



Legal Services Unit, Financial Services Division

## PRIVACY POLICY

<b>Date approved</b>	11 October 2002	<b>Date Policy will take effect</b>	On approval	<b>Date of Next Review</b>	October 2007
<b>Approved by</b>	University Council				
<b>Custodian title &amp; e-mail address</b>	UOW Privacy Officer, Legal Services Unit				
<b>Author</b>	Angela Taylor, UOW Privacy Officer				
<b>Responsible Faculty/ Division &amp; Unit</b>	Legal Services Unit, Financial Services Division				
<b>Supporting documents, procedures &amp; forms of this policy</b>	<a href="#">Privacy Complaints Procedure</a> <a href="#">Privacy Complaint Internal Review Application Form</a>				
<b>References &amp; Legislation</b>	<a href="#">Privacy and Personal Information Protection Act, 1998 (NSW) ("PPIPA")</a> <a href="#">Health Records and Information Privacy Act, 2002 ("HRIPA")</a> <a href="#">Privacy Act, 1988 (Commonwealth)</a> <a href="#">National Privacy Principles (NPP)</a> <a href="#">NSW Privacy Commissioner</a> <a href="#">Freedom of Information Act, 1989 (NSW)</a> <a href="#">Independent Commission Against Corruption Act, 1988 (NSW)</a> <a href="#">Protected Disclosures Act, 1994 (NSW)</a> <a href="#">State Records Act, 1998 (NSW)</a> <a href="#">University of Wollongong Act, 1989 (NSW)</a> <a href="#">University of Wollongong By Law, 2005 (NSW)</a> <a href="#">Rules of the University of Wollongong</a>				
<b>Audience</b>	Public – accessible to anyone				
<b>Expiry date of Policy</b>	Not applicable				



Contents

[1 Purpose of Policy.....3](#)

[2 Definitions.....3](#)

[3 Application & Scope.....3](#)

[4 UOW's Commitment to Privacy.....3](#)

[5 Policy Principles.....3](#)

[6 Complaints and Further Information.....6](#)

[7 Roles & Responsibilities.....6](#)

[8 Version Control and Change History.....6](#)



## 1 Purpose of Policy

1. The University is committed to ensure that your privacy is protected. UOW and its controlled entities take all reasonable steps so that the collection, use, disclosure and handling of your information by UOW complies with the law.

## 2 Definitions

Word/Term	Definition (with examples if required)
UOW	University of Wollongong including all associated and controlled entities of the UOW established by the University of Wollongong Act 1989.
Student	Any person who is a member of the public and not an employee of the University, and is entitled to protection under current privacy legislation in Australia

## 3 Application & Scope

Not Available

## 4 UOW's Commitment to Privacy

1. The University is committed to ensuring the protection of the privacy of individuals pursuant to the Privacy and Personal Information Protection Act, 1998 ("PPIPA"), the Health Records and Information Privacy Act, 2002 ("HRIPA"), and the Privacy Amendment (Private Sector) Act, 2000 (Commonwealth).
2. A full explanation of the National Privacy Principles (NPP) for which the University adheres to can be found at <http://www.privacy.gov.au>
3. As part of the University's commitment to comply with the Privacy and Personal Information Protection Act, 1998 (NSW) a [Privacy Management Plan](#), details the steps to be taken.

## 5 Policy Principles

### Collection of Personal and Health Information

1. In connection with the collection of personal and health information the University will:
  - a. not collect such information unless the information is necessary for one or more of its functions or activities;
  - b. collect such information by lawful and fair means;
  - c. not act in an unreasonably intrusive way to collect such information;
  - d. take reasonable steps to ensure the individual is aware of:
    - i. the identity of the organisation collecting the information;
    - ii. the University's contact details;
    - iii. the purpose for which the information is collected;
    - iv. any organisation which the University may pass the collected information to;
    - v. any law that requires the collection of particular information; and
    - vi. any consequences (if any) arising from the failure to provide any requested information.
  - e. collect the required information from the actual individual, where it is reasonable and practical to do so; and
  - f. take reasonable steps to inform an individual of the above statements where information has been collected on that individual by someone else.



---

## Use and Disclosure

2. In its use and disclosure of personal and health information the University will not use or disclose such information about an individual for a purpose other than the stated primary purpose unless:
  - a. a secondary purpose is related to the primary purpose;
  - b. it was reasonable for the individual to expect the University to use or disclose the information for a second purpose;
  - c. consent from the individual has been granted;
  - d. the information is to be used for direct marketing and is not of a sensitive nature; but not for use by an external marketing organization, for example a bank, unless:
    - i. it is related to the primary purpose;
    - ii. it was reasonable for the individual to expect such use; and
    - iii. it is easy and free to “opt out” of receiving further material,
  - e. the information is health related and its use or disclosure is necessary for research, statistical use or relevant to public health and safety;
  - f. the University believes that its use or disclosure is necessary to lessen or prevent:
    - i. a serious and imminent threat to someone’s life, health, or safety; or
    - ii. a serious threat to public health or public safety.
  - g. suspected unlawful activity has, or is being, or may be engaged in and the use and disclosure is necessary for the investigation of these acts or to the supply of relevant persons or authorities;
  - h. the University believes that information is necessary for particular enforcement bodies for their investigation into criminal offences or breaches of law.
3. This specifically includes electronic mail (e-mail) in that:
  - a. the University reserves the right to read, copy, audit and take action on all email sent received and or stored on its servers or networks;
  - b. email can be subject to production in litigation or other investigations; and
  - c. it is unacceptable to use the email facilities of the University contrary to the University’s rules.

## Information Quality

4. The University takes all reasonable steps to make sure that any personal and/or health information it collects, uses or discloses is accurate and up-to-date.

## Security

5. The University will take all reasonable steps to protect the personal and health information it holds from misuse and loss.
6. The University will also take adequate precautions to protect such information from any unauthorised access, modification, or disclosure.
7. The University holds information on a series of databases which are password protected and protected by other security measures established and enforced by its IT Service department.
8. The University takes all reasonable steps to destroy or de-identify any personal information in its possession or control when this information is no longer needed for any purpose for which it was collected.
9. The University will ensure that any destruction of information is by a secure means, such as shredding, pulping, or disintegration of paper. For electronically held information, reasonable steps will be taken to remove information dependent on the medium on which it is held and available erasure methods at the time.



- 
10. In de-identification of information, the University will ensure that all traces of information that may identify an individual are removed. This de-identification will be permanent so that no cross-referencing from other information can ascertain an individual's identity by the University or any other organisation.

### **Openness**

11. The University sets out this document in compliance with NPP 5 to provide a clear reference to the University's Privacy Policy, which is available to anyone who requests it.
12. The University also provides reference on its own website to this and other related Privacy documents, for public perusal.
13. The University will, upon request, inform an individual of what sort of information the University holds, and for what purpose and how it collects, uses and discloses that information.

### **Access and Correction**

14. The University holds personal and health information on some or all students enrolled in University courses. Such information is available for the individual to access on request except to the extent that:
  - a. providing the information, be it personal or health related information, poses a threat to the life of an individual, or compromises the privacy of other individuals; and
  - b. the access would be deemed unlawful, may prejudice a current negotiation/investigation or it has been requested by an enforcement body performing a lawful security function to deny access.
15. The University requires written requests for access to personal information. The University will only supply personal information to an individual once the University is satisfied as to the identity of the individual. The individual will be expected to provide adequate proof of identification.
16. The University takes reasonable steps to ensure all information is accurate, correct, and up-to-date. If an individual believes that the University holds out-of-date, incorrect or inaccurate information the University will endeavour to change this information unless it deems the changes to be unnecessary or incorrect.
17. If the University denies a request for access or change to an individual's personal or health information, it will provide reasons for this refusal.
18. If the University and individual cannot agree on the status of the information held, the University will, at the request of the individual, take reasonable steps to attach a statement of this fact to the individuals currently held information.
19. The University may charge a reasonable but not excessive administration fee to provide information after a request for access has been made. The charge will be notified to the individual on receipt of a written access request to the Privacy Officer.

### **Identifiers**

20. The University will not adopt identifiers for individuals that have been previously assigned by:
  - a. an agency;
  - b. an agent of an agency acting in the its capacity as an agent; and
  - c. a contracted service provider for that contract.
21. The University provides its own identifier in the form of a Student Identification Number.

### **Anonymity**

22. The University will, where lawful and practicable, offer an individual the option of not identifying him or herself when entering transactions with the University for the purposes of a health service provided by the University.



## Transborder Data Flows

23. In the course of its business the University may provide student details to organisations outside of Australia, especially where overseas students are concerned. The University will only provide this information:
  - a. where it believes the recipient is subject to similar privacy laws and policies to its own; or
  - b. where an individual consents to the transfer of information; or
  - c. where the transfer is necessary for the performance of a contract between the individual and the University.
24. The University will take all reasonable steps to ensure that any information, which is transferred to a recipient abroad, is held, used or disclosed under a consistently similar policy.

## 6 Complaints and Further Information

1. If an individual believes that the University has breached their privacy that person should make a complaint, in writing, to the Privacy Officer of the University.
2. The individual should notify the University of any suspected breach within six (6) months of them discovering that breach.
3. The University will conduct an internal investigation on receiving a complaint.
4. The University will endeavour complete the internal review within 60 days.
5. On completion of the internal review the University will inform the individual in writing of the outcome of the review. The University will choose to do one or more of the following:
  - a. take no further action;
  - b. make a formal apology to the individual who made the complaint;
  - c. take any remedial action deemed necessary or appropriate; and
  - d. put in place practices and/or policies to ensure that this type of breach does not occur again.
6. The individual will be informed of the reasons behind whatever decision is made.
7. Please direct your enquiries in writing in the first instance to:
 

The Privacy Officer  
Administration Building (36)  
University of Wollongong  
Wollongong NSW 2522
8. For further information regarding Privacy contact:
  - a. the Federal Privacy Commissioner on 1300 363 992 or see their website at <http://www.privacy.gov.au>
  - b. Privacy NSW, the Office of NSW Privacy Commissioner on (02) 9268 5588 or see their website at [http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_index](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index)

## 7 Roles & Responsibilities

1. The UOW Privacy Officer is responsible for dealing with all issues regarding privacy.

## 8 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	11 October 2002	University Council	New Policy.



2	26 October 2004	Administrative Committee	Privacy Policy put into new Policy Template.
3	6 May 2009	Vice Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh