



# University Recordkeeping Manual

## Part Eleven

# PRIVACY

# Part 11 – Privacy

## Table of Contents

1. The University Privacy Policy	2
2. University responsibilities	2
3. Dealing with requests for personal information from outside the University	3
3.1 Requests from the police	3
3.2 Requests from Government departments	3
3.3 Subpoenas and court orders	4
3.4 Confirming is someone is a graduate	4
4. Frequently asked questions	4
5. Further information	5

# Part 11 - Privacy

## 1. The University Privacy Policy

In June 2000 the Vice-Chancellor approved the following policy. It was amended by Senate in August 2007.

The University will collect, manage, use and disclose personal information in accordance with all relevant legislation and standards. The Information Protection Principles contained in Part 2 of the NSW *Privacy and Personal Information Protection Act 1998*, except when qualified by any relevant Codes of Practice, will underpin all matters related to personal information in the University.

The University will:

- Only collect personal information for lawful purposes;
- When reasonably possible, only collect personal information from the individual to whom it relates;
- Only collect such information as is reasonably necessary;
- Notify the individual concerned when it collects personal information either at the time of collection or as soon as practicable thereafter;
- State what the personal information will be used for;
- State who will receive the personal information;
- State if the collection is voluntary, and the consequences for individuals if it is not, or only in part, provided;
- Provide contact details regarding who to contact regarding access to and correction of the personal information;
- Take reasonable steps to ensure that personal information holdings are relevant, not excessive, accurate, up to date, complete and that the collection does not unreasonably intrude on the personal affairs of individuals;
- Retain personal information for no longer than is necessary and then dispose of it lawfully and securely;
- Protect personal information from loss, unauthorised access, use, modification or disclosure or other misuse;
- Ensure that all reasonable steps are taken to ensure that personal information is not used or disclosed without authorisation by external service providers;
- not disclose personal information outside the University or its affiliated student bodies except where:
  - the subject of information has consented to the disclosure, or has been notified of the likelihood of the disclosure; or
  - the University is required by legislation, court order or other legally enforceable instrument and the request isn't in an appropriate written form; or
  - disclosure is reasonably believed to be necessary to prevent or lessen a serious and imminent threat to the life or health of any person

- otherwise and to the extent permitted by the Privacy and Personal Information Protection Act 1998.

In no other circumstances will personal information be disclosed.

The NSW Privacy and Personal Information Protection Act defined personal information very broadly. For more details see the University's Privacy Management Plan ([www.usyd.edu.au/arms/privacy](http://www.usyd.edu.au/arms/privacy)).

In 2004 the NSW Health Records and Information Privacy Act 2002 instituted a more rigorous privacy regime for matters concerned with health information. See the University's privacy web site as above or contact the privacy officers for more information.

## **2. University responsibilities**

- only collect personal information for lawful purposes;
- when reasonably possible, only collect personal information from the individual to whom it relates;
- only collect such information as is reasonably necessary;
- notify the individual concerned when it collects personal information either at the time of collection or as soon as practicable thereafter;
- state what the personal information will be used for;
- state who will receive the personal information;
- state if the collection is voluntary and the consequences for individuals if it is not, or only in part, provided;
- provide contact details regarding who to contact regarding access to and correction of the personal information;
- take reasonable steps to ensure that personal information holdings are relevant, not excessive, are accurate, up to date, complete and that the collection does not unreasonably intrude on the personal affairs of individuals;
- retain personal information for no longer than is necessary and then dispose of it lawfully and securely;
- protect personal information from loss, unauthorised access, use, modification or disclosure or other misuse;
- ensure that all reasonable steps are taken to ensure that personal information is not used or disclosed without authorisation by external service providers;
- not disclose personal information outside the University or its affiliated student bodies except where:
  - the subject of the information has consented to the disclosure, or has been notified of the likelihood of the disclosure; or
  - the University is required by legislation, court order or other legally enforceable instrument and the request is in an appropriate written form; or
  - Disclosure is reasonably believed to be necessary to prevent or lessen a serious and imminent threat to the life or health of any person.

In no other circumstances will personal information be disclosed.

### **3. Dealing with requests for personal information from outside the University**

Both the University Policy and the Act mean we cannot release personal information except in particular circumstances.

#### **3.1 Requests from the police for personal information**

Requests for information from the police must never be accepted over the telephone. Members of staff receiving requests for personal information from law enforcement agencies must direct the enquirer to the University Office of General Counsel. The decision regarding disclosure of personal information will be made by the University's Registrar in relation to students and the Pro-Vice-Chancellor (Employee Relations) for information regarding staff. The Registrar and PVC (Employee Relations) may seek advice on the matter from the Office of General Counsel.

This procedure does not apply in cases where there is an imminent threat to life or safety, however even then reasonable attempts should be made to discuss the matter with the University officers mentioned. In most other circumstances it may be assumed that the University will require the issuing of a search warrant or subpoena. Records of all requests and disclosures of personal information to the law enforcement agencies will be kept on the appropriate file maintained by Records Management Services.

#### **3.2 Requests for personal information from the Government Departments**

Departments such as Social Security (including Centrelink), Department of Immigration and Multicultural and Indigenous Affairs and Taxation sometimes have a lawful need to access personal information held by the University. Where this need exists it is recognised in the legislation which establishes the departments and regulates their functions. While the University wishes to be cooperative with the Commonwealth, it has a duty to its staff and students. Therefore, any Commonwealth Department requiring personal information should be informed that the University will supply personal information only in response to a formal notice under the Department's legislation. In any event, all such requests should be referred to the University's Privacy Officer.

Notices issued under Commonwealth Acts override any provisions of NSW legislation by virtue of s109 of the *Constitution*.

#### **3.3 Subpoenas and court orders**

The personal information held by the University is often required as evidence in court and tribunal proceedings. These may be matters which do not involve the University, or litigation to which the University is joined as a party. For all matters, the Proper Officer to be named in subpoenas and other orders is the University Registrar. Subpoenas received by the University must be directed to the University's Office of General Counsel.

### **3.4 Confirming if someone is a graduate**

Requests are often made to confirm if someone is a graduate of the University. Such requests may be answered if:

- The request is made in writing, providing full name and date of birth if possible;
- The response is also in writing;
- Only the date of graduation and degree conferred can be disclosed;
- No comment can be made regarding the subject results, academic record period of time that the student was enrolled;

The fact that someone is a graduate is publicly available information. No other information or comments may be made regarding graduates except with the consent of the graduate themselves, or in accordance with the University Privacy Policy.

Note: the University cannot confirm or deny that someone is a currently enrolled student without the consent of the student. This restriction applies, regardless of the identity of the enquirer.

## **4. Frequently asked questions**

*What is the situation regarding photographing staff or students?*

- It is common to have photographs of staff or students on identity cards that are carried or worn. It is preferable not to keep copies of such photographs. If copies are kept, they should only be used to issue replacement cards. Any other use requires the written consent of the individuals concerned.
- Photographs are often taken of staff and students for use in University publications. The definition of "personal information" in the Privacy and Personal Information Protection Act includes photographs and video. As a result, it is important that the written consent be obtained from identifiable individuals appearing in photographs (or video footage) intended for publication.
- Where security video cameras are installed there must be adequate notices that cameras are operating and who is responsible for them.

*When can I pass personal information to other members of the University's staff?*

Almost everyone in the University has access to personal information in order to do their job, it may be about students, staff or alumni. Generally the business processes make it clear who needs access to particular information. These processes are documented and understood by those carry them out on a regular basis. Occasionally staff may receive a request for access to information from a staff member or part of the University that they do not normally deal with. Some requests may be made by senior officers or

accompanied by an authorisation from a senior officer. The general rule is that it is appropriate for a University staff member to have access to the information that they need to carry out their duties. Some obvious examples of staff requiring access to information from across the entire University include audit investigations, misconduct or discipline cases that are handled by the appropriate University units.

## **5. Further information**

The University Privacy Policy and Privacy Management Plan are both available at:

[www.usyd.edu.au/arms/privacy](http://www.usyd.edu.au/arms/privacy)

*Or contact:*

**Tim Robinson,**  
Manager,  
Archives and Records Management Services  
Ext. 14263.

Or

**Anne Picot,**  
Assistant Manager,  
Archives and Records Management Services  
Ext 17262.