THE UNIVERSITY OF
NEW SOUTH WALES

PRIVACY MANAGEMENT PLAN

May 2009

UNSW PRIVACY MANAGEMENT PLAN

The *Privacy and Personal Information Protection Act 1998* (NSW) ("the Privacy Act") provides for the protection of personal information collected and held by the University. It also establishes information protection principles that must be observed.

UNSW Privacy Management Plan

Section 33 of the Privacy Act requires the University to prepare and implement a privacy management plan. This UNSW Privacy Management Plan ("Privacy Plan") has been prepared to meet these requirements.

Scope

This Privacy Plan applies to:

• all employees of the University, including casual employees and:
• affiliates of the University, including:
- conjoint and visiting appointees;
- consultants and contractors;
- agency staff;
- emeriti;
- members of University committees; and
- any other person appointed or engaged by the University to perform duties or functions for the University.

This Privacy Plan has been approved by the Vice-Chancellor in May 2009.

Comments on this Privacy Plan should be forwarded to the UNSW Privacy Officer at privacy@unsw.edu.au.

PART 1: PRIVACY PROTECTION

PART 2: INTERNAL REVIEW GUIDELINE

1 INTRODUCTION

This Privacy Plan identifies how the University will comply with the information protection principles in the Privacy Act. In so far as the University holds any health information, it will comply with the Health Privacy Principles set out in the *Health Records and Information Protection Act 2000* (NSW).

The Information Protection Principles ("IPPs")

The information protection principles set out in Part 2 of the Privacy Act establish standards for collecting and dealing with personal information so as to minimise the risk of misuse of that information. The principles also allow individuals to exercise control over what happens to their own personal information.

The privacy principles address the collection (four principles), storage (four principles), use (two principles) and disclosure (two principles) of personal information.

Under section 21 of the Privacy Act, any breach of the principles by the University gives a person an automatic right to seek an internal review from the University.

Privacy Code of Practice

The Privacy Act allows the Attorney General to make a privacy code of practice which can exclude the University from the operation of one or more information protection principles in the Privacy Act. At the time of approval of this Plan there are no Privacy Codes of Practice which apply to the University.

Section 41 Directions

Under section 41 of the Privacy Act, the NSW Privacy Commissioner may make a direction to waive or modify the application of one or more of the information protection principles to public sector agencies, including the University. Public interest directions are usually temporary in nature. The currency and applicability of section 41 directions can be obtained from the Privacy NSW website.

2 DEFINITIONS

2.1 Personal Information

The Privacy Act defines personal information as "information or an opinion (including information or an opinion forming part of a data base 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". This includes an individual's name, address, student number, video recordings and photographs of an individual, body samples and electronic records. The person's identity does not have to be expressly indicated by the information, it is only necessary that it "can reasonably be ascertained from the information".

The Privacy Act excludes certain types of information from the definition of personal information. The most significant exceptions are:

- information contained in a publicly available publication
- information about an individual's suitability for public sector employment
- information about people who have been dead for more than 30 years
- a number of exceptions relating to law enforcement investigations.

2.2 Personal Information held by UNSW

Personal information is held by the University when:

- it is in possession or control of the information, or
- the information is in the possession or control of a person employed or engaged by the University in the course of such employment or engagement, or
- the information is contained in a State record for which the University is responsible under the *State Records Act 1998* (NSW).

If the personal information held by the University is unsolicited, the principles relating to collection do not apply, however, the other provisions of the Privacy Act will apply in so far as it is personal information.

2.3 Sensitive Information

The degree of sensitivity of the personal information may influence the way in which the information protection principles are applied. Many of the principles only require that "reasonable" steps be taken having regard to all the circumstances. The more sensitive the nature of the information, the higher the level of care should be used by staff when dealing with the information, particularly where disclosure to a third party is being considered.

Although all personal information should be considered sensitive, an individual may indicate that some of their information is particularly sensitive. Examples of highly sensitive information include ethnicity, union membership, sexual preference and medical conditions.

2.4 Privacy and Confidentiality

Privacy and confidentiality have different meanings.

Privacy applies only to personal information and applies irrespective of who provided it to the University. Privacy is a broader concept than confidentiality and relates to an individual's ability to control the extent to which their personal information, enabling identification, is available to others.

Confidentiality is an obligation which restricts the University from using or disclosing some information in a way which is contrary to the interests of the person or organisation which provided it in the first place. Confidentiality can be defined as a mode of managing private information, by the restriction of access to information to authorised persons, entities and processes at authorised times, in an authorised manner.

2.5 Use and Disclosure of Personal Information

The information protection principles distinguish between use and disclosure. Use refers to the treatment and handling of personal information within an organisation, particularly when this involves making decisions on the basis of the information. Disclosure refers to making personal information available to people outside the organisation, other than to the individual concerned and includes the publication of personal information.

3 INFORMATION PROTECTION PRINCIPLES

Principles 1-4 (sections 8-11 of the Privacy Act) deal with the requirements to be followed when collecting information.

3.1 Principle 1 (Section 8)—Collection 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.

Application
This principle limits the amount of personal information collected by reference to the function and purposes of the University. It creates the requirement that personal information collected by the University must be reasonably necessary for the specified purpose of the collection. Personal information can only be collected for a lawful purpose.

The objects and purpose of the University are set out in the *University of New South Wales Act 1989* (NSW). Examples of purposes for which personal information is collected include education delivery, conferring of degrees and other awards, research, funding and payments, and management of employees.

3.2 Principle 2 (Section 9)—Collection of personal information directly from the 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.

Application
This principle requires the collection of information directly from the person concerned, unless they have given consent otherwise. Parents and guardians can give consent for children under 16.

Where the information is acquired from a private or non-government agency, arrangements will need to be made for the individuals concerned to authorise its transfer to the University.

Exceptions to Section 9
Section 9 does not apply:

- if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal (section 23(2))
- where the University is investigating or otherwise handling a complaint which could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency (section 24(4))
- to information collected with lawful authorisation or permission not to comply (section 25)
- if compliance by the University would, in the circumstances, prejudice the interests of the individual to whom the information relates (section 26(1))
- Collection from other agencies: Where a disclosure by a public sector agency A to another public sector agency B, is a disclosure authorised by law by A under the Privacy Act, for example, between UNSW and other Universities then the receipt of the information by agency B is legitimate, and the collection from a source other than the individual concerned is unaffected by section 9.

3.3 Principle 3 (Section 10)—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.

Application

This principle aims to ensure that when people are asked to provide their personal information to the University, they are given enough information in order to exercise any rights that they may have under the Privacy Act.

When personal information is collected from an individual, the University has an obligation to provide information in broad terms about the collection, including the recipients of the information and purposes for which the information will be used. In most cases these requirements can be met by including the necessary information on the application form used to collect personal information or, where information is collected over a counter, by an appropriately displayed sign. When information is collected over the phone and people are asked to identify themselves, or are capable of being automatically identified, an appropriate verbal notice should be prepared or a written notice sent by way of acknowledgement of the call.

Exceptions to section 10

Section 10 does not apply to information collected:

- where the University is investigating or otherwise handling a complaint which could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency (section 24(4))
- with lawful authorisation or permission not to comply (section 25)
- if compliance by the University would, in the circumstances, prejudice the interests of the individual to whom the information relates (section 26(1))
- if the individual to whom the information relates has expressly consented to the University not complying with the principle (section 26(2)).

3.4 Principle 4 (Section 11) – 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.

Application
The University must take reasonable steps to ensure that the personal information it collects from an individual is accurate, and that the way it is collected does not unreasonably intrude on the personal affairs of the individual to whom it relates. What is reasonable to satisfy this requirement will involve a balancing of factors which vary from case to case such as:

- the purpose for which the information was collected;
- the sensitivity of the information;
- how many people will have access to the information;
- the importance of accuracy to the proposed use;
- the potential effects for the individual concerned if the information is inaccurate, out-of-date or irrelevant ;
- the opportunities to subsequently correct the data;
- the ease with which agencies can check the data.

Principles 5-8 (sections 12-15 of the Privacy Act) deal with the requirements to be followed when storing information.

3.5 Principle 5 (Section 12) – 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.

Application
This principle sets out standards for the storage of personal information once it has been collected. Section 12(d) places an obligation on the University if it transfers personal information to outside parties to ensure that this information is not used or disclosed inappropriately. It will generally apply where the University transfers personal information to an outside person or organisation for the performance of a service to the University, including consultants, information technology service providers, and external providers of accounting services.

The University will comply with the provisions of the *State Records Act* 1998 (NSW), which covers retention, storage and disposal of state records. The University will apply security safeguards in accordance with the *State Records Act* 1998 (NSW) including the following:

- data will be kept in safe custody, sufficient to prevent unauthorised access
- the data will be properly handled and preserved to prevent loss or deterioration or unauthorised destruction

- where transmission of data is required, reasonable measures will be taken to ensure its safety, integrity and confidentiality.

The level and type of security will depend respectively, on the sensitivity of the personal information and the medium in which it is stored.

In relation to section 12(d), where it is necessary for personal information to be transferred to any third party for the purpose of providing the University with a service, the University will seek wherever possible, to obtain from that party a Confidentiality Agreement to prevent unauthorised use or disclosure of that information, and to indemnify the University against any breaches of the Privacy Act or the undertaking.

3.6 Principle 6 (Section 13) – Information about personal information held by agencies

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,
(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.

Application

This principle is designed to allow people to ascertain whether the University holds personal information, and if so, whether the University holds personal information relating to them.

The Privacy Act also provides that this section should be read as if the provisions of the Freedom of Information Act 1989 (NSW) ("the FOI Act") apply, meaning the University is entitled to rely on any conditions or limitations imposed (on access or other matters) under the FOI Act.

This principle requires only that the University takes steps that are "reasonable in the circumstances" to enable people to find out if personal information is held. What is reasonable in the circumstances will depend on a number of factors including:

- the nature of the information
- the method of storing the information, and
- any other future consequences that the information may have.

The University will take reasonable steps in the circumstances to enable individuals who have submitted a written request to ascertain whether personal information is held about them. An application for information can only be made by the person to whom the personal information relates. The University reserves the right to request an individual to make an FOI application.

Exceptions to section 13

Section 13 does not apply if the University is lawfully authorised or has permission not to comply (section 25)

3.7 Principle 7 (Section 14) – Access to personal information held by agencies

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.

Application
This principle allows people a right of access to their personal information which may be held by the University. The Privacy Act also provides that section 14 should be read as if the provisions of the FOI Act apply, meaning the University is entitled to rely on any conditions or limitations imposed (on access or other matters) under that Act. These conditions and limitations should not be applied rigidly to stop people having access to information about themselves.

Individuals have a right of access to information about them held by the University. They also have a right to access their records under the FOI Act.

The University may request an individual to make an FOI application. Cases where FOI procedures for access will be more appropriate are where the structure of the FOI Act assists the University to manage a difficult or complex case. For example, cases which are:

- resource intensive, or
- complex, or
- where the request for information may impact on other persons, or identify another person, or
- where there is a clear public interest against access.

The following conditions will apply to access requested under section 14 of the Privacy Act:

- an application for information can only be made by the person to whom the personal information relates or with their authority
- access to relevant personal information will be provided as soon as practicable, and should usually be within 35 days of the date of request
- applications for access will be dealt with by appropriately qualified personnel
- charges for applications and processing of applications will be in compliance with the FOI Act.
- verification of the identity of individuals seeking access to their personal information will be required
- forms of access to personal information will correspond to those provided under the FOI Act

3.8 Principle 8 (Section 15) – Alteration to 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.

Application
This principle provides a right to either amend or to attach a statement to personal information which a person believes to be incorrect or inappropriate. In some cases, this principle will allow the University to delete information from their records system, despite requirements of the *State Records Act 1998* to the contrary (section 20(4)).

The Privacy Act sets up an alternative method of amending personal information held by the University to that which operates under the FOI Act. However, the Privacy Act does not provide any procedural requirements in relation to this. The Privacy Act also provides that section 15 should be read as if the provisions of the FOI Act apply, meaning the University is entitled to rely on any conditions or limitations imposed (on access or other matters) under the FOI Act.

Amendments to records will be done by an addendum to the record. Alterations or deletions will not ordinarily be made.

Generally, amendments can be made under existing procedures, or under the Privacy Act, and will be applied if the application relates to a minor amendment (for example, the update of an address), and amendment is timely and its accuracy can be verified. FOI procedures for amendment apply where there is an application for a significant or substantial amendment of a record of a permanent or semi-permanent nature, and where the information is available for use by the University in connection with its administrative functions (section 39 of the FOI Act).

The University will apply the following conditions to amendment of personal information under section 15 of the Privacy Act:

- an application for amendment can only be made by the person to whom the personal information relates
- applications for amendment will be dealt with in consultation with the University's FOI Officer
- the application must be in writing and should provide appropriate evidence to satisfy the FOI Officer that the proposed amendment is in fact correct and appropriate
- an application to amend relevant personal information will be dealt with within 21 days of the date of application
- verification of the identity of individuals seeking amendment of their personal information will be required
- any amendment to personal information will be done by way of an attachment to the information, so that the attachment is capable of being read with the information.

If personal information is amended under section 15 of the Privacy Act, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the University. Factors to be taken into account in deciding whether it is reasonably practicable to have recipients of information notified of amendments made under section 15 of the Privacy Act include:

- the purpose for which the information was collected
- who the recipients are
- the sensitivity of the information
- the number of people who will have access to the information

- the importance of accuracy of the information
- the potential effects to the individual if the information is inaccurate, out-of-date or irrelevant
- the ease of notifying recipients
- the cost of notifying recipients.

Principles 9-10 (sections 16-17 of the Privacy Act) deal with the requirements to be followed when using information.

3.9 Principle 9 (Section 16) – 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.

Application

This principle places an obligation on the University to try to ensure that all personal information used by the University is relevant and accurate. The University should take reasonable steps to check information before use. Factors that should be taken into account include:

- the purpose for which the information was collected
- the sensitivity of the information
- the number of people who will have access to the information
- the importance of accuracy
- the potential effects for the individual concerned if the information is inaccurate, out-of-date or irrelevant
- any opportunities to correct inaccuracies before the information is used
- the difficulty of checking the information
- the cost of checking the information.

Where the University relies on information collected by other agencies to make decisions, this principle requires that adequate standards for information exchange are introduced to ensure that the data is uniformly defined and securely and unambiguously transmitted.

3.10 Principle 10 (Section 17) – 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.

Application

This principle generally restricts use of personal information to the purpose for which the information was collected unless consent is obtained for other uses.

Where use of personal information is authorised for a purpose other than that for which the information was collected, consent should be obtained in writing, where practicable, and signed by the subject of the personal information. Evidence of informed consent may also be provided in the form of contemporaneous notes.

Exceptions to section 17
This section does not apply:

- to the University where the use is reasonably necessary for law enforcement purposes or for the protection of public revenue (section 23(4))
- to the University which is investigating or otherwise handling a complaint which could be referred or made to an investigative agency (section 24(4)
- if the University is lawfully authorised or has permission not to comply (section 25)
- to any use which relates to a disclosure to another agency under the administration of the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier (section 28(3)).

Principles 11-12 (sections 18-19 of the Privacy Act) deal with the requirements to be followed when disclosing information.

3.11 Principle 11 (Section 18) – 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.

Application
This principle makes a general rule that personal information should be disclosed only for purposes directly related to the purposes for which the information was collected, subject to the exceptions contained within the principle, and elsewhere in the Privacy Act. Refer to 3.1 of this Privacy Plan for information about purposes for which information is collected.

Exceptions to section 18
This section does not apply:

- where the disclosure is made in connection with proceedings for an offence or for law enforcement purposes (section 23(5)(a))

- where the disclosure is to a law enforcement agency to locate a person who has been reported as missing to the police (section 23(5)(b))
- where the disclosure is authorised by a subpoena, search warrant or statutory instrument (section 23(5)(c))
- where the disclosure is reasonably necessary for the protection of the public revenue (section 23(5)(d)(i))
- where the disclosure is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed (section 23(5)(d)(ii))
- to any public sector agency which is investigating or otherwise handling a complaint which could be referred or made to an investigative agency (section 24(4))
- if the University is lawfully authorised or has permission not to comply (section 25)
- where the individual expressly consents (section 26(2))
- to any disclosure to another agency under the administration of the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier (section 28(3)).

3.12 Principle 12 (Section 19) – Special restrictions on disclosure of personal information

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 NSW 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 latter.

Application

The first part of this principle deals with a number of identified categories of personal information which are subject to more stringent disclosure requirements than those which apply to other kinds of personal information under section 18. The second part of this principle places restrictions on disclosures of personal information to persons or bodies outside New South Wales.

Circumstances where section 19 applies will vary and will be a matter for professional judgment. Factors which may be taken into account include:

- who the recipients of the information are
- the sensitivity of the information
- the number of people who will have access to the information
- the potential effects on the individual
- the urgency with which the information is required
- the capacity to inform the person and seek their consent
- the seriousness and nature of any threat to life or health.

Exceptions to section 19

This section does not apply:

- if the disclosure is reasonably necessary for the purposes of law enforcement where there are reasonable grounds to believe an offence has been committed or may be committed (section 23(7))
- if the University is lawfully authorised or has permission not to comply (section 25)
- where the individual expressly consents (section 26(2))
- to any disclosure to another agency under the administration of the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier (section 28(3)).

4 UNSW PRIVACY INFORMATION GUIDELINE

A separate Guideline is being developed by the Executive Director University Services to assist staff in ensuring that personal information is collected, stored and used in accordance with information privacy protection principles. The Guideline will include recommended practices concerning personal information. The Guideline will identify some relevant privacy policies and supplement the University's other policies and procedures that affect the handling of personal information by the University, and which are disseminated through the University website.

PART 2: INTERNAL REVIEW GUIDELINE

1 INTRODUCTION

Under section 53 of the Privacy Act, individuals have the right to seek a review of certain conduct of the University, in circumstances where the individual believes that the University has breached the terms of the Privacy Act.

The request for review can only be made where it is alleged that the University has:

- breached any of the information protection principles
- breached any code made under the Privacy Act applying to the University
- disclosed personal information kept in a public register of the University.

The review shall be undertaken in accordance with the procedures set out in this Guideline.

All complaints, inquiries about information privacy, and requests for review should be treated as serious matters. If individuals are not satisfied with either the findings of the review or the action taken by the University in relation to their application for review they can make an application to the Administrative Decisions Tribunal (ADT). The ADT can make orders, including the imposition of fines up to $40,000.

2 BACKGROUND

2.1 When does this guideline apply?

Where a person makes an application for a review under section 53, the Privacy Act establishes certain requirements for how and when the application can be made, and how it should be dealt with.

Sometimes a person may raise some general concerns as to how personal information is being handled and not specify that they are requesting a review under the Privacy Act. In such cases, the University should seek to address the person's concerns by reference to existing policies and complaint handling guidelines. For example, an individual may request to have the details of his or her address revised to ensure the record is accurate. This can readily be done without referral to the internal review processes under the Privacy Act. Sometimes the person's concerns may not be able to be resolved through these mechanisms. In such cases, the University may provide the person with details of their right to an internal review under the Privacy Act, and the requirements for lodging an application for review. If the person chooses to exercise this right, the terms of this guideline will again apply.

2.2 The process for internal review

Internal review is a process whereby the University will handle complaints about how it has dealt with personal information.

This guideline:

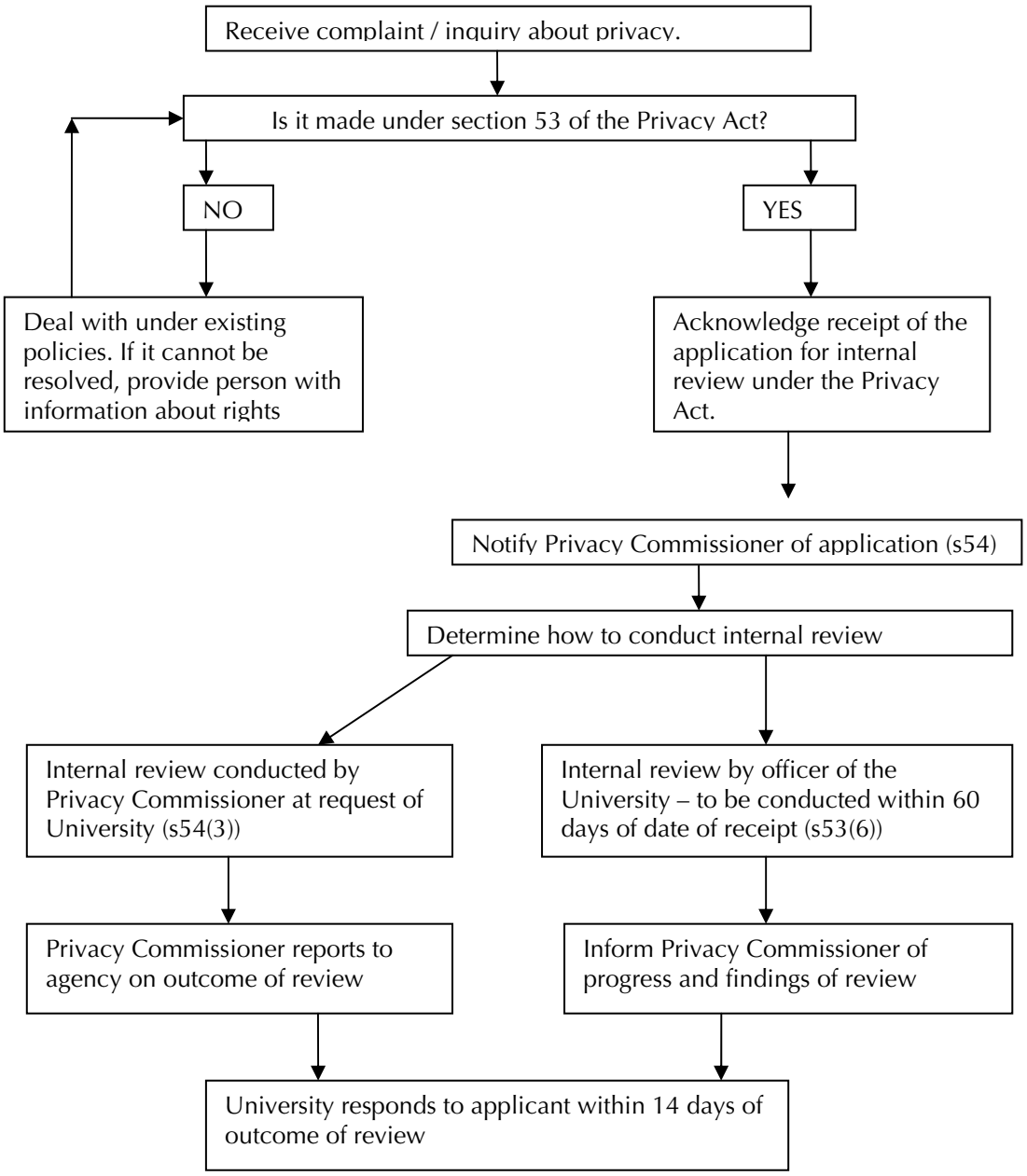
- specifies how individuals are informed about their right to internal review and how to seek a review by the ADT
- includes an application form for requesting an internal review under the Privacy Act
- indicates who will process applications, and how this will be done, including time limits
- sets requirements for recording applications and outcomes
- explains the role of the NSW Privacy Commissioner in the internal review process.

It is important that a record is kept of the progress of applications for review at each stage of the review process. The record of the internal review will be required by the

University if an application goes to the ADT.

2.3 Complaint handling and the process of internal review

Below is a diagram describing a typical complaint handling process, where the complaint concerns an alleged privacy breach or is a request for an internal review.



3 INTERNAL REVIEW PROCESS

3.1 Information about Internal Review

The University has an obligation to inform individuals of their right to request an internal review, and of their right to seek a review by the ADT. This information and information about the formal requirements for requesting an internal review shall be made available to the public via the University website and University publications.

3.2 The Application

The Application for Internal Review can be submitted by anyone who is "aggrieved" by the conduct of the University. A review can also be sought where the action taken by the University might only affect the personal information of other individuals. An application for an internal review must, under section 53 (3):

- be in writing
- be addressed to the University
- specify an address in Australia to which the applicant is to be notified after the completion of the review
- be lodged with the Privacy Officer of the University within six months from the time the applicant first became aware of the conduct to be the subject of the review.

The form to be used by individuals making an Application for Internal Review is attached.

3.3 Privacy Officer

The Privacy Officer is a senior manager responsible for ensuring the University meets its obligations under the Privacy Act, including keeping the NSW Privacy Commissioner informed of the progress of internal reviews, and of the action proposed to be taken by the agency in relation to the matter. These notifications must be in writing. The Privacy Officer keeps a record of internal review requests received and details regarding internal reviews are included in the University's annual report, in compliance with section 33(3) of the Privacy Act.

3.4 Determining whether the Privacy and Personal Information Protection Act has been breached

The Office of the NSW Privacy Commissioner advises that prior to conducting an internal review, the University must be satisfied that the complaint or application meets the criteria for an internal review. If a complaint or internal review application concerning a privacy matter is lodged at any office of the University, then this must be sent to the Privacy Officer immediately. The Privacy Officer is required to notify the NSW Privacy Commissioner of all applications for internal review as soon as practicable after receiving the application.

The Privacy Officer will determine whether the matter will be treated as a breach of an information privacy principle, a code or a public register provision. If the Privacy Officer is satisfied that the complaint or application does not meet the criteria for an internal review, then the complaint should be handled as part of the usual policies for complaint handling, with a notification required to the NSW Privacy Commissioner of action proposed to be taken in relation to the matter.

Where internal review is required, then the application will either be dealt with by the Privacy Officer or be forwarded by the Privacy Officer to an appropriate Reviewing Officer. The officer undertaking the internal review will deal with the review as far as practicable in accordance with the Privacy NSW Internal Review Checklist.

3.5 The Reviewing Officer

A Reviewing Officer is any person within the University who deals with the application under the terms of the Privacy Act. The Reviewing Officer must be, as far as is

practicable, a person who:

- was not substantially involved in any matter relating to the conduct which is the subject of the application
- is an employee or officer of the University
- is otherwise suitably qualified to deal with the matters raised by the application.

3.6 The Conduct of the Review

Upon receipt by the Reviewing Officer of an application, the Reviewing Officer must consider any relevant material submitted by the applicant and the NSW Privacy Commissioner. The Reviewing Officer should, where practicable and appropriate, give an opportunity to the applicant to provide written submissions in relation to the matter.

The Reviewing Officer should complete the review as soon as is reasonably practicable and, in any event, within 60 days from the day on which the application was received. If the review is not completed within 60 days from the day on which the application was received, the applicant is entitled to make an application to the Administrative Decisions Tribunal for a review of the conduct concerned.

3.7 Completion of the Review

The review must recommend any one or more of the following:

- take no further action on the matter
- make a formal apology to the applicant
- take appropriate remedial action (for example, the correction of a record)
- provide undertakings that the conduct will not occur again
- implement administrative measures to ensure that the conduct will not occur again.

3.8 Notification to the Applicant

Within 14 days of the completion of the review the Privacy Officer must notify the applicant in writing of:

- the findings of the review (and the reasons for those findings), and
- the action proposed to be taken by the University (and the reasons for taking that action), and
- the right of the person to have those findings and the agency's proposed action reviewed by the Administrative Decisions Tribunal.

4 THE ROLE OF THE NSW PRIVACY COMMISSIONER

The NSW Privacy Commissioner has a monitoring role during the course of an internal review. When an application for internal review is received under section 53 of the Privacy Act, the University:

- notifies the NSW Privacy Commissioner of the application as soon as practicable
- keeps the NSW Privacy Commissioner informed of the progress of the internal review
- informs the NSW Privacy Commissioner of the findings of the review and of the action proposed to be taken by the University in relation to the matter.

Under section 45 of the Privacy Act, a complaint may be made to the NSW Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual. A complaint must be made within 6 months (or such later time as the NSW Privacy Commissioner may allow) from the time the complainant first became aware of the conduct or matter that was the subject of the complaint.

Individuals are encouraged to make a complaint to the University in the first instance.

THE UNIVERSITY OF NEW SOUTH WALES

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

Details of Applicant	(Title)_____Surname_____ Given Names _____ Australian Postal Address_____ _____ Postcode _____ Telephone Number(s) _____
Details of the complaint	What is the conduct complained of? _____ _____ _____ _ When did the conduct you are complaining about occur? (Use dates if possible) _____ 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 had on you or another person? _____ _____ _____ Continue on additional sheets if not enough space
Desired outcome	What would you like to see the University do about the conduct? _____ _____ _
Application Lodgement	This Application must be addressed to The Privacy Officer, UNSW Sydney NSW 2052 Email: privacy@unsw.edu.au
Declaration	I understand that details of my application for review will be referred to the NSW Privacy Commissioner in accordance with section 54(1) of the Act and that the NSW Privacy Commissioner will be kept advised of the progress of the review. Applicant's Signature_____ Date: / /
Advice on Application	The University will complete the internal review within 60 days of receipt of the application and advise you of the findings within 14 days after completing the internal review.