usually use the information and to whom it is usually disclosed
- the fact that the University's Privacy Policy is accessible on the University website
- the fact that an individual has the right to gain access to their personal information held by the University
- privacy enquiries may be emailed to [privacy-officer@unimelb.edu.au](mailto:privacy-officer@unimelb.edu.au)

- 4.1 If possible, the University must collect information about an individual only from that individual.
- 1.5 If the University does collect information about an individual from someone else, it must still take reasonable steps to ensure that the individual is or has been made aware of the matters listed in 1.3 above.

### **Sensitive or Health Information**

- 4.1 The University must not collect sensitive or health information about an individual unless:
- (a) the individual has consented; or
  - (b) the collection is required under law, or authorised by law in the case of health information; or

**Example:** In a job interview, Mary observes that the applicant is wearing a turban and makes a written note that the applicant is Sikh. This is a collection of sensitive information without the consent of the individual concerned.

There are limited additional circumstances where the University **may** collect sensitive or health information. The Privacy Officer must be consulted in relation to the collection of sensitive or health information contrary to the above guidelines.

### **[The detailed guidelines about the limited additional circumstances where sensitive and health information may be collected]**

View the provisions of the University's Privacy Policy dealing with the collection of information. It is effectively a summarised version of the above.

There are limited additional circumstances where the University **may** collect sensitive or health information. The Privacy Officer must be consulted in each instance to ensure that information is not collected in breach of Privacy laws. The **Privacy Officer** may authorise collection of information in the followings circumstances:

**For sensitive information:**

1. Where the collection is necessary for the establishment, exercise or defence of a legal claim; or
2. Where 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
3. Where the collection:
  - (a) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
  - (b) 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
  - (c) there is no reasonably practical alternative to collecting the information for that purpose; and
  - (d) it is impractical for the University to seek the individual's consent to the collection.

**Example:** If the University is being sued and hires an investigator to collect sensitive information on its behalf, the collection would be necessary for the defence of a claim.

**For health information:**

1. Where the collection is necessary for the establishment, exercise or defence of a legal claim; or
2. Where the information is collected from an organisation who is disclosing the information to the University for a purpose that the individual would reasonably expect; or
3. Where the information is collected from an organisation who is disclosing the information to the University for the purpose of:
  - (a) funding, management, planning, monitoring, improvement or evaluation of health services; or
  - (b) training provided by a health service provider to employees or persons working with the University,
4. Where the collection is made on suspicion that unlawful activity has been engaged in.

5. Where the collection is on behalf of a law enforcement agency and the University reasonably believes that the collection is necessary for a law enforcement function;
6. Where the information is necessary to provide a health service to the individual and the individual is **incapable of giving consent** and:
  - (a) it is not practical to obtain the consent of an authorised representative of the individual; or
  - (b) the individual does not have such an authorised representative;
7. Where the collection is necessary to prevent or lessen a serious and imminent threat to life, health, safety or welfare.
8. Where the collection is necessary for research, or the compilation or analysis of statistics, in the public interest:
  - (a) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
  - (b) it is impractical for the University to seek the individual's consent to the collection;

## 2. USE & DISCLOSURE

4.1 The University must not use or disclose information about an individual for a purpose (the secondary purpose) other than the main purpose of collection unless:

- (a) both of the following apply:
  - (i) the secondary purpose is related to the main purpose of collection and, in the case of sensitive and health information, determined by the Privacy Officer to be directly related to the main purpose of collection; and
  - (ii) the individual would reasonably expect the University to use or disclose the information for the secondary purpose; or
- (b) the individual has consented to the use or disclosure; or
- (c) the use or disclosure is required or authorised by law.

**Example:** If a department of the University placed the names and work contact details of its staff on its web site, this would constitute a disclosure of those individuals' personal information. Such a disclosure would be one that is made for a purpose that is related to the main purpose of collection (to facilitate the employment of the individual) and that would be reasonably expected by the individual. Hence, such a disclosure is allowed under the Act, and under the University's policy. However, individuals would not reasonably expect that their home contact details would be placed on the web site. Such a disclosure would be in breach of the Act and the University's policy.

**Example:** A company contacts the University wishing to verify a job applicant's qualifications. In these circumstances the University would be permitted to disclose the qualifications of the individual, as information pertaining to the qualifications attained by the individual are a matter of public record. Note: the actual grades obtained by students should not be released.

**Example:** Jane calls the University and asks for the contact details of a former tutor who she wishes to catch up with. In this case, the University should not disclose the information without consent because the information wasn't collected for this purpose.

**Example:** The University is served with a subpoena to produce certain documents containing health information in the Supreme Court. Unless the University applies to have the subpoena set aside, the documents must be produced as this is required by law.

**Example:** The University collects health information from a student through a special consideration application. The information should only be used by the University to assess special consideration and not for another purpose.

**Example:** A person telephones claiming to be the mother of a student and wishes to know the value of monies owed for a library fine for the student and how to pay. In these circumstances, the information should only be disclosed to the student himself or herself and not to the student's mother, regardless of the student's age, as this would not be reasonably expected.

**Example:** Every time a particular Internet service is used by a student, the student's log in details are recorded. These details can be linked to the student's personal information that the University holds (eg. subjects, age, etc). This information is kept on a database for statistical purposes and analysis of the service. Occasionally students who have used the service are contacted to answer questions to assist in management of the service offered. These uses of information are acceptable as long as students are made aware, even in a general sense, that information about their usage of various Internet services may be captured by the University and used for such purposes.

**Example:** A University department gets a call from Student Administration wanting to know if a student is accessing a service, or has outstanding fees. Using information in this way is a valid administrative purpose and one that is related to the primary purpose of collection and reasonably expected by any student.

**Example:** An information service provider requires login details of all students in order to allow them to have access to an Internet based resource. In these circumstances information may be disclosed to the service provider as the purpose of the disclosure is education related. Note requirements of security.

There are limited additional circumstances where the University **may** use or disclose personal information. The **Privacy Officer** must be consulted in relation to release or use of information contrary to the above guidelines.

[for detailed guidelines about the limited additional circumstances where information may be released or used]

View the provisions of the University's Privacy Policy dealing with the use and disclosure of information. It is effectively a summarised version of the above.

## LIMITED ADDITIONAL CIRCUMSTANCES FOR USE & DISCLOSURE OF INFORMATION

There are limited additional circumstances where the University **may** use or disclose information. The **Privacy Officer** must be consulted in each instance to ensure that information is not used or disclosed in breach of Privacy laws. The **Privacy Officer** may authorise use or disclosure of information in the followings circumstances:

### For both personal and health information:

1. 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 impractical 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 of the information will not disclose the information; and
  - (c) in the case of health information, the purpose cannot be served by the use or disclosure of information that does not identify the individual;
2. If the University believes that the use or disclosure is necessary to lessen or prevent a threat to life, health, safety or welfare
3. If 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 to investigate the matter or in reporting its concerns to relevant persons or authorities, in which case the **Privacy Officer** must make a written note of the use or disclosure
4. If the University believes that the use or disclosure is necessary for a law enforcement function by or on behalf of a law enforcement agency in which case the **Privacy Officer** must make a written note of the use or disclosure.

**Example:** A researcher at another University is conducting serious research and wishes to obtain the personal details of all students who have graduated from a particular course, over a certain number of years. In this case, the University could disclose the information if the researcher signs an agreement that the information will not be disclosed.

**Example:** Police wish to verify if an individual is enrolled at the University and whether they were in attendance at a particular tutorial. In this case the University can only disclose the information if the request is accompanied by a warrant or official police form quoting the specific section of an Act that entitles them to request the information or by a letter from someone of suitable authority (to be determined by the Privacy Officer) stating that the information is reasonably necessary for the investigation of an offence (in which case the matter should be referred to the Privacy Officer). A note should be made of the circumstances of the disclosure by the **Privacy Officer**.

**For personal information only:**

1. If disclosure is made to an officer or employee of the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS) and the officer or employee is authorised in writing by the Director-General of ASIO or ASIS to:
  - (a) receive the disclosure; and
  - (b) certify that the disclosure would be connected with the performance by ASIO or ASIS of its functions.

**For health information only:**

1. If all of the following apply--
  - (a) the University is a health service provider providing a health service to the individual; and
  - (b) the use or disclosure for the secondary purpose is reasonably necessary for the provision of the health service; and
  - (c) the individual is incapable of giving **consent** and--
    - (i) it is not reasonably practical to obtain the consent of an authorised representative of the individual; or
    - (ii) the individual does not have such an authorised representative
2. If all of the following apply--
  - (a) the organisation is a health service provider providing a health service to the individual; and
  - (b) the use is for the purpose of the provision of further health services to the individual by the organisation; and
  - (c) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively;
3. If the use or disclosure is for the purpose of:
  - (a) funding, management, planning, monitoring, improvement or evaluation of health services; or
  - (b) training provided by a health service provider to employees or persons working with the University,

and:

  - (c) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impractical for the University to seek the individual's consent to the use or disclosure; or
  - (d) reasonable steps are taken to de-identify the information,

and:

- (e) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

4. Where the University is a health service provider to an individual, the University may disclose health information about an individual to an immediate family member of the individual if--

- (a) either--
  - (i) the disclosure is necessary to provide appropriate health services to or care of the individual; or
  - (ii) the disclosure is made for compassionate reasons; and
- (b) the disclosure is limited to the extent reasonable and necessary for the purposes mentioned in paragraph (i); and
- (c) the individual is incapable of giving **consent** to the disclosure; and
- (d) the disclosure is not contrary to any wish--
  - (i) expressed by the individual before the individual became incapable of giving consent and not changed or withdrawn by the individual before then; and
  - (ii) of which the organisation is aware or could be made aware by taking reasonable steps; and
- (e) in the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, the immediate family member has sufficient maturity to receive the information.

5. The University may use or disclose health information about an individual where--

- (a) it is known or suspected that the individual is dead; or
- (b) it is known or suspected that the individual is missing; or
- (c) the individual has been involved in an accident or other misadventure and is incapable of consenting to the use or disclosure--

and the use or disclosure is to the extent reasonably necessary--

- (d) to identify the individual; or
- (e) to ascertain the identity and location of an immediate family member or other relative of the individual for the purpose of--
  - (i) enabling a member of the police force, a coroner or other prescribed organisation to contact the immediate family member or other relative for compassionate reasons; or
  - (ii) to assist in the identification of the individual--

and, in the circumstances referred to in paragraph (b) or (c)--

- (f) the use or disclosure is not contrary to any wish--
  - (i) expressed by the individual before he or she went missing or became incapable of consenting and not withdrawn by the individual; and
  - (ii) of which the organisation is aware or could have become aware by taking reasonable steps;

### 3. ACCURACY OF INFORMATION

- 4.1 The University must take reasonable steps to make sure that the personal and health information it collects, uses or discloses is accurate, complete and up to date, having regard for the purposes for which the information is to be used.
- 4.1 If you become aware or are notified that information is not accurate you should correct the situation as soon as possible.

**Note:** Because much information regarding a student's academic life is used to determine eligibility for allowances, etc, it is very important to students that this information is correct. The University should therefore take significant steps to ensure the accuracy of the information. On the other hand, less effort is needed to ensure that the addresses of past students are up to date, because there will be less serious consequences if they are wrong.

View the provisions of the University's Privacy Policy dealing with accuracy of information. It is effectively a summarised version of the above.

#### 4. SECURITY OF INFORMATION

- 4.1 The University must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- 4.2 The University should do everything within its power to prevent unauthorised use or disclosure of information that is transferred to an organisation in connection with the provision of services to the University.
- 4.3 The University must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose, except as described below. In relation to destruction of records, if the University has an obligation under an Act of Parliament to retain certain documents for certain periods, the University is able to do this.
- 4.4 If the University is providing health services to an individual, the University must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless--
- (a) the deletion is permitted, authorised or required by law; or
  - (b) the deletion is not contrary to law and occurs--
    - (i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or
    - (ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider--

whichever is the later.
- 4.5 If health information is deleted in the above circumstances, the **Privacy Officer** should make a written note of the name of the individual to whom the health information relates, the period covered by it and the date on which it was deleted.
- 4.6 If the University is a health service provider who transfers health information to another individual or organisation and does not continue to hold a record of that information it must make a written note of the name and address of the individual or organisation to whom it was transferred.
- 4.7 Staff are referred to the **Information Security Policy** and the **Information Technology Security Policy** which set out guidelines for the management & security of information.

**Note:** All contracts that the University enters into whereby information is transferred to a third party should contain extensive 'Privacy Clauses' requiring compliance with this policy to protect the information from misuse or loss. All such clauses should be reviewed and approved by the University's legal department.

**Note:** Sensitive or health information should not be left in unlocked filing cabinets or unattended on desks

**Note:** Information should only be accessed by those employees who need to access it to perform their duties and databases should be password protected where appropriate.

**Example:** If the University is asked to provide information over the phone **to anybody**, suitable security checks should be conducted before the information is provided.

**Example:** Under the Copyright Act there is a requirement that the University retains a record of photocopy requests. While such records are no longer needed by the University for its own purpose, the University would not be required to delete the records as the requirement of the Copyright Act is considered a legitimate 'purpose' under the Privacy Act.

View the provisions of the University's Privacy Policy dealing with security of information. It is effectively a summarised version of the above..

## 5 OPENNESS

- 5.1 The University must set out in a document clearly expressed policies on its management of personal information. The University must make the document available to anyone who asks for it.
- 5.2 On request by a person, the University must take reasonable steps to let the person know, generally, what sort of personal information it holds about them, for what purposes, how it collects, holds, uses and discloses that information and how individuals can get access to the information.

**Note:** The University's public Privacy Policy is available on the University web site and from University Administration. Any further questions can be directed to the Privacy Officer.

## 6 ACCESS

- 6.1 The University is required to provide individuals with access to and correction of the personal information it holds about them in accordance with the *Freedom of Information Act 1982 (Vic)*.
- 6.2 If the University is providing health services to an individual, the University must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless--
- (a) the deletion is permitted, authorised or required by law; or
  - (b) the deletion is not contrary to law and occurs--
    - (i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or
    - (ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider—whichever is the later.
- 6.3 If health information is deleted in the above circumstances, the **Privacy Officer** should make a written note of the name of the individual to whom the health information relates, the period covered by it and the date on which it was deleted.

View the provisions of the University's Privacy Policy dealing with access to information . It is effectively a summarised version of the above.

## 7 IDENTIFIERS

- 7.1 The University must not adopt as its own unique identifier of an individual a unique identifier that has been assigned by another organisation unless:
- (a) it is necessary to enable the University to carry out any of its functions efficiently; or
  - (b) it has obtained the consent of the individual to the use of the unique identifier;
- 7.2 The University must not use or disclose a unique identifier assigned to an individual by another organisation unless:
- (a) it is necessary for the University to fulfil its obligations to the other organisation; or
  - (b) it is necessary to lessen or prevent a threat to life, health or public welfare;
  - (c) it is necessary to investigate a crime, or assist an official body with law enforcement; or
  - (d) it has obtained the consent of the individual to the use or disclosure.
- 7.3 The University must 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 purposes for which the unique identifier was assigned.

**Example:** We can use a student number from Monash University when a Monash student enrolls with us to use the reciprocal borrowers program, as they are necessary to run the program efficiently.

**Example:** We cannot use an identifier used by Australian Tax Office (eg tax file number), Vic Roads (drivers licence number) etc as a student number to identify a student enrolled at the University

## 8 ANONYMITY

- 8.1 Wherever it is lawful and practical, individuals must have the option of not identifying themselves when entering transactions with the University.

**Example:** An individual wishing to make a cash purchase of a souvenir from the University Shop should not be required to give their details before purchase.

## 9 TRANSFER OF INFORMATION OUTSIDE VICTORIA

- 9.1 The University may transfer personal information about an individual to someone (other than the University or the individual) who is outside Victoria only if:
- (a) the recipient of the information is subject to a law, binding scheme or contract (including a contract with the University) which upholds principles that are substantially similar to this Policy; or
  - (b) the individual consents to the transfer; or
  - (c) the transfer is necessary for the performance of a contract in the interest of the individual; or
  - (d) the transfer is for the benefit of the individual and it would be impractical to obtain their consent; or
  - (e) in the case of health information, the transfer is authorised by law.

**Example:** An official alumni organisation of the University operates from Singapore and is organising an event for former overseas students. The organisation wants contact details of the former students from the University. Assuming that the University already had consent from students in general to use and disclose information for alumni purposes, the University would still have to be sure that Singapore's privacy laws are substantially the same as ours, or ask the alumni organisation to sign a contract guaranteeing that the information will be treated in accordance with this policy.

View the provisions of the University's Privacy Policy dealing with the transfer of information outside Victoria. It is effectively a summarised version of the above.

## **10 TRANSFER OF INFORMATION TO ANOTHER HEALTH SERVICE PROVIDER**

10.1 If the University is a health service provider to an individual and the individual--

- (a) requests the University to make health information relating to the individual held by the University available to another health service provider; or
- (b) authorises another health service provider to request the University to make health information relating to the individual available to the requesting health service provider--

the University must, on payment of a fee not exceeding the prescribed maximum fee, provide a copy or written summary of that health information to that other health service provider.

10.2 The University must comply with these requirements as soon as practical.