



Privacy Information Sheet – General

The University is subject to Commonwealth and NSW privacy laws, which protect the privacy of a person's personal or health information ("Privacy Laws").

The University collects, holds and uses personal and health information about staff and students. The Privacy Laws outline how the University can collect, store, use and disclose that information.

Personal information is any information or opinion about a person whose identity is apparent or can reasonably be deduced. This includes records containing a person's name, address, sex etc or physical information such as fingerprints, DNA or body samples.

Personal information does not include information about:

- a person who has been dead for more than 30 years
- a person contained in a publicly available document
- information about a person's suitability for employment as a public sector official

Health information is personal information:

- about the physical or mental health or disability of a person,
- about a person's express wishes about future health services,
- about health services provided to a person,
- collected to provide a health service,
- about donation of body parts by a person;
- genetic information predictive of health.

There are 12 Rules of Information Protection¹ that the University must comply with, that outline how the University can:

1. collect
2. store
3. provide access to;
4. use; and
5. disclose

personal or health information. These rules are contained in a table at the end of this Information Sheet.

¹ Sourced from a Privacy NSW brochure titled "Your Privacy: Protecting Privacy in NSW".



Disclosure

The most frequently asked question within the University regarding privacy is “**when can I disclose someone’s personal information?**”.

The University has publicly stated in the media and through adoption of its [Privacy Policy](#) that it will comply with the spirit and letter of the Privacy Laws.

There are certain circumstances where disclosure won’t breach the Privacy Laws, such as:

- the person providing written consent to that disclosure (whether this is when the University collects that information, or is provided later in writing).
- The University is compelled to disclose by:
 - Order of Law – such as subpoena, [FOI application](#). In other words, we cannot refuse to provide documents under a court order or FOI Application on the basis of privacy.
 - A Law Enforcement Agency – such as police investigation proceedings for an offence, or seeking information about a person reported to police as missing

However, **any disclosure of personal or health information must be made with the utmost caution**, and you should consult the Principal Privacy Officer, contact details below.

Who to Contact About Privacy

Legal Services has three privacy officers registered with Privacy NSW.

Your first contact should be to Angela Taylor, who is principal privacy officer. Her contact details are:

Angela Taylor

Principal Privacy Officer
University of Wollongong
Legal Services
Building 36, Level 4
Wollongong NSW 2522

Phone: (02) 4221 3277

Fax: (02) 4221 4254

Email: angelata@uow.edu.au

If she is not available, you should contact either Jovanka Naumoska or Kristine Sheridan.

Jovanka Naumoska
Privacy Officer
University of Wollongong
Legal Services
Building 36, Level 4

Kristine Sheridan
Privacy Officer
University of Wollongong
Legal Services
Building 36, Level 4



Wollongong NSW 2522

Wollongong NSW 2522

Phone: (02) 4221 5817

Phone: (02) 4221 3131

Fax: (02) 4221 4254

Fax: (02) 4221 4254

Email: jovanka@uow.edu.au

Email: kristine@uow.edu.au

The 12 Rules of Information Protection are:

| | |
|------------|---|
| Collection | 1. Must be for a lawful purpose and be directly related to the University's activities. |
| | 2. Must be collected directly from a person, unless they have given their consent otherwise (such as a parent or guardian giving consent to minors to provide information). |
| | 3. Inform the person why the information is being collected, who will be storing and using it, and how it will be used. |
| | 4. accuracy – the University must ensure the information is accurate, up to date and not unreasonably intrusive. |
| Storage | 5. information must be stored securely and kept no longer than is required under the State Records Act. |
| Access | 6. In addition to 3 above, must advise the person that they have a right of access to their information. |
| | 7. access for a person to their own information must be without unreasonable delay and expense. |
| | 8. the person has a right to update, correct or amend their information. |
| Use | 9. the University must ensure the information is accurate before using it. |
| | 10. the University can only use that information for: <ul style="list-style-type: none"> a. the purpose for which it is collected b. a directly related purpose to (a) above. |
| Disclosure | 11. disclosure of information about a person can only be made if: <ul style="list-style-type: none"> a. upon collection, such disclosure was advised to the person; b. the person has consented to the disclosure; c. it is for a purpose related to the purpose stated upon collection, and the University doesn't think the person will object d. there is a serious and imminent threat to that person or another person's life or health. |



- | | |
|--|---|
| | <p>12. disclosure of the following information can only be made if it is necessary to prevent a serious and imminent threat to the life or health of that person or another person:</p> <ul style="list-style-type: none">a. ethnic or race origin;b. political opinions;c. religious or philosophical beliefs;d. trade union membership; ore. sexual activities. |
|--|---|

Please consult with a [Privacy Officer](#) if you have any questions.