



The University of Sydney

**University of Sydney
Privacy Management
Plan**

Produced by Archives and Records Management Services
University of Sydney

www.usyd.edu.au/arms

Printed August 2007

© The University of Sydney 2000

University of Sydney Privacy Management Plan

Contents

	Page
1. Introduction	2
2. Privacy policy and practices	2
3. Personal Information Holdings	17
4. Communication strategy	19
5. Public Registers	20
6. Internal Review Procedures	20
7. Codes of Practice	23
8. Other relevant matters	24
9. Operational Plan	32
10. Appendices	44
11. Index	56

1. Introduction

This Plan is produced in accordance with section 33 of the NSW *Privacy and Personal Information Protection Act 1998* (the Act). It details the University's Privacy Policy and how it will be translated into the University's business practices. This Plan also explains how the University will conduct Internal Reviews in accordance with Part 5 of the Act and some other matters relevant to the protection of personal information in the University.

This plan may be amended from time to time. All amendments are to be approved by the Vice-Chancellor.

In accordance with s33(5) a copy of this plan must be provided to Privacy NSW as soon as practicable after it is completed and whenever it is amended.

2. Privacy Policy and practices

2. (1) Definition of Personal Information

Section 4 of the Act consists of the following definition of personal information:

- (1) In this Act, 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.
- (2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.
- (3) Personal information does not include any of the following:
 - (a) information about an individual who has been dead for more than 30 years,
 - (b) information about an individual that is contained in a publicly available publication,
 - (c) information about a witness who is included in a witness protection program under the Witness Protection Act 1995 or who is subject to other witness protection arrangements made under an Act,
 - (d) information about an individual arising out of a warrant issued under the Telecommunications (Interception) Act 1979 of the Commonwealth,
 - (e) Information about an individual that is contained in a protected disclosure within the meaning of the Protected Disclosures Act 1994, or that has been collected in the course of an investigation arising out of a protected disclosure,
 - (f) information about an individual arising out of, or in connection with, an authorised operation within the meaning of the Law Enforcement (Controlled Operations) Act 1997,
 - (g) information about an individual arising out of a Royal Commission or Special Commission of Inquiry,
 - (h) information about an individual arising out of a complaint made under Part 8A of the Police Service Act 1990,

- (i) information about an individual that is contained in a document of a kind referred to in clause 1 or 2 of Schedule 1 (restricted documents) to the Freedom of Information Act 1989 (ie Cabinet documents or Executive Council documents),
 - (j) information or an opinion about an individual's suitability for appointment or employment as a public sector official,
 - (k) 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.
- (5) For the purposes of this Act, personal information is held by a public sector agency if:
- (a) the agency is in possession or control of the information, or
 - (b) the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement, or
 - (c) the information is contained in a State record in respect of which the agency is responsible under the State Records Act 1998.
- (6) For the purposes of this Act, personal information is not collected by a public sector agency if the receipt of the information by the agency is unsolicited.

2.(2) Information Protection Principles

Part 2 Division 1 of the Act contains a set of information protection principles which govern the collection, use, retention, access, alteration and disclosure of personal information. The sections of the Act are:

Section 8 (IPP 1). Collection of personal information for lawful purposes

- (1) A public sector agency must not collect personal information unless:
- (a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and
 - (b) the collection of the information is reasonably necessary for that purpose.
- (2) A public sector agency must not collect personal information by any unlawful means.

Section 9 (IPP 2). Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:

- (a) the individual has authorised collection of the information from someone else, or
- (b) in the case of information relating to a person who is under the age of 16 years the information has been provided by a parent or guardian of the person.

Section 10 (IPP 3). Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

- (a) the fact that the information is being collected,
- (b) the purposes for which the information is being collected,
- (c) the intended recipients of the information,
- (d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,
- (e) the existence of any right of access to, and correction of, the information,
- (f) the name and address of the agency that is collecting the information and the agency that is to hold the information.

Section 11 (IPP 4). Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

- (a) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete, and
- (b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Section 12 (IPP 5). Retention and security of personal information

A public sector agency that holds personal information must ensure:

- (a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
- (b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and
- (c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and
- (d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

Section 13 (IPP 6). Information about personal information

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

- (a) whether the agency holds personal information, and
- (b) whether the agency holds personal information relating to that person, and
- (c) if the agency holds personal information relating to that person:
 - (i) the nature of that information, and
 - (ii) the main purposes for which the information is used, and
 - (iii) that person's entitlement to gain access to the information.

Section 14 (IPP 7). Access to personal information

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

Section 15 (IPP 8). Alteration of personal information

- (1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:
 - (a) is accurate, and
 - (b) 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.
- (2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.
- (3) If personal information is amended in accordance with this section, 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 public sector agency.

Section 16 (IPP 9). Agency must check accuracy of personal information before use

A public sector agency that holds 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.

Section 17 (IPP 10). Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

- (a) the individual to whom the information relates has consented to the use of the information for that other purpose, or

- (b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or
- (c) 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.

Section 18 (IPP 11). Limits on disclosure of personal information

- (1) A public sector agency that holds 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 public sector agency, unless:
 - (a) 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
 - (b) 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
 - (c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.
- (2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

Section 19 (IPP 12). Special restrictions on disclosure of personal information

- (1) A public sector agency 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.
- (2) A public sector agency that holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales unless:
 - (a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or
 - (b) the disclosure is permitted under a privacy code of practice.
- (3) For the purposes of subsection (2), a relevant privacy law means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.
- (4) The Privacy Commissioner is, within the year following the commencement of this section, to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales.

(5) Subsection (2) does not apply:

- (a) until after the first anniversary of the commencement of this section, or
- (b) until a code referred to in subsection (4) is made, whichever is the later.

2. (3) The University Privacy Policy

Approved By: Vice-Chancellor on 28 June 2000. Amended by Senate 6 August 2007.

Date of Effect: 29 June 2000

Contact: Manager, Archives and Records Management Services

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

In no other circumstances will personal information be disclosed.

2. (4) Application of the Information Protection Principles in the University

It should be noted that the application of the Information Protection Principles in relation to some functions within the University may be varied by Codes of Practice issued under Part 3 of the Act. For example, Privacy NSW has issued an Investigations Code of Practice.

The Act defines personal information very broadly (see the definition from s4 of the Act on page 4 of this document). Apart from the specific exemptions given in s4(3), personal information includes any information which identify, or enable the identification of, any individual. Within the University the greatest quantity of personal information will be embodied in the University's records. Staff and student records, both hardcopy and electronic, must be managed in accordance with the Act and the University's Recordkeeping Policy. Personal information may also be contained in other record formats, such as photographs, video tapes and voice mail messages.

2. (4) (a) *Section 8 - IPP 1- Collection of personal information for lawful purposes*

Personal information must only be collected for purposes related to the functions and activities of the University. These include:

- admission, enrolment, assessment, and graduation of students;
- communication with current students and graduates;
- selection, employment, appraisal, and remuneration of staff;
- teaching and research.

The personal information must only be collected by means that are permissible by law.

2. (4) (b) *Section 9 - IPP 2 - Collection of personal information directly from individuals*

Whenever possible, the University must collect personal information directly from the individual to whom the information relates. The individual may authorise the collection of information from someone else or, in the case of a person under the age of 16, it may be authorised by a parent or guardian of that person. Section 26(1) of the Act exempts the University from compliance with IPPs 2 and 3 (sections 9 and 10 of the Act) if compliance would "in the circumstances, prejudice the interests of the individual to whom the information relates."

Examples of circumstances when it is acceptable to collect personal information from other sources include:

- HSC result data from UAC;
- Examiners' reports on higher degree theses;
- Assessments of students on field work or professional experience programs.

2. (4) (c) *Section 10 – IPP 3 - Requirements when collecting personal information.*

When personal information is collected by the University, the University must clearly state:

- (i) The fact that the information is being collected.
- Forms (both hardcopy and electronic) should clearly indicate that they are an instrument for the collection of personal information and are covered by this Management Plan.
 - Where information is collected over the phone, the provider of the information must be notified that the personal information they supply about themselves is being retained.
 - When video cameras or closed circuit TV is used for security purposes there must be adequate signage or it must be clear that the camera operator is an employee of the University

(ii) the purposes for which the information is being collected,

On every occasion that personal information is collected the provider of the information must be told why the information is sought. This may be for reasons such as:

- University administrative processes such as payroll, student assessment management, to facilitate communication between the University and staff and/or students etc;
- In compliance with legislation;
- In compliance with the requirements of external government agencies, eg DETYA statistics.

(iii) the intended recipients of the information,

On every occasion that personal information is collected the provider of the information must be told who will receive the information. This will include both recipients within the University (such as Student Administration, Personnel Services, the relevant Faculty and/or Department) and external agencies (Such as DETYA, NSW Department of Health).

- (iv) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,

This is self explanatory, and such information must be supplied on every occasion that personal information is collected.

- (v) the existence of any right of access to, and correction of, the information,

Section 14 of the NSW *Privacy and Personal Information Protection Act* and section 16 of the NSW *Freedom of Information Act* provide statutory rights of access to most personal information. In addition, the University has procedures enabling staff and students to apply for access to their student and staff files outside the legislative regimes. Section 15 of the *Privacy and Personal Information Protection Act* and section 39 of the NSW *Freedom of Information Act* provide mechanisms for the amendment or correction of personal information. The University has its own administrative means for students and staff members to update or correct routine matters such as changes of address.

Again, on every occasion that personal information is collected the provider of the information must be told of their rights in relation to the correction of information.

- (vi) the name and address of the agency that is collecting the information and the agency that is to hold the information.

In most cases the University will be both the agency collecting and holding the information. This should always be clearly indicated at the time of the collection of the information. Similarly, if the University is only acting as a collecting agent this must be made clear along with the name and address of the recipient of the information.

An example of a notice to be included when collecting personal information may be found at appendix 1.

2. (4) (d) *Other requirements relating to collection of personal information*

When staff of the University are designing tools for the collection of personal information the Act requires that reasonable steps are taken to ensure that the information collected:

- Is relevant to the purpose;

- Is not excessive;
- Is up to date and complete;
- Does not unreasonably intrude into the personal affairs of the individual to whom the information relates.

2. (4) (e) *Retention and security of personal information*

All personal information held by the University must be managed in accordance with the University Recordkeeping Policy and the *NSW State Records Act 1998*.

In particular, retention and disposal of personal information must be strictly in accordance with the General Disposal Authorities and Functional Disposal Schedules approved by the NSW State Records Authority. Destruction of personal information must be carried out in accordance with *Destruction of Records - A Practical Guide* issued by the NSW State Records Authority. (<http://www.records.nsw.gov.au/publicsector/disposal/destroy/destroy.htm>)

Personal information must be protected by all security measures reasonable in the circumstances against loss, unauthorised access, modification or disclosure and against all other misuse. The appropriate measures regarding physical storage are set out in Part 6 of *AS4390 – Records Management* and in *The Standard on the Physical Storage of State Records* issued by the NSW State Records Authority. (<http://www.records.nsw.gov.au/publicsector/rk/storage/toc.htm>)

Computer systems containing personal information must be maintained in accordance with best practice relating to security from unauthorised access and use as expressed in the University's IT Security Policy. Appropriate measures include secure password protection and possibly encryption of some information.

In day to day work staff are required to ensure that hardcopy staff or student files containing personal information are kept in locked furniture when not in use. Files should not be left on desks when offices are unattended, or when people other than the normal staff are present. They should not be left where members of the public (including students) may accidentally see them.

When the University gives personal information to an external service provider (for example, the supply of names and addresses to a mailing house) part of the contract must include a clear delineation of the use to which the information may be put or disclosed. The personal information must also be

returned to the University, or destroyed in a secure manner as specified in the Confidentiality Agreement, at the end of the contract and the service provider must certify that no copies of the information have been retained by them. Appendix 2 contains a Confidentiality Agreement prepared by the University Solicitor which should be used when personal information is supplied to an external service provider.

2. (4) (f) *Information about personal information*

Individuals are entitled to know whether personal information about them is held by the University, the nature of the information, the main purposes for which it is used and their entitlements to gain access to it.

The University, in its *Statement of Affairs*, published annually in accordance with the *NSW Freedom of Information Act*, indicates the type of personal information it holds and how applications for access to it may be made.

Part 3 of this Management Plan contains information about the personal information held by the University.

2. (4) (g) *Access to personal information*

Section 14 of the Act establishes a right of access to personal information, as it is defined by the Act. It is important to note that personal information in this context does not include information or an opinion about an individual's suitability for appointment or employment as a member of the University's staff. Staff, or applicants for positions within the University, who wish to access personal information regarding their appointment or promotion should be advised to use the administrative mechanisms that exist providing feedback to applicants for appointment or promotion. If the administrative mechanisms do not satisfy the person they should be advised of their rights under the Act and the *NSW Freedom of Information Act 1989*.

Part 8 of this Management Plan contains information regarding gaining access to their University staff and student records by members of staff or students. Appendix 3 is a form to be used when the granting of access to the subject of a file through routine administrative means is not possible or appropriate. The form may also be used for applications for access to personal information by the subject of the information under the *NSW Freedom of Information Act*.

It is good practice, and contributes to the efficient operation of the University, to establish appropriate mechanisms for staff and

students to access personal information easily. Secure web interfaces are suitable for this purpose.

2. (4) (h) *Alteration of personal information*

An individual about whom the University holds personal information may request changes to that information. The University has administrative mechanisms for routine changes of personal information such as name changes, contact details etc. Students may notify the University of such changes through the Student Centre or by on-line web interfaces. Staff wanting to amend personal information should contact the relevant Personnel Service Team.

Applications for changes regarding the accuracy, relevance, currency, completeness or alleged misleading nature of personal information which are not routine matters should be referred to the Registrar.

The person to whom the information relates is entitled, if it is reasonably practicable, to have any recipients of the information notified of an amendment made by the University.

In some circumstances the University may not be prepared to make the amendment sought by the subject of the information. In such a case the individual may request that a statement of the amendment sought be attached in such a way that it can be read with the information. The University must take reasonable steps to attach the statement, which is to be supplied by the individual to whom the information relates.

2. (4) (i) *Accuracy of personal information must be checked before use*

The University must not use personal information without taking reasonable steps to ensure that the information is relevant, accurate, up to date and not misleading. The steps that are reasonable to take will depend upon the circumstances in which the information will be used. Students have the opportunity to verify personal information as a part of the enrolment process. Staff may correct or amend personal information as and when appropriate or when a Data Census is conducted by Personnel Services.

2. (4) (j) *Limits on use of personal information*

The University must only use personal information for the purpose for which it was collected. There are exceptions in some circumstances, such as:

- where the individual to whom the information relates has consented to the other use;
- where the other purpose is directly related to the purpose for which the information was collected.
- if the use is necessary to prevent or lessen a serious and imminent threat to life or health of any person.
- in relation to some investigations and law enforcement purposes.

It is relevant to note that when the University collects personal information as a part of its normal operations, the variety of internal uses it puts that personal information to are permissible under the Act¹. However, it remains important that providers of personal information are fully informed at the time of collection of the purposes for which the information will be used.

Any other use which involves the disclosure of personal information outside the University can only be carried if it is in accordance with the Act.

2. (4) (k) *Limits on disclosure of personal information*

The University must not disclose personal information to anyone or any organisation:

- Unless the disclosure is related to the purpose for which the information was collected. There must be no reason to believe that the individual concerned would object to the release of the information;
- Unless the individual concerned was reasonably likely to have been aware, or had been notified, that the personal information is usually disclosed to the person or agency;
- Unless the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of any person.

2. (4) (l) *Special restrictions on disclosure of personal information*

The Act specifically prohibits the disclosure of personal information relating to an individual's:

- Ethnic or racial origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Health;

¹ This is consistent with advice provided by Privacy NSW at the training programs for the Act.

- Sexual activities,

unless the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of any person.

There are certain exemptions related to law enforcement or investigative matters, or where the individual concerned has expressly consented to the disclosure. Disclosure may be permissible if it is required or contemplated by other legislation.

3. Personal Information Holdings

The University holds personal information on its current and former students and members of staff. In addition, the University holds deposited records which may contain personal information.

3. (1) Staff

The major series of hardcopy records relating to University staff are the Personnel Files used by Personnel Services and managed by Records Management Services. There are files on all current members of staff. In addition, the University Archives holds files on some, senior, former members of the University's staff. At the Faculty of Health Sciences Cumberland Campus Administration, and at the Faculty of Rural Management there are series of staff files of current and former staff. Other faculties, and some departments, may also hold records relating to staff

The major electronic recordkeeping application relating to University staff is the PeopleSoft Human Resources and Finance System.

In addition, the University's *Calendars*, *Faculty Handbooks* and other publications² also contain lists of the University's staff. In addition, the University's internal phone directories, both electronic and hardcopy, contains the names of staff.

3. (2) Students

The major series of hardcopy records relating to students of the University are held in the Student Files managed by Records Management Services. In addition, the University Archives holds records on former students of the University and the

² Section 4(3)(b) of the Act states that, for the purposes of the Act, personal information does not include "information about an individual that is contained in a publicly available publication."

amalgamated colleges and their predecessors. At the Faculty of Health Sciences Cumberland Campus, and at the Faculty of Rural Management there are records of current and former students.

The major electronic recordkeeping systems relating to current and former University Students are the Student Records System (SRS) and FLEXSIS. There are also electronic records at the Cumberland Campus and the Faculty of Rural Management. Many faculties and departments also hold records relating to students.

The Alumni Relations Office holds records regarding graduates of the University.

There are other, publicly available³, sources of information regarding graduates of the University:

- The University *Calendar* and *Supplements* included lists of graduates until 1970, with a special publication in 1974 of graduates and holders of diplomas.
- In addition, graduation lists, order of merit and prizes were regularly published in the past *Sydney Morning Herald*.
- *Graduation Handbooks* which list graduates at each conferring ceremony are distributed to Fisher Library, the State Library of NSW, NSW Parliamentary Library and the National Library of Australia under the deposit provisions of the NSW and Commonwealth *Copyright Acts*.

3. (3) **University Library**

The University Library has records identifying those persons entitled to use its services.

3. (4) **Donors to the University**

The University Development Office holds records relating to donors to the University, as do the various foundations within the University. A current listing of the foundations may be found in the University's *Annual Report* each year.

3. (5) **Research records**

Records created by members of the academic staff of the University conducting or supervising research may contain personal information.

³ Section 4(3)(b) of the Act states that, for the purposes of the Act, personal information does not include "information about an individual that is contained in a publicly available publication."

3. (6) **Deposited records**

Deposited records which may contain personal information may be held in the University Archives, the Macleay Museum or the University Library. Access to these records is available by contacting each office. Details of any restrictions relating to the records may be found in the relevant finding aids, guides or catalogues.

4. **Communication strategy**

4. (1) **Publications**

Hardcopy versions of the Privacy Management Plan will be produced and distributed to heads of departments (HOAs and HODS). Information regarding the existence of the Plan and the major features of the Act will be regularly incorporated into the *Bulletin Board*.

Electronic versions of the Privacy Management Plan will be made available through USYDnet. In addition, the University's Privacy Home Page will contain information regarding the Act and the implementation of the Plan.

4. (2) **Training**

Training courses will be held under the auspices of the Staff Support and Development Unit. These courses will include specific sessions on the implementation of the Management Plan.

Information sessions targeted at specific audiences within the University will be conducted by Archives and Records Management Services. Specific groups will include the senior executive staff, Heads of Departments (HOAs and HODs), particular sectors of the administration such as Personnel Services and Student Services staff. In each case the training will be tailored to the needs of the group.

Specific privacy related material will be incorporated into the training sessions and materials used in relation to the major administrative computing systems in the University such as, SRS, FLEXSIS or PeopleSoft HR and Finance.

5. **Public Registers**

5. (1) **What is a public register?**

The Act defines public registers as:

...a register of personal 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).

5. (2) **The University's public registers**

The University has no public registers.

6. **Internal Review Procedures**

6. (1) **What is an Internal Review?**

Section 53(1) of the Act allows an "aggrieved" person to apply for review of the University's conduct in relation to a privacy matter. The aggrieved person may believe that their privacy has, or might be, breached. Such a breach may relate to contravention of:

- an Information Protection Principle;
- a Code Of Practice applying to the University;
- the conditions of disclosure of information kept in a Public Register.

Complaints which do not relate to any of these 3 cannot be dealt with as an application for Internal Review under the Act. The checklist at appendix 4 should assist in identifying the precise nature of the issue.

6. (2) **How are applications for Internal Review made?**

Section 53(3) of the Act requires that applications:

- Be in writing;
- Are addressed to the Registrar of the University;
- Include a return address in Australia;
- Be lodged with the University within six months of the time the applicant first became aware of the conduct which is the subject of the application.

The form at Appendix 5 provides an example of such an application.

Section 53(3)(d) gives the University the discretion to allow an applicant a longer period than six months from the event to be reviewed to lodge their application. Except in extraordinary circumstances, the University will decline to deal with applications outside the six month limit. It is important to note that the University must investigate any application meeting the formal requirements for an internal review.

6. (3) **Who will conduct Internal Reviews?**

Where there is no conflict of interest, the University Registrar will delegate the conducting of Internal Reviews under the Act to the Director, Secretariat and Corporate Information Unit (SCIU).

If the Director, SCIU is unable to conduct the Internal Review, it may be dealt with by another Director from within the Registrar's Division. Other senior staff of the University may also be called upon to conduct Internal Reviews if warranted by the circumstances.

Section 54(3)(b) requires that the person conducting the review be a member of the staff of the University.

6. (4) **How will Internal Reviews be conducted?**

The Act does not specify how a review is to be conducted, but does require that the person dealing with the application consider any relevant material submitted by:

- The applicant;
- The Privacy Commissioner.

The Privacy Commissioner must be informed as soon as practicable that an application for Internal Review has been received by the University. The Commissioner must also be kept informed of the progress of the Review, of its outcome and any action the University proposes to take as a result of the review. The duty to keep the Privacy Commissioner informed is set out in s54 of the Act.

As well as considering any relevant material submitted by the applicant and the Privacy Commissioner, the person conducting the review should seek information from University staff, or others, with knowledge of or a connection with the subject matter of the application. In seeking relevant material, particular consideration should be given to procedure manuals, operational guidelines and awareness of the University's Privacy Policy.

A copy of the application for Internal Review should be sent to the Privacy Commissioner together with a covering letter. A draft of such a letter may be found at appendix 6.

Once the Internal Review has commenced, the Privacy Commissioner must be notified of its progress. This should be done in writing every twenty-one days. The letters should indicate what relevant material has been considered, who has been approached for statements regarding the matter under

investigation, what discussions have been held and the progress of drafting the report. In addition, reasons for any delays in conducting the review should be notified, such as the absence of relevant staff, or a difficulty in locating and retrieving relevant documents.

All documents created or acquired during the process of conducting the review must be retained on a file registered with Records Management Services. The file number must appear on all correspondence related to the review.

6. (5) Time period for conducting Internal Reviews

The Act requires that the review be conducted as soon as is reasonably practicable in the circumstances. In practice 60 days will be the maximum time to conduct a review. If it is not completed within this time the applicant has the right under s55 to apply to the NSW Administrative Decisions Tribunal for review of the matter.

6. (6) Outcome of an Internal Review

Section 53(7) sets out the possible outcome of a review. Accordingly, 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 appropriate remedial action, which may include the payment of monetary compensation to the applicant;
- Undertake that the conduct will not occur again;
- Implement administrative measures to ensure that the conduct will not occur again.

Within 14 days of completing the review the University must write to the applicant providing him/her with:

- The findings of the review and the reasons for those findings;
- The actions the University proposes to take, if any, and the reasons for those actions;
- Information regarding the right to have the findings reviewed by the NSW Administrative Decisions Tribunal.

The University must also notify the Privacy Commissioner of the findings of the review and the actions the University proposes to take, if any, in relation to the matter.

6. (7) Role of the Privacy Commissioner in the Internal Review process

Section 54 of the Act sets out the role of the NSW Privacy Commissioner in relation to reviews. It has been mentioned above that the Commissioner must be informed of the receipt of an application for review of certain conduct, and that regular progress reports must also be made. In addition, the Commissioner is entitled to make submissions to the University in relation to the application. Any submission must be considered by the University in conducting the review.

The University may, if it wishes, request the Commissioner to conduct the internal review on its behalf and to report to the University regarding the application. The Commissioner is able to charge an appropriate fee for this service and staff of Privacy NSW must be given access to the University's records (in accordance with the University's standard confidentiality agreement referred to above). The Commissioner must conduct the review in accordance with the procedures in the Act.

7. Codes of Practice

Part 3, Division 1 of the Act enables the preparation, approval and adoption of Codes of Practice. A Code of Practice under the Act is a statement of how an agency is going to depart from the Information Protection Principles, or the public register provisions of the Act. Such codes should not be confused with a usual code of conduct or practice which are statements of ethical standards.

Codes of Practice may be produced which apply solely to the University, to some functions or parts of the University, or to all universities in NSW or to the University and other agencies subject to the Act. Codes must be consistent with the basic intention of the Act, and protect the privacy rights of individuals. Codes may be prepared by the University, other agencies in NSW or the NSW Privacy Commissioner.

Draft Codes of Practice under the Act, if not produced by the Privacy Commissioner, must be developed in consultation with the Commissioner. Draft Codes have to be submitted to the responsible Minister (the Attorney General) who may take into consideration any submissions regarding the draft Code made by the Privacy Commissioner.

At the time of preparing this Privacy Management Plan no Codes of Practice had been approved by the Minister. Codes of Practice are being developed by the NSW Privacy Commissioner which will cover the University in relation to:

- Disclosure of personal information outside NSW;
- Inter-agency transfers of information;
- Investigative functions.

The University will consider the draft Code of Practice for “Access to records of public sector agencies for research purposes” prepared by Privacy NSW. It may adopt the Code, or develop its own for approval by the Minister.

The contravention of a Code of Practice may be the subject of the Review mechanisms contained in Part 5 of the Act.

8. Other relevant matters

8. (1) Annual Report

In accordance with s33(3) of the Act, the University’s *Annual Report* must include a statement regarding actions taken by the University to comply with the requirements of the Act. Statistical details must also be given of any reviews (internal or external by the Administrative Decisions Tribunal) conducted by on behalf of the University.

8. (2) Requests for personal information by members of police services or other law enforcement agencies

The University regularly receives requests for personal information from members of the NSW and Australian Police Services. The individual circumstances of the requests will determine the appropriate response.

The Act defines law enforcement agencies as being:

- the Police Service, or the police force of another State or a Territory;
- the New South Wales Crime Commission;
- the Australian Federal Police;
- the National Crime Authority;
- the Director of Public Prosecutions of New South Wales, of another State or a Territory, or of the Commonwealth;
- the Department of Corrective Services;
- the Department of Juvenile Justice.

8. (2) (a) *Provisions of the Act*

Section 18 (IPP 11) limits the disclosure of personal information outside the University. However s18(1)(c) permits the disclosure of personal information if the University “believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.”

Section 23(5) enables the University to disclose personal information to the police **if it so decides** without breaching s18 when disclosure:

- Concerns proceedings for an offence or for law enforcement purposes;
- Is related to the whereabouts of a person reported as missing to the police, and the disclosure is to be made directly to a law enforcement agency;
- Is authorised by a search warrant;
- Is reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe that an offence has been committed.

It is important to note that s23(5) – and other related sections – **do not require** the University to disclose personal information in the absence of a search warrant, subpoena or other lawful requirement. Section 23(7) provides an exemption from s19 (IPP 12) where disclosure of the information concerned is reasonably necessary for the purposes of law enforcement where there are reasonable grounds to believe that an offence has been committed.

8. (2) (b) *Procedure for dealing with requests from law enforcement agencies*

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 Solicitor. 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 University Solicitor.

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.

8. (3) **Requests for personal information from Commonwealth Government Departments**

It is not unusual for Commonwealth Government Departments to request personal information from the University. Departments such as Social Security (including Centrelink), Immigration and

Ethnic Affairs and Taxation on occasions 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*.

8. (4) **Subpoenas and similar court orders for documents**

The personal information held by the University is often required as evidence in court and tribunal proceedings. These may be matters which do not include 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 office of the University Solicitor.

8. (4) (a) *Matters to which the University is not a party*

Solicitors regularly seek personal information from the University. They should be informed that the University will not supply personal information without:

- the written consent of the subject of the information; or
- a subpoena or similar court order.

All subpoenas and similar court orders are to be directed to the University Solicitor. Records Management Services will document the matter on the appropriate files and direct subpoenas appropriately. Individual departments or officers are not to accept or deal with subpoenas or other orders.

No personal information, including confirmation that an individual is, or is not, a student or staff member of the University, is to be given over the telephone.

8. (4) (b) *Legal proceedings to which the University is joined as a party*

The University Solicitor will deal with any subpoenas, discovery orders or similar instruments related to legal proceedings involving the University. Apart from the University Solicitor and any other officer who has carriage of the matter for the

University, no other officer is permitted to disclose University records in relation to legal proceedings.

8. (5) **Staff access to personnel files**

In most cases the University will enable staff to have access to personnel files (including electronic records) concerning them without the general need for a formal application under the *NSW Freedom of Information Act 1989* or the *NSW Privacy and Personal Information Protection Act 1998*. Application to view a staff file should be made using the appropriate form available from personnel service teams. A sample of the form may be found at appendix 7.

It should be noted that access to referees reports and similar documents may require a formal application under one of the Acts mentioned above.

8. (6) **Student access to student files and related records**

In most cases the University will enable students to have access to student files (including electronic records) concerning them without the general need for a formal application under the *NSW Freedom of Information Act 1989* or the *NSW Privacy and Personal Information Protection Act 1998*. Applications to view a student file should be made using the form attached at appendix 8.

Access to student files will be administered, in the first instance, by Faculty offices.

It should be noted that access to examiners and assessors reports, and similar documents, may require a formal application under one of the Acts mentioned above.

The Academic Board has resolved⁴ that students are able to request the numerical marks for the various components of assessment (where there is more than one) which comprise the final numerical mark reported on annual examination result notices.

The Academic Board has also resolved to allow students to peruse and/or obtain a copy of their examination scripts or any other written answers to questions that they may have made. Such requests must be made within three months of the release of the examination results, but cannot be made in relation to

⁴ University of Sydney *Calendar 1999*, Admissions and Enrolment, Resolutions of the Academic Board, page 91.

examinations where the questions are used on more than one occasion.

8. (7) Dealing with applications for access to personal information under sections 14 and 15 of the Act

Section 14 of the *Privacy and Personal Information Protection Act* states:

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

Section 15:

- (1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:
 - (a) is accurate, and
 - (b) 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.
- (2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.
- (3) If personal information is amended in accordance with this section, 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 public sector agency.

The University will deal with such applications in accordance with the procedures set out in the *NSW Freedom of Information Act 1989* and the *FOI Procedures Manual* published by the Premiers Department. Conditions and limitations relating to the disclosure of personal information may be claimed by the University in accordance with s20(5) of the *Privacy and Personal Information Protection Act*. This section states:

Without limiting the generality of section 5, the provisions of the Freedom of Information Act 1989 that impose conditions or limitations (however expressed) with respect to any matter

referred to in section 13, 14 or 15 are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions were part of this Act.

In practice this will mean that applications under s14 of the Act will attract a fee in accordance with the *Freedom of Information (Fees and Charges Order) 1989*. Currently this fee is \$20⁵ for those not entitled to a reduction, or \$10 for those who are.

The form at appendix 3 enables applications to be made for personal information, by the subject of the information, under either the Act of the *Freedom of Information Act*.

Applications will be dealt with within 21 days, providing that it is not necessary to consult a third party, in which case an additional 14 days may be added to the time to process the application.

Where the University claims documents, or sections of documents, to be exempt in accordance with the conditions and limitations of the *Freedom of Information Act* the applicant will be provided with a written determination of the type set out by s28 (for access) or s45 (for amendment of records) of the *Freedom of Information Act*. Applicants aggrieved by the University's determination have the rights under Part 5 of the *Privacy and Personal Information Protection Act* for Internal Review and for review by the NSW Administrative Decisions Tribunal of the University's conduct in relation to the application.

8. (8) Tax file numbers

The collection, use and disclosure of Tax file numbers within the University is controlled by the Commonwealth *Privacy Act 1988*. The Commonwealth Privacy Commissioner has issued extensive, legally binding *Tax file number guidelines* which are available at http://www.privacy.gov.au/news/p6_4_53.doc

The *Guidelines* requirements are similar to those of the NSW *Privacy and Personal Information Protection Act*. For example, when tax file numbers are collected individuals must be informed of the legal basis for collection, that declining to quote a tax file number is not an offence and the consequences of not quoting the number.

The University must ensure that tax file numbers are protected against loss, unauthorised access, use, modification, disclosure or other misuse. The security safeguards to be put in place are to be all those reasonable in the circumstances. Access to tax

⁵ The University set its application fee for personal information at the lower figure permitted by the *Freedom of Information (Fees and Charges) Order 1989*.

file numbers should be restricted to those who need such access in order to carry out their duties.

The *Guidelines* include a list of lawful tax file number recipients. The following extract from that list is of particular relevance to the University:

Higher education institutions as listed in section 4 of the *Higher Education Funding Act 1988* authorised under subparagraph 41B(2) of that Act for the purposes of administering the Higher Education Contribution Scheme (HECS). The institutions receive tax file numbers on Payment Option Forms from students, send forms to the Tax Office, and keep a record of the tax file numbers for notification of the HECS debt to the Tax Office. Students can also lodge tax file number applications/enquiry forms with institutions and the institutions receive lists from the Tax Office with the tax file number details of such students.

Disclosure: to the Tax Office. The institutions do not disclose the file numbers to the Department of Employment, Education, Training and Youth Affairs.

The Commonwealth Privacy Commissioner's *Guidelines* should be consulted by any officer of the University whose responsibilities involve the collection, use, storage or disclosure of tax file numbers.

9. Operational Plan

IPP 1. Collection of personal information for lawful purposes

INFORMATION MANAGEMENT – Acquisition

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 1 by ensuring that the University is not collecting information other than for its own lawful purposes. Eg for superannuation schemes, or bodies such as the Union.	Records surveys, privacy audits and communication strategy.	Archives and Records Management Services.	Within existing.	Continuing.	Ensuring lawful collection of personal information continues.

IPP 2. Collection of Information directly from the individual

Activity: COMMUNITY RELATIONS – Alumni Relations

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 2 by ensuring that alumni bodies who may supply personal information to the University inform their members of this activity.	Liaison, in writing and in person, with office bearers of alumni bodies.	Director, Alumni Relations	Within existing	31 August 2000	Notification to members of alumni bodies.

Activity: STUDENT ADMINISTRATION – Admissions - UAC

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 2 by confirming that UAC is a public sector agency within the definition in s3 of the Act. ⁶	Seek confirmation	Director, Student Centre	Within existing	31 August 2000	Confirmed in writing

Activity: STUDENT ADMINISTRATION – Admissions – Foundation Studies Program

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 2 by ensuring all University forms distributed by Taylors Institute of Advanced Studies to students of the Foundation Studies Program include seeking authorisation from the individual for the information to be collected	Include provision for authorisation on all forms.	Managing Director (International)	Within existing	31 August 2000	New forms

⁶ If the UAC is subject to the Act, its data collection processes will have to be in accordance with the IPPs. UAC should disclose to its clients who will be receiving the personal information they supply – to a very large extent this is already done. Privacy NSW has expressed the view that it is reasonable to argue that where one public sector agency collects personal information in accordance with the Act and then lawfully discloses it to another public sector agency, receipt of such information by the second agency must also be legitimate.

It should also be noted that s26(1) of the Act provides an exemption from sections 9 and 10 where compliance would prejudice the interests of the individual to whom the information relates.

by TIAS.					
----------	--	--	--	--	--

IPP 3. Requirements when collecting personal information

Activity: RESEARCH(ACADEMIC) - Funding applications (University schemes)

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring funding applicants are notified of procedures to store, process and use the information provided on the application forms.	<ul style="list-style-type: none"> a. Include statement on application forms b. new forms 	Director, Research and Scholarships	Within existing	30 June 2000 1 January 2001	Label on existing forms New forms

Activity: STUDENT ADMINISTRATION - Enrolment

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring enrolling and re-enrolling students are notified of procedures to store, process and use the information provided on the enrolment forms. Include notification that name and contact data will be supplied to student organisations; academic	Include statement on enrolment forms	Director, Student Centre/Registrar/Privacy Officer	Within existing	1 June 2000	Completed

record information may be supplied to UAC and/or other universities; statistical data to DETYA					
--	--	--	--	--	--

Activity: INFORMATION MANAGEMENT – ACQUISITION - Personnel Records

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring staff are notified of procedures to store, process and use their personal information.	Include on application and forms collecting personal information	PVC Employee Relations	Within existing	30 September 2000 1 January 2001	Label on existing forms New forms
	Induction material to advise staff	Staff Support and Development Unit	Within existing	Continuing	

Activity: STUDENT ADMINISTRATION – ADMISSIONS - Telephone enquiries

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring staff notify callers requesting information that their contact details will be entered into a database for mailouts of University related matter.	Prepare standard statement to be read to callers.	Privacy Officer	Within existing	31 August 2000	Statement to be read to callers.

--	--	--	--	--	--

Activity: COMMUNITY RELATIONS – MARKETING- Surveys

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring that when conducting surveys the Institute for Teaching and Learning include statements regarding the purpose for which the information is being collected, the recipients of the information, that the supply of the information is voluntary and the existence of rights of access and correction.	Prepare standard statement to be included on all survey instruments Prepare standard statement to be read by staff conducting phone surveys.	Privacy Officer with Director, Institute for Teaching and Learning.	Within existing	31 August 2000	Statements.

Activity: PERSONNEL – SECURITY - Site Signage

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring that where CCTV cameras are installed there is appropriate signage stating that cameras are in use for security purposes,	Install signs where necessary.	University Security.	Within existing	31 August 2000	Signage.

who controls them and the tapes.					
----------------------------------	--	--	--	--	--

Activity: STUDENT ADMINISTRATION – ADMISSIONS – Foundation Studies Program

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring students of the Foundations Studies Program are notified of procedures to store, process and use the information provided on University data collection forms .	Include statement on forms.	Managing Director, International	Within existing	31 August 2000	New forms

Activity: INFORMATION MANAGEMENT - Privacy

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 3 by ensuring that University Web sites include a link to a Privacy Statement.	<ul style="list-style-type: none"> a. Re-draft existing Privacy Statement b. Include in corporate web pages 	A/PVC Information Technology/ITS/Privacy Officer	Within existing	31 August 2000	Completed Links in place.

IPP 4. Other requirements relating to collection of personal information – relevance, accuracy and currency

Activity: INFORMATION MANAGEMENT – DATA ADMINISTRATION - Personnel Records

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 4 by ensuring that personal information about staff is relevant, not excessive, up to date and accurate.	Review of Employee Data Census	Personnel Services	Within existing	30 June 2000	Completed

IPP 5. Retention and security of personal information

Activity: INFORMATION MANAGEMENT – DISPOSAL – Personal Information

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 5 by ensuring that personal information about staff and students is kept no longer than necessary and disposed of securely.	Implement all relevant State Records General Disposal Authorities.	Archives and Records Management Services	Within existing	Continuing	Timely and lawful destruction of records.
	Implement State Records <i>Destruction of Records: A Practical Guide</i>	Archives and Records Management Services	Within existing	Continuing	Procedures implemented.
	Ensure awareness and appropriate use of the Confidential Paper Disposal service.	Property Management Services	Within existing	Continuing	Appropriate use of the service.

Activity: INFORMATION MANAGEMENT – SECURITY- ACCESS – Personal Information

To comply with IPP 5 by ensuring that personal information about staff and students is protected against loss, unauthorised access, use, modification disclosure or other misuse.	Review and revise guidelines for access to and use of personnel and student files.	Archives and Records Management Services/Personnel Services/Student Administration	Within existing	31 December 2000	New guidelines.
	Include privacy notice on the cover of all hardcopy files.	Archives and Records Management Services	Within existing	Continuing When ordered	Sticker on existing files. Completed
	Review security procedures for access to FLEXSIS and PeopleSoft HRMS.	Director ITS	Within existing	30 June 2000	Revised procedure
	Review University Privacy Policy and include in Privacy Management Plan	Registrar	Within existing	30 June 2000	New policy
	Implement the Communications Strategy contained in the Privacy Management Plan.	Archives and Records Management Services.	Within existing	Continuing	Publication and training sessions.
	Design and incorporate privacy module into all training and manuals for the use of all University administrative systems (including FLEXSIS, SRS, Peoplesoft)	Privacy Officer/SSDU/ITS/system owners.	Within existing	31 December 2000	Training materials
	Add privacy notice into logon screens for all University administrative systems where necessary.	Privacy Officer/ITS/system owners	Within existing	31 December 2000	New logon screens
	Prepare privacy agreement to be signed by staff.	Privacy Officer/PVC Employee Relations	Within existing	30 August 2000	New form

	Require all new staff (academic, general and casual) to sign privacy agreements as part of the appointment process.	Personnel Services	Within existing	31 December 2000	New form signed by all new staff.
	Progressively require all existing staff (academic, general and casual) to sign privacy agreements.	Personnel Services	Within existing	Continuing	New form signed by staff.
	Establish and promulgate standards for security of all electronic systems containing personal information.	Assistant Pro-Vice-Chancellor IT	Within existing	31 December 2000	New standard
To comply with IPP 5 by ensuring that where personal information is given by the University to an external service provider that everything reasonable is done to prevent unauthorised use or disclosure. Examples – mail houses, mediators, adjudicators, data processing agencies.	Require all external providers to sign, as appropriate, form of Confidentiality Agreement attached as Appendix 2 or other agreement prepared or approved by the University solicitor.	DVCs, PVCs, HODs, HOAs.	Within existing	Continuing	Contract/Agreements used.
To comply with IPP 5 by ensuring that where personal information is given by the University to external examiners or assessors of higher degree	(a) Draft leaflet for inclusion with information sent to examiners and assessors.	Postgraduate Studies Committee/Privacy Officer	Within existing	31 December 2000	Leaflet drafted.

theses the examiner or assessor is aware of the University's Privacy Policy					
	(b) Enclose leaflet with information for examiners and assessors.	Faculty Postgraduate advisers	Within existing	Continuing	Leaflet distributed.

IPP 6. Information about personal information

Activity: INFORMATION MANAGEMENT – PRIVACY – Records – Personal Information

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 6 by making information about the University's holdings of personal information public.	Include statement regarding holdings of personal information in the Privacy Management Plan, <i>Statement of Affairs</i> and <i>Annual Report</i> .	Freedom of Information Coordinator/Privacy Officer.	Within existing	30 June 2000	Statement prepared and included.

IPP 7. Access to personal information

Activity: INFORMATION MANAGEMENT - PRIVACY – ACCESS

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 7 by ensuring mechanisms exist for students to have access to their student file.	Review existing policies regarding student access to student records.	Student Centre/ARMS	Within existing	31 August 2000	Revised procedures.
To comply with IPP 7 by ensuring mechanisms exist for staff to have access to	Review existing policies regarding staff access to staff records.	PVC Employee Relations/ARMS	Within existing	31 August 2000	Revised procedures.

their staff file.					
	Implement FOI/PPIP awareness program.	Archives and Records Management Services		Continuing	

IPP 8. Alteration of personal information

Activity: INFORMATION MANAGEMENT - PRIVACY – ACCESS – Amendment of records

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 8 by ensuring mechanisms exist for staff to apply to alter or amend their personnel files.	Review existing policies and procedures regarding correction of personal information on staff.	Personnel Services/ARMS	Within existing	31 August 2000	Revised policy
To comply with IPP 8 by ensuring mechanisms exist for students to apply to amend their student file.	Review existing policies and procedures regarding correction of personal information on students.	Student Centre/ARMS	Within existing	31 August 2000	Revised policy

IPP 9. Agency must check accuracy of personal information before use

Activity: INFORMATION MANAGEMENT – DATA MANAGEMENT - Personal Information

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 9 by ensuring students are aware of the personal information held by the University about them, and the mechanisms that exist for correction.	Enrolment forms and confirmation of enrolment notices showing details of the personal information held and requesting changes where necessary.	Director, Student Centre	Within existing	Continuing	Already comply.
To comply with IPP 9 by ensuring staff are aware of the personal information held by the University about them, and the mechanisms that exist for correction.	Conducting regular data census	Senior Manager, Personnel Services	Within existing	Continuing	Already comply.

IPP 10. Limits on use of personal information

Activity: INFORMATION MANAGEMENT – PRIVACY – Personal Information - use

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 10 by ensuring that personal information is not used except in accordance					

with the Act and as set out in the University's Privacy Management Plan.					
	Conduct Privacy Audit of major holding of personal information and identify and correct potential difficulties.	ARMS	Within existing	30 June 2000	Complete
	Ensure understanding of the Act and Privacy Management Plan through the Awareness Program	ARMS	Within existing	Continuing	Wide understanding of the Act.

IPP 11. Limits on disclosure of personal information

Activity: TEACHING-AGREEMENTS-Cross Institutional

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 11 by ensuring mechanisms exist for the exchange of personal information regarding students engaged in cross institutional study (including <i>cotutelle</i> arrangements).	Notify all students engaged in such arrangements that a condition of their mode of study includes the exchange of personal information with the other institution(s).	Archives and Records Management Services/Director Student Centre	Within existing	31 August 2000	Notice to students in such schemes.

Activity: STUDENT ADMINISTRATION-Enrolments

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To enable compliance with IPP 11 should it be necessary to release limited personal information to the major student bodies.	Working party to be established by Registrar consisting of staff from Archives and Records Management Services and Student Centre.	Registrar	Within existing	31 August 2000	Revised enrolment form.
To comply with IPP 11 by ensuring that all students are aware that the University may disclose personal information to the University Admission Centre	Include notice on enrolment form.	Director, Student Centre	Within existing	30 June 2000	Completed.

Activity: INFORMATION MANAGEMENT – Loans – Unison Borrowing Agreement

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 11 by ensuring Library users applying for authorisation as a borrower through the Unison Borrowing Agreement are aware that some personal information will be disclosed to other libraries.	Include statement on UBA authorisation application form.	University Librarian	Within existing	31 August 2000	Revised application form.

IPP 12. Special restrictions on disclosure of personal information

Activity: STUDENT ADMINISTRATION -

Objectives	Strategy	Responsibility	Resources	Timeframe	Outcome
To comply with IPP 12 by ensuring understanding of, and adherence to , the Act.	<ul style="list-style-type: none"> a. Implement Communications strategy; b. Adopt and implement relevant Codes of Practice 	<ul style="list-style-type: none"> a. Archives and Records Management Services; b. Vice-Chancellor 	Within existing	Continuing	<ul style="list-style-type: none"> a. Training and information; b. Codes adopted when relevant

Appendix 1

Sample notice to be used when collecting personal information:

By completing this form you are supplying the University of Sydney with personal information about yourself. The University need this information so that it can _____

_____ (explain what the administrative process is).

The University is required to collect this information by _____

_____.
(if appropriate, give details of the legislation or external body's requirements as appropriate).

The information you supply will be supplied to _____

_____.
(give details of recipients – the department within the University or any external bodies).

The supply of this information by you IS/IS NOT voluntary. However, should you not supply the information, or only part of it, you should be aware that

_____.
(explain consequences of not supplying all or part of the information)

You have the right to request access to and/or correct any personal information concerning you held by the University. Routine corrections, changes and enquiries etc should be directed to _____

_____.
(name of office or University officer collecting the information).

Any other requests for access may require a formal application under the NSW *Freedom of Information Act 1989* or the NSW *Privacy and Personal Information Protection Act 1998*. Please contact the University's Freedom of Information Coordinator regarding such applications.

This information is being collected by _____
(name of office)

and will be held by _____
(if not the same).

Enquiries should be directed to _____
(name and contact details of appropriate contact officer)

Appendix 2



The University of Sydney

CONFIDENTIALITY AGREEMENT

DETAILS OF THIS AGREEMENT		
Date:		
Parties	<i>Owner</i>	THE UNIVERSITY OF SYDNEY
	<i>Name and address of recipient</i>	
Description of Confidential/Personal Information		
Purpose for which Confidential/Personal Information may be used		

TERMS OF THIS AGREEMENT

1. *Obligation of confidence*

- 1.1. The Recipient:
 - 1.1.1. may use the **Confidential/Personal Information** described above only for **purpose** specified in the Schedule above;
 - 1.1.2. must not disclose to another person the Confidential/Personal Information except as permitted under clause 1.2 of this Agreement;
 - 1.1.3. must take reasonable steps to ensure Confidential/Personal Information is always kept secure; and
 - 1.1.4. must not reproduce, store or transmit the Confidential/Personal Information in any medium or format..
- 1.2. The Recipient may disclose any Confidential/Personal Information to any of its officers or employees who:
 - 1.2.1. have a need to know for the purpose described in the Schedule; and
 - 1.2.2. before disclosure, have been directed by the Recipient to observe the Recipient's obligations under clause 1.1.

Indemnity

- 1.3. The Recipient indemnifies the Owner against any claim, loss or damage the Recipient suffers arising from a non-observance of the Recipient, or any employee, contractor or agent of the Recipient, of the Recipient's obligations under this Agreement.
- 1.4. The indemnity in clause 2.1 does not apply if the Recipient is required by law to disclose the Confidential/Personal Information to a third party, provided the Recipient has first:
 - 1.4.1. notified the Owner that disclosure is required; and
 - 1.4.2. given the Owner a reasonable opportunity to take any steps that the Owner considers necessary to protect the confidentiality of the Confidential/Personal Information.

2. *Governing law*

- 2.1. The laws in force in New South Wales govern the terms of this Agreement. Each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of courts exercising jurisdiction in that state, including any courts of appeal.

SIGNING THIS AGREEMENT

University's delegate must sign here

on

insert date on which University signs

Signature

Name

Position

on behalf of **THE UNIVERSITY OF SYDNEY**

in the presence of:

Witness' signature

Witness' name

Recipient must sign here

on

insert date on which Recipient signs

Signature

Name

Position

on behalf of **[INSERT NAME]**

in the presence of:

Witness' signature

Witness' name

Appendix 3

Application for access to personal information about myself held by the University.

(NB this form is not to be used for routine access to staff or student files)

The Registrar
University of Sydney 2006

Name: _____

Australian Postal Address: _____

Post-code: _____

Telephone number(s): _____

Staff or Student Identification Number: _____

Details of Application

I request access to document(s) concerning:

I wish to apply for access under:

The NSW *Freedom of Information Act* 1989

The NSW *Privacy and Personal Information Protection Act* 1998

Form of Access

I wish to inspect the document(s) Yes No

I require a copy of the document(s) Yes No

I require access in another form Yes No

(specify; for example transcript of audio recording)

Fees and Charges

Attached is a cheque/money order/cash to the amount of \$20 (\$10 for full time students or those of limited means) to cover the application fee.

I understand that I may be required to pay processing charges in respect of this request for any time in excess of 20 processing hours and that I will be supplied with a statement of charges if appropriate.

Applicant's signature: _____

Date: _____

Appendix 4

Internal Review Checklist to be completed officer assessing application

File Number

<p>1. Is the complaint a matter which involves a possible breach of the <i>Privacy and Personal Information Protection Act</i> or a code made under the Act?</p> <p><input type="checkbox"/> yes – go to question 2</p> <p><input type="checkbox"/> no – follow the University’s normal complaint handling procedures</p>
<p>2. When was the request for review first received?</p>
<p>3. When will the 60 day period for completion of the review elapse?</p>
<p>4. Date Privacy Commissioner notified of receipt of the request and invited to make submissions?</p>
<p>5. Has the Privacy Commissioner been asked to conduct the review on behalf of the University?</p>
<p>6. Has the applicant provided the necessary information under section 53(3) of the Privacy and Personal Information Protection Act?</p>
<p>7. Nominate the IPP code section or public register provision to which the conduct relates</p>
<p>8. Is the request being dealt with by an officer who was not substantially involved in the subject matter of the request for review?</p>
<p>9. Name designation and contact number of person now dealing with the complaint</p>
<p>10. Preliminary comments by the University and/or the Privacy Commissioner in relation to the application.</p>
<p>11. What was the outcome of the review?</p>
<p>12. Date the applicant was notified of the outcome of the review the proposed action and their right to seek a review of the findings within 14 days of the review being completed?</p>

Appendix 5

Application for review of conduct under section 53 of the *Privacy and Personal Information Protection Act 1998*.

Forward to: The Registrar, University of Sydney, 2006

Your full name	Staff/student no.
Your residential address	
Your postal address (if different from your residential address)	
What is your complaint?	
When did the conduct you are complaining about occur? (be as specific as you can)	
When did you become aware of this conduct?	
What effect did the conduct have on you or another person?	
What effect could the conduct have on you or another person?	
What would you like to see the University do about the conduct?	

I understand that details of my application will be referred to the Privacy Commissioner in accordance with section 54(1) of the Privacy and Personal Information Protection Act 1998 and that the Privacy Commissioner will be kept advised of the progress of the review.

Signature of Applicant
Dated:

Appendix 6

Draft letter to Privacy Commissioner regarding receipt of application for Internal Review under s53

File number:

Date

NSW Privacy Commissioner
PO Box A2122
SYDNEY SOUTH NSW A1235

Dear Mr Puplick,

Notification in accordance with s54(1) of the NSW *Privacy and Personal Information Protection Act 1998*.

The University has received an application for Internal Review under s53 of the *Privacy and Personal Information Protection Act 1998*. A copy of the letter of application is attached.

The matter is being investigated. I shall keep you informed of the progress and outcome of the review.

Should you have any submissions regarding this matter, please send them to me at the above address.

Yours sincerely,

Registrar

Appendix 7

Application for appointment to access staff file

Appointments must be made with the relevant Personnel Service Team to view your staff file. This form should be submitted to the Personnel Service Team at least one week prior to the time of the appointment to view the file. The exact time should be negotiated with the staff in the Team.

Conditions of Access to staff files:

- ◆ I will only be able to view the file under the supervision of a member of the staff of the Personnel Service Team;
- ◆ I may be charged for copies of material held on the file;
- ◆ I may not remove, add to or annotate the file or its contents;
- ◆ Incidental material relating to other staff that may be on my file will not be made available to me;

Name: _____

Address: _____

Staff number: _____

I wish to access the staff file held on me by the University.

Signature: _____

Date: _____

Personnel Service Team use only:

Appointment date and time: _____

Staff member supervising access: _____

Date access provided: _____

This form to be placed on the applicant's staff file.

Appendix 8

Application for appointment to access student file

Appointments must be made with the relevant Faculty Office to view your student file. This form should be submitted to the Faculty Office at least one week prior to the time of the appointment to view the file. The exact time should be negotiated with the staff in the Faculty Office.

Conditions of Access to student files:

- ◆ I will only be able to view the file under the supervision of a member of the Faculty staff;
- ◆ I may be charged for copies of material held on the file;
- ◆ I may not remove, add to or annotate the file or its contents;
- ◆ Incidental material relating to other students that may be on my file will not be made available to me;

Name of student: _____

Faculty: _____

SID: _____

I wish to access the student file held on me by the University.

Signature: _____

Date: _____

Faculty use only:

Appointment date and time: _____

Staff member supervising access: _____

Date access provided: _____

This form to be placed on the applicant's student file.

11. Index

Index term ⁷	Page
Access to personal information	14-15, 28-29, 50,54,55
Accuracy of personal information	15
Alteration of personal information	15
Amendment of plan	2
Annual Report	24
Codes of practice	23-24
Collection of personal information	10-13,46
Communications strategy	19
Confidentiality agreement	47-49
Court orders	26-27
Deposited records	19
Disclosure of personal information	16-17
Donors to the University	18
Government departments, requests for personal information by	26
Information about personal information	14
Information Protection Principles (application of)	10-17
Information Protection Principles (from the Act)	5-9
Internal review	20-23, 51, 52, 53
Personal information - definition	4-5
Personal information holdings of the University	17-19
Police, requests for personal information by	24-25
Policy - University Privacy	9-10
Public registers	20
Publications	19
Research records	19
Retention of personal information	13
Security of personal information	13
Staff - personal information	17, 27,54
Students - personal information	18, 27, 55
Subpoenas	26-27
Tax file numbers	29-30
Training	19
University Archives	19
University Library	18, 19
Use of personal information	16

⁷ This index does not cover the Operational Plan.