



## Information Privacy Policy

### Table of Contents

Purpose .....	1
Scope .....	1
Definitions .....	1
Policy Statement .....	2
Complaints Provision .....	3
Responsibilities .....	3
Legislative Context .....	4
Associated Documents .....	4
Information Privacy Principles and Health Privacy Principles .....	4
Principle 1 - Collection .....	4
Principle 2 - Use and Disclosure .....	5
Principle 3 - Data Quality .....	6
Principle 4 - Data Security .....	6
Principle 5 - Openness .....	6
Principle 6 - Access and Correction .....	6
Principle 7 - Unique Identifiers .....	7
Principle 8 - Anonymity .....	8
Principle 9 - Transborder Data Flow .....	8
Principle 10 - Sensitive Information .....	8

### Purpose

This document describes the University’s policy regarding the collection, use, storage, disclosure of and access to personal information, including health information, in relation to the personal privacy of past and present staff, students and other members of the University.

### Scope

This policy applies to personal and health information collected by the University concerning staff, students, prospective students, individual clients and other individuals. It does not apply to information about corporations.

This policy does not apply to personal information that is:

1. in a publication that is available to the public;
2. kept in a library, art gallery or museum for reference, study or exhibition purposes;
3. a public record under the control of the Keeper of Public Records that is available for public inspection; or
4. an archive within the meaning of the *Commonwealth Copyright Act* 1968.

This policy must be observed by all University staff, consultants, external contractors and students who have access to personal and health information held by the University.

### Definitions

<b>Personal information</b>	Means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true
-----------------------------	---

**Warning - Uncontrolled when printed! The current version of this document is kept on the UB website.**



	or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
<b>Health information:</b>	<p>means-</p> <ul style="list-style-type: none"> <li>a. information or an opinion about: <ul style="list-style-type: none"> <li>i. the physical, mental or psychological health (at any time) of an individual; or</li> <li>ii. a disability (at any time) of an individual; or</li> <li>iii. an individual's expressed wishes about the future provision of health services to him or her; or</li> <li>iv. a health service provided, or to be provided, to an individual;</li> </ul> </li> <li>b. that is also personal information; or</li> <li>c. other personal information collected to provide, or in providing, a health service; or</li> <li>d. 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</li> <li>e. 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.</li> </ul>
<b>Sensitive information:</b>	<p>means information or an opinion about an individual's:</p> <ul style="list-style-type: none"> <li>1. racial or ethnic origin;</li> <li>2. political opinions;</li> <li>3. membership of a political association;</li> <li>4. religious beliefs or affiliations;</li> <li>5. philosophical beliefs;</li> <li>6. membership of a professional or trade association;</li> <li>7. membership of a trade union;</li> <li>8. sexual preferences or practices; or</li> <li>9. criminal record;</li> </ul> <p>that is also personal information.</p>

## Policy Statement

It is University policy that:

1. The collection and use of personal and health information must relate directly to the legitimate purposes of the University.
2. Individuals must aware of, or informed of, the purposes for which personal and health information is obtained.
3. The University will take all reasonable measures to ensure that the personal and health information it receives and holds is up to date.
4. The University will take all reasonable measures to store personal and health information securely.
5. Individuals are entitled to have access to their own records, unless prevented by law.
6. Third party access to personal and health information may only be granted in accordance with privacy principles and University policy and procedure.
7. The University will amend records shown to be incorrect.

**Warning - Uncontrolled when printed! The current version of this document is kept on the UB website.**



8. The University will observe the Information Privacy Principles specified in the *Information Privacy Act 2000* (Vic), and the Health Privacy Principles specified in the *Health Records Act 2001* (Vic), as outlined in the attached Addendum – Information Privacy Principles and Health Privacy Principles.

Principle 1 – Collection

Principle 2 – Use and Disclosure

Principle 3 – Data Quality

Principle 4 – Data Security

Principle 5 – Openness

Principle 6 – Access and Correction

Principle 7 – Unique Identifiers

Principle 8 – Anonymity

Principle 9 – Transborder Data Flow

Principle 10 – Sensitive Information

## Complaints Provision

Any person, whether or not a member of the University, who on reasonable grounds believes that the University has breached this policy may complain in writing to the University Privacy Officer – [privacyofficer@ballarat.edu.au](mailto:privacyofficer@ballarat.edu.au) specifying details of the alleged breach.

It is requested that the written complaint be forwarded within six (6) months of the time the complainant first became aware of the breach. If a complaint is received after this time, the University may not be able to investigate the complaint.

The Privacy Officer shall investigate complaints as expeditiously as practicable and shall provide a written copy of the findings of fact and recommendations made to both the Vice-Chancellor and to the complainant within 45 days of receipt of the complaint.

The Vice-Chancellor or nominee will determine what action will be taken on any recommendation contained in the findings of the Privacy Officer.

The Privacy Officer will keep a confidential record of complaints.

The University's Privacy Officer is located within the Legal Office.

## Responsibilities

The Vice President, Corporate Services will be responsible for control and maintenance of the [Information Privacy Policy](#).

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

1. keep records which are required to be kept under this Policy;

**Warning - Uncontrolled when printed! The current version of this document is kept on the UB website.**



2. investigate complaints concerning a breach of the Information Privacy Principles and Health Privacy Principles;
3. conduct an ongoing review of the University's practices and procedures to ensure that they comply with this Policy, current legislation and best practice; and
4. inform and assist staff with respect to privacy issues.

The Privacy Officer(s) are located within the Legal Office, Mt Helen Campus and can be contacted by email to [privacyofficer@ballarat.edu.au](mailto:privacyofficer@ballarat.edu.au).

## Legislative Context

- Victorian Information Privacy Act 2000
- Victorian Health Records Act 2001
- Commonwealth Copyright Act 1968
- Commonwealth Privacy Act 1988
- Victorian Freedom of Information Act 1982
- Victorian Public Records Act 1973

## Associated Documents

- [Information Privacy Statement - Collection, Use and Disclosure of Personal Information](#).

## Information Privacy Principles and Health Privacy Principles

The University will comply with the Information Privacy Principles contained in the *Information Privacy Act 2000* (Vic) and the Health Privacy Principles contained in the *Health Records Act 2001* (Vic). A summary of these principles, as adapted for the University, is set out below:

### Principle 1 - Collection

1. The University:
  - will collect personal information only if the information is necessary for one or more of its functions or activities;
  - must collect personal and health information only by lawful and fair means and not in an unreasonably intrusive way.
2. The University will collect health information only if the information is necessary for one or more of its functions or activities and with consent, or it falls within an exception specified in the *Health Records Act*.
3. When the University collects personal and health information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of:
  - a. the identity of the University and how to contact it; and
  - b. the fact that he or she is able to gain access to the information; and
  - c. the purposes for which the information is collected ("the primary purposes"); and
  - d. to whom (or the types of individuals or organisations to which) the University usually discloses information of that kind; and
  - e. any law that requires the particular information to be collected; and
  - f. the main consequences (if any) for the individual if all or part of the information is not provided.
4. If it is reasonable and practicable to do so, the University will collect personal and health information about an individual only from that individual. However, there will be instances where the University will obtain such information from other sources, e.g. references for employment purposes, results data for prospective students,

**Warning - Uncontrolled when printed! The current version of this document is kept on the UB website.**



verification of formal qualifications of staff and students etc. In such instances the University will take reasonable steps to ensure that the individual is or has been made aware of the matters listed in Principle 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

## Principle 2 - Use and Disclosure

1. The University will not without the prior consent of an individual use or disclose personal or health information about that individual for a purpose (“the secondary purpose”) other than the primary purpose of collection except in any of the following situations:
  - a. both of the following apply
    - the secondary purpose is related to the primary purpose of collection and, if the personal information is *sensitive information*, directly related to the primary purpose of collection;
    - the individual would reasonably expect the University to use or disclose the information for the secondary purpose; or
  - b. for personal information, if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual;
    - 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 that the recipient of the information will not disclose the information;

for health information, if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest as contained in the Statutory Guidelines on Research 2002 under the *Health Records Act 2001 (Vic)* or

- a. the University reasonably believes that the use or disclosure is necessary to lessen or prevent either:
  - a serious and imminent threat to an individual’s life, health, safety or welfare; or
  - a serious threat to public health, public safety or public welfare; or
- b. the University has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- c. the use or disclosure is required or authorised by or under law; or
- d. the University reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency:
  - the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
  - the enforcement of laws relating to the confiscation of the proceeds of crime;
  - the protection of the public revenue;
  - the prevention, detection, investigation or remedying of seriously improper conduct;
  - the preparation for, or conduct of, proceedings before any court or tribunal; or
- e. the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Service (ASIS), in connection with its function, has requested the University to disclose the personal information and:
  - the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and
  - an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.
- f. Any disclosure under paragraph 2.1(c), (d), (e), (f) and (g) can only be made by the Vice-Chancellor or by the University Solicitor. A written note must be made of a disclosure made under paragraph 2.1(d) or (e).



## Principle 3 - Data Quality

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

## Principle 4 - Data Security

4.1 The University will take reasonable steps to protect the personal and health information it holds from misuse and loss and from unauthorised access, modification or disclosure.

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

## Principle 5 - Openness

5.1 The University will make the Privacy Policy available to anyone who asks for it.

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

## Principle 6 - Access and Correction

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

- a. providing access would pose a serious and imminent threat to the life or health of any individual; or
- b. providing access would have an unreasonable impact on the privacy of other individuals; or
- c. the request for access is frivolous or vexatious; or
- d. the information relates to existing legal proceedings between the University and the individual, and the information would not be accessible by the process or discover or subpoena in those proceedings; or
- e. 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; or
- f. providing access would be unlawful; or
- g. denying access is required or authorised by or under law; or
- h. providing access would be likely to prejudice an investigation of possible unlawful activity; or
- i. providing access would be likely to prejudice:
  - the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or
  - the enforcement of laws relating to the confiscation of the proceeds of crime; or
  - the protection of public revenue; or
  - the prevention, detection, investigation or remedying of seriously improper conduct; or
  - the preparation for or conduct of, proceedings before any court or tribunal, or implementation of its orders by or on behalf of a law enforcement agency; or

**Warning - Uncontrolled when printed! The current version of this document is kept on the UB website.**



j. ASIO, ASIS or a law enforcement agency performing a lawful security function asks the University not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 Where providing access would reveal evaluative information generated within the University in connection with a commercially sensitive decision-making process, the University may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

6.3 If the University is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (j) (inclusive), the University will, if reasonable, upon request by the individual to the University's Privacy Officer consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 The University reserves the right to charge for providing access to personal and health information, and if it does so it will:

- a. advise an individual who requests access to personal or health information that the University will provide access on the payment of the prescribed fee; and
- b. may refuse access to the personal or health information until the fee is paid.

6.5 If the University holds personal or health information about an individual and the individual is able to establish to the satisfaction of the University that the information is not accurate, complete and up to date, the University will take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the University disagree about whether the information is accurate, complete and up to date, and the individual asks the University to associate with the information a statement from the individual claiming that the information is not accurate, complete or up to date, the University will take reasonable steps to do so.

6.7 The University will provide reasons for denial of access or a refusal to correct personal or health information.

6.8 If an individual requests access to, or the correction of, personal or health information held by the University, the University will:

- a. provide access, or reasons for the denial of access; or
- b. correct the personal or health information, or provide reasons for the refusal to correct the information; or
- c. provide reasons for the delay in responding to the request for access to or for the correction of personal or health information

as soon as practicable, but no later than 45 days for personal information and access to health information or 30 days for correction of health information after receiving the request.

6.9 Nothing in the Privacy Policy applies to a document containing information which would be subject to the provisions of the *Freedom of Information Act 1992* ("FOI Act").

If a person requests access to such a document then he or she must make an application under the FOI Act and access and correction of any errors will then be determined by the FOI Act. However, staff members may have access to their personal files on request, without the need for an FOI application to be made.

6.10 The University is not required to provide an individual with access to information about that individual if that information is generally available to the public.

## Principle 7 - Unique Identifiers

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

**Warning - Uncontrolled when printed! The current version of this document is kept on the UB website.**



7.2 The University will not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation.

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

## Principle 8 - Anonymity

Because of the nature of the University's core business, it will usually be impractical for individuals transacting with the University to have the option of not identifying themselves. However where it is lawful and practical to do so, the University will give the individual this option.

## Principle 9 - Transborder Data Flow

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

- a. the University reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information Privacy Principles or the Health Privacy Principles set out in this Policy; or
- b. the individual consents to the transfer; or
- c. the transfer is necessary for the performance of a contract between the individual and the University, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- d. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the University and a third party; or
- e. all of the following apply:
  - the transfer is for the benefit of the individual;
  - it is impracticable to obtain the consent of the individual to that transfer;
  - if it were practicable to obtain that consent, the individual would be likely to give it; or
- f. the University has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles or Health Privacy Principles set out in this Policy.

## Principle 10 - Sensitive Information

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

- a. the individual has consented; or
- b. the collection is required under law; or
- c. 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 cannot communicate consent to the collection; or
- d. the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite paragraph 10.1, the University may collect sensitive information about an individual if:

- a. the collection:

**Warning - Uncontrolled when printed! The current version of this document is kept on the UB website.**



- 
- 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
- b. there is no reasonably practicable alternative to collecting the information for that purpose; and
- c. it is impracticable for the University to seek the individual's consent to the collection.