# TABLE OF CONTENTS

1. INTRODUCTION
   1.1 Definitions
   1.2 Our Commitment to Privacy

2. WHAT IS PERSONAL INFORMATION?

3. WHAT ARE THE INFORMATION PROTECTION PRINCIPLES?
   3.1 Principle 1 – Collection of Personal Information for Lawful Purposes
   3.2 Principle 2 – Collection of Personal Information Directly from an Individual
   3.3 Principle 3 – Requirements when Collecting Personal Information
   3.4 Principle 4 – Other Requirements Relating to the Collection of Personal Information
   3.5 Principle 5 – Retention and Security of Personal Information
   3.6 Principle 6 – Information about Personal Information Held by Agencies
   3.7 Principle 7 – Access to Personal Information Held by Agencies
   3.8 Principle 8 – Alteration of Personal Information
   3.9 Principle 9 – Agency Must Check Accuracy of Personal Information before Use
   3.10 Principle 10 – Limits on Use of Personal Information
   3.11 Principle 11 – Limits on Disclosure of Personal Information
   3.12 Principle 12 – Special Restrictions on Disclosure of Personal Information

4. WHAT ARE THE HEALTH PRIVACY PRINCIPLES (HPPS)?
   4.1 HPP 12 – Identification
   4.2 HPP 13 – Anonymity
   4.3 HPP 15 – Linkage of Health Records

5. WHAT IS A PUBLIC REGISTER?

6. WHAT ARE INTERNAL REVIEWS UNDER THE PPIPA?

7. COLLECTING PERSONAL AND/OR HEALTH INFORMATION

8. PRIVACY IMPLEMENTATION PLAN

9. CONTACTING THE UNIVERSITY
1. **Introduction**

The University of Wollongong (“the University”) has produced this Privacy Management Plan (“Plan”) to comply with Section 33 of the NSW Privacy and Personal Information Protection Act 1998 (“PPIPA”).

The Plan is a strategic planning document which identifies:

- the policies and practices that the University has in place to comply with PPIPA and the Health Records and Information Privacy Act 2002 (“HRIPA”);
- the dissemination of privacy policies and practices within the University;
- procedures in relation to an internal review under part 5 of the Act; and
- other matters which are considered relevant to the University in relation to the Act.

This Plan may be revised or amended on occasions, in line with changes to the Act or any directions or rulings from the Office of the Commissioner.

As part of the University’s compliance to the Act, a copy of this Plan is freely available to any person.

Information relating to the PPIPA and HRIPA can be found at the Privacy Commissioner’s website: [http://www.lawlink.nsw.gov.au](http://www.lawlink.nsw.gov.au)

Click here for the University of Wollongong’s Privacy Website

1.1 **Definitions**

For the purposes of this Management Plan, “the University” means the University of Wollongong as established by the University of Wollongong Act 1989 (NSW) and includes all its associated and controlled entities.

1.2 **Our Commitment to Privacy**

The University is committed to ensuring the protection of the privacy of individuals pursuant to the PPIPA, the HRIPA and the Privacy Amendment (Private Sector) Act 2000 (Commonwealth).

2. **What is Personal Information?**

The PPIPA defines Personal information as follows:

“…”personal information” means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.”

“Personal information includes such things as an individual’s fingerprints, retina prints, body samples or generic characteristics. “
However, there are several exclusions to what Personal Information includes, for example:

- Information regarding an individual who has been deceased for more than 30 years;
- Information about an individual that is readily available in a publicly available publication;
- Information or an opinion about an individual’s suitability for appointment or employment as a public sector official; and
- Information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection.

The HRIPA defines health information as follows:

“In this Act, health information means:
(a) personal information that is information or an opinion about:
   (i) the physical or mental health or a disability (at any time) of an individual, or
   (ii) an individual’s express 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, 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, or an individual’s body parts, organs or body substances, or
(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual, but does not include health information, or a class of health information or health information contained in a class of document, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of the Act.”

3. **What are the Information Protection Principles?**

There are twelve Information Protection Principles (IPP’s), described in Sections 8 to 19 of the PIPPA.

**3.1 Principle 1 – Collection of Personal Information for Lawful Purposes**

The University must not collect personal information unless:

- The information is collected for a lawful purpose that is directly related to a function or activity of the University; and
- The collection of the information is reasonably necessary for that purpose.

The University must not collect any personal information by unlawful means.

**3.2 Principle 2 – Collection of Personal Information Directly from an Individual**

The University must, when collecting personal information, collect it from the individual to whom the information relates, unless:

- The individual has given consent for the collection of personal information from someone else, or
The information is provided by a parent or guardian of a person who is under the age of 16.

3.3 Principle 3 – Requirements when Collecting Personal Information

The University must ensure when collecting personal information from an individual that during or at a practicable time soon after the collection, the individual is made aware that:

- The fact that the information is being collected;
- The purposes for which the information is being collected;
- All recipients of the information;
- Whether the giving of information is voluntary or a legal requirement and any consequences that may arise from refusal to provide the requested information;
- What rights of access and/or correction (if any) that are allowed of the information; and
- The contact details of the University that is collecting the information and any other agent that is to hold the information.

3.4 Principle 4 – Other Requirements Relating to the Collection of Personal Information

The University must take reasonable steps to ensure that:

- The information it is collecting is relevant to that purpose, not excessive, accurate, up-to-date and complete; and
- The collection does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

3.5 Principle 5 – Retention and Security of Personal Information

The University must ensure that:

- The information collected is not kept for longer than is required for the purpose it was collected for;
- The information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information;
- All personal information held is protected, by taking safeguards to ensure that there is reasonable security in place to guard against loss, unauthorised access, use, modification or disclosure; and against all other misuse; and
- If it is necessary for the information to be given to a third party that the University takes all reasonable measures to prevent unauthorised use or disclosure of the information.

3.6 Principle 6 – Information about Personal Information Held by Agencies

The University must take such steps that it is reasonable for an individual to ascertain:

- Whether the University holds personal information;
- Whether that information held, relates to the individual;
- If the University holds such information on that individual:
  o The nature of that information;
  o The main purpose for which the information is used; and
  o The individual’s entitlement to gain access to the information.
3.7 Principle 7 – Access to Personal Information Held by Agencies

The University must, at the request of the individual to whom personal information relates and without excessive delay or expense, provide the individual with access to the information.

3.8 Principle 8 – Alteration of Personal Information

The University must, at the request of an individual to whom held personal information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

- is accurate; and
- having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up-to-date, complete and not misleading.

If the University believes that information provided by an individual does not warrant a change to the information held, then the University will take all reasonable steps necessary (if requested by the individual) to attach any statement, provided by the individual, of the amendment sought, so that it is capable of being read with the held information.

If the personal information is amended, in accordance with this principle, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the University.

3.9 Principle 9 – Agency Must Check Accuracy of Personal Information before Use

The University, in holding personal information, must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up-to-date, complete and not misleading.

3.10 Principle 10 – Limits on Use of Personal Information

The University, in holding personal information, must not use the information for a purpose other than that for which it was collected unless:

- The individual to whom the information relates has consented to the use of the information for that other purpose, or
- The other purpose for which the information is used is directly related to the purpose for which the information was collected, or
- The use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.
3.11 Principle 11 – Limits on Disclosure of Personal Information

The University, in holding personal information, must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a University or Public sector agency, unless:

- The disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or
- The individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or
- The University believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of the individual concerned or another person.

3.12 Principle 12 – Special Restrictions on Disclosure of Personal Information

The University must not disclose personal information relating to an individual’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

The University, in holding personal information, must not disclose the information to any person or body which is in a jurisdiction outside New South Wales unless:

- A relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or
- The disclosure is permitted under a privacy code of practice.

4. What are the Health Privacy Principles (HPPs)?

There are 15 HPPs set out in Schedule 1 of the HRIPA.

Other than HPP 12, 13 and 15, the HPPs are identical to the IPPs in relation to the collection, use, storage, and disclosure of health information.

4.1 HPP 12 – Identification

The University may only assign identification numbers if such identifiers are reasonably necessary to carry out its functions efficiently.

4.2 HPP 13 – Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves whenever entering into transactions with or receiving health services from the University.
4.3 HPP 15 – Linkage of Health Records

The University must obtain the express consent of an individual before the health information of the individual is included in linked records extending beyond the University.

5. What is a Public Register?

Both the PIPPA and the HRIPA define a public register as:

“A register of personal or health information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee).”

The University does not have any public registers.

6. What are Internal Reviews under the PIPPA?

An internal review will be held when a person is aggrieved by the conduct of the University over a privacy matter and brings it to their attention. The review will be conducted internally by the University.

An application for such a review must:

- be in writing;
- be addressed to The Privacy Officer at the University of Wollongong;
- specify an address in Australia to which a notice may be sent; and
- be lodged at an office of the University within 6 months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct which is the subject of the application.

The review will be conducted by the Privacy Officer, where the Privacy Officer is not substantially involved in the matter relating to the application. Other suitably qualified members of University staff may be called upon to conduct the review if the Privacy Officer is involved in the matter. At all times, the review will be held by an employee or officer of the University.

In reviewing the conduct which is the subject of the application, the individual dealing with the application must consider any relevant material submitted by:

- the applicant; and
- the Privacy Commissioner.

The University will endeavour to complete the review as soon as is reasonably practicable. The University will complete the review within 60 days from the day on which the application was received. If the review is not completed within this time the applicant may apply for a review of the conduct concerned to the Administrative Decisions Tribunal under Section 55.

On receiving an application for an internal review, the University must:

- inform the Privacy Commissioner as soon as is practicably possible of the application;
- keep the Privacy Commissioner informed of the progress of the internal review; and
■ inform the Privacy Commissioner of the findings of the review and of the action proposed to be taken by the agency in relation to the matter.

Once the internal review has been completed, the University may do one or more of the following:

■ take no further action on the matter;
■ make a formal apology to the applicant;
■ take such remedial action as it thinks appropriate;
■ provide undertakings that the conduct will not occur again; and
■ implement administrative measures to ensure that the conduct will not occur again.

Within 14 days of the completion of the review, the University will notify the applicant in writing of:

■ the findings of the review (and the reasons for those findings);
■ the action proposed to be taken by the agency (and the reasons for taking them); and
■ the right of the person to have those findings, and the agency’s proposed action, reviewed by the Tribunal.

7. Collecting Personal and/or Health Information

In the course of carrying out its functions, the University collects and records various personal information of individuals which is collected via application forms on paper or electronically. Such collected information includes:

■ Full Name
■ Date of Birth
■ Email Address
■ Academic Background
■ Languages spoken
■ Visa status
■ Health conditions (allergies / dietary requirements / physical restrictions/ mental health/disability
■ Nationality (inc Australian Aboriginal or Torres Straight Islander descent)

■ Full Address (inc overseas address)
■ Gender
■ Telephone Number (inc Mobiles)
■ Marital status
■ Tax File Number (TFN)
■ Passport details
■ Emergency Contact name and address

The University is obliged to collect and forward a students tax file number (TFN) to the Australian Taxation Office.

8. Privacy Implementation Plan

<table>
<thead>
<tr>
<th>Phase 1 Access</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Steps</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carry out workshop interviews with key stakeholders</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Identify and document information systems and processes that will have to be assessed</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Determine what information the University is collecting</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Determine how this information is being collected</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Determine where and how this information is being stored (e.g. on which databases, paper documents)</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Identify the purposes for which information is used and to whom this information is disclosed (internal and external to the University)</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Identify the extent to which customers are informed of the use of this information</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Determine if the information is accurate, current and relevant</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Collate all University forms &amp; document</td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>

### Phase 2 Design

<table>
<thead>
<tr>
<th>Steps</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop Privacy Policy for University</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Develop Privacy Management Plan (this plan)</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Develop Consent and disclosures and opt out for application forms</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Produce internal policy for access and complaints requests</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Develop training and awareness strategy for all staff</td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>

### Phase 3 Implement

<table>
<thead>
<tr>
<th>Steps</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement all disclosures / opt outs onto University forms</td>
<td>Completed</td>
<td></td>
</tr>
<tr>
<td>Provide training and awareness to all University staff</td>
<td>Completed</td>
<td></td>
</tr>
</tbody>
</table>

### Phase 4 Monitor

<table>
<thead>
<tr>
<th>Steps</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop reviews and audit procedures, run on regular basis</td>
<td>Ongoing</td>
<td></td>
</tr>
</tbody>
</table>
9. **Contacting the University**

In all instances, please contact the University in writing, at the following address:

The Privacy Officer  
Administration Building (36)  
University of Wollongong  
Wollongong NSW 2522