

UNIVERSITY OF NEW ENGLAND**Privacy Management Plan**

- 1 Goal/Purpose
- 2 Definitions
- 3 Information Protection Principles
 - 3.1 Privacy codes of practice
 - 3.2 Public Registers
- 4 Other Legislative Requirements affecting Personal Information held by UNE.
 - 4.1 Legislation that has impact on the handling of personal information include:
 - 4.2 Internal codes concerning record and information controls .
- 5 Significant Collections of Personal Information held by the University of New England.
 - 5.1 The university is obliged to collect and record the following personal information on students:
 - Purpose of collecting the information*
 - Purpose of supplying the information to related entities*
 - Storage, security and disposal of personal information*
 - 5.2 The University is required to collect the following personal information on staff
 - Purpose of collecting the information*
 - Storage, security and disposal of personal information*
6. Compliance with the IPPs
 - 6.1 Collection – principles 1 to 4
 - 6.2 Retention and security – principle 5
 - 6.3 Notification, access and correction – principles 6 to 8.
 - 6.4 Use – principles 9 to 10
 - 6.5 Disclosure – principles 11 to 12
7. Compliance with the Public Register Provisions
8. Internal Review at The University of New England
 - 8.1 Internal review procedure
 - 8.2 Obligations of the Investigating Officer in an internal review.
9. UNE Implementation
 - 9.1 Staff Development – Privacy Management
 - 9.2 Effective Date
 - 9.3. Review

Appendix

1. Information Protection Principles
2. University Purposes for Collecting Personal Information

UNIVERSITY OF NEW ENGLAND Privacy Management Plan

1. Goal/Purpose

The *Privacy and Personal Information Protection Act 1998* applies enforceable standards on NSW public sector agencies to collect, store, use and disclose personal information. The University of New England is an agency created by the *University of New England Act 1993*. Its purpose is to pursue excellence in teaching, research and scholarship and, in so doing, serve its regional, national and international communities. The institution collects personal information about its students and staff in the course of its business and is bound to comply with the NSW legislation.

The goal of this document is to provide the University with objectives consistent with the 12 Information Protection Principles under the *Privacy and Personal Information Protection Act*, and the additional National Privacy Principles from the Privacy Amendment (Private Sector) Act 2000, which extend the State legislation.

These Principles bear a strong correlation with many of the standards already adopted in the UNE Records Management Program aiming at compliance with the *NSW State Records Act 1998* and the *NSW Freedom of Information Act 1989*.

This Plan outlines the ways in which the University intends to meet its obligations through:

- the development of policies and practices to ensure compliance by the University with the requirements of the Act,
- the dissemination of these policies and practices to persons within the University,
- the procedures that the University proposes to provide in relation to internal review (under Part 5 of the Act), and
- any other matters that are considered relevant by the University in relation to privacy and the protection of personal information held by the University.

2. Definitions

Personal information collected by the University in the conduct of its business affairs may also fall under the definition of a University Record:

A University Record is recorded information, in any form, that is created or received and maintained by an employee of the University in the course of a transaction of teaching, research or other business activity and as such has to be maintained as evidence of that activity. University records may be created in a variety of forms including, but not restricted to: paper documents, email messages, electronic documents, photographs, plans, film, sound recordings,

publications, or other textual, audio-visual or computerised electronic information.

The Privacy and Personal Information Protection Act defines personal information as:

Information or an opinion (including information or an opinion forming part of database and whether or not recorded in material form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion.

All personal information collected in the course of university business will therefore fall within the definition of a University Record. As such personal information on campus is subject to Records Management Guidelines and the Information Privacy Principles.

3. Information Protection Principles

The Privacy and Personal Information Protection Act 1998 sets out the 12 Information Protection Principles (IPPs) in sections 8–19 of the Act. A brief summary of the IPPs are listed below. A complete description of the principles stated in the Act are listed in the Appendix to this document.

Principle 1

Collection of personal information must be for a lawful purpose that is directly related to a function of the University and must be reasonably necessary.

Principle 2

Collection of personal information must be directly from the individual.

Principle 3

When collecting personal information, the University must make the individual aware of:

- the fact that the information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information
- whether the supply of information by the individual is required by law or is voluntary and any consequences for the individual if the information is not provided, and
- the existence of any right of access to, and correction of, the information.

Principle 4

The University must take reasonable steps to ensure that personal information collected is:

- relevant to the purpose of the University
- not excessive
- accurate
- up to date, and
- complete.

Principle 5

Personal information must be:

- kept for no longer than is necessary for the purposes for which the information may be lawfully used,
- disposed of securely in accordance with any University requirements for retention and disposal of personal information, and
- protected against misuse.

Principle 6

Information about personal information held by the University should be accessible so as to allow individuals to ascertain whether it relates to them and, if so:

- the nature of the information,
- the purposes for which it is used, and
- the individual's entitlement to access the information.

Principle 7

Personal information relating to an individual must be accessible to that individual without excessive delay or expense.

Principle 8

The University, on the request of an individual to whom the information relates, must amend personal information (through the correction, deletion or additions) to ensure that it is accurate, up to date, relevant, complete and not misleading.

Principle 9

The University must check the accuracy of personal information before use.

Principle 10

Personal information should not be used for purposes other than for those for which it was collected unless:

- the individual concerned consents,
- the new purpose relates to the old purpose, or
- it is used to prevent or lessen a threat to the life and health of any individual.

Principle 11

The University must not disclose personal information unless:

- it directly relates to the purpose it was collected for,
- the person to whom it relates is reasonably aware that the disclosure usually occurs, or
- it is disclosed to prevent or lessen a threat to the life and health of any individual.

Principle 12

The University must not disclose sensitive information relating to ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities except to prevent death or injury. Personal information must not be disclosed to a jurisdiction outside NSW unless it has a privacy law approved by the Privacy Commissioner.

In addition to the above principles included in the State legislation, the following National Privacy Principles(NPP), as set out in the Commonwealth legislation (Privacy Amendment (Private Sector) Act 2000), further extend the obligations upon the University and private sector agencies such as ABRI and UNEP.

NPP Principle 7

The University must not:

- adopt as its own identifier of an individual an identifier that has been assigned by another organisation, unless permission is given to do so,
- disclose an identifier assigned to an individual by a third party.

NNP Principle 8

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

NNP Principle 9

The University, operating in Australia or an external territory, may transfer personal information about an individual to someone who is in a foreign country only if:

- the recipient of the information is effectively bound to uphold the principles outlined above,
- the individual consents to the transfer,
- there is a good reason for the transfer eg. contractual arrangements.

3.1 Privacy codes of practice

Draft Codes of practice for university activities have been submitted detailing functions common to NSW Universities. Only after a code has been approved by the Privacy NSW can it be included in the Privacy management scheme. The University of New England will rely on the anticipated code of practice to cover personal information disclosures to national and international jurisdictions in relation to global Academic Links programs including staff and student exchange schemes.

3.2 Public Registers

The University of New England maintains a Register of Graduates that is published annually. This contains the name, degree awarded and year of conferral of all graduates of the institution.

4. Other Legislative Requirements affecting Personal Information held by UNE.

In addition to the Privacy and Personal Information Protection Act, The University of New England is subject to other legislation and Government policy and procedures that help to ensure privacy is protected.

4.1 Legislation that has impact on the handling of personal information include:

The *NSW State Records Act 1998*, identifies the University as a public body accountable under its provisions to provide the following:

- maintenance of full and accurate records across the records continuum;
- establishment and maintenance of a records management program as expanded in Australian Standard AS4390 Records Management;
- monitoring and reporting on the recordkeeping program to government;
- maintenance of recordkeeping systems that ensure the preservation and an appropriate access to records in all formats.

The *NSW Evidence Act 1995* stipulates the standards for accuracy, authenticity and completeness required for the production of documents as evidence in court.

The *NSW Freedom of Information Act 1989* provides guidelines for determining access to confidential information held by the institution.

The *NSW ICAC Act 1988* and the *Protected Disclosures Act 1994*, provides requirements for the reporting of corrupt conduct and protection of personal information regarding the identity of informants.

4.2 Internal codes concerning record and information controls .

4.2.1 The UNE Staff Code of Conduct states that personal and professional behaviours are achieved by maintaining adequate documentation to support decisions made. This includes maintaining the confidentiality of personal information.

- 4.2.2 The UNE Records Policy states that University records are to be created, stored, accessed, used and disposed of in accordance with the procedures consistent with the Standards of the NSW State Records Act.
- 4.2.3 The Code of Conduct for Research provides guidelines on acceptable research procedures for staff.
- 4.2.4 The Code of Conduct for Research in Research Higher Degrees provides guidelines on acceptable research procedures for students.
- 4.2.5 The UNE Professional Confidential Records Policy confirms that some university records are generated by staff consistent with professional confidential privilege in the course of affairs.

5. Significant Collections of Personal Information held by the University of New England.

The University of New England stores the majority of personal information held on its staff and students in the Management Information Systems designed for the purpose. Records providing the audit trail and authorisation for action are maintained in paper format.

These primary databases systems are:

- The Student Management Information System
- The Personnel Management and Payroll System
- The Finance Administration System
- The Corporate Recordkeeping System

These systems provide automatic download of personal information as required to subsidiary Management Information Systems required for specific business purposes on campus:

- The Library Management System
- The ID Card System
- Electronic Mail Accounts

For the purposes of conducting its business as a University and meeting the reporting requirements of the for funding under the *Federal Higher Education Funding Act 1988* as well as under reporting requirements required under both Commonwealth and State Legislation, significant levels of personal information are required.

5.1 The university is obliged to collect and record the following personal information on students:

Name	Date of Birth
Gender	Country of Citizenship
Addresses Details	Contact telephone numbers

Occupation	Details of enrolment and academic results
------------	---

Australian Aboriginal or Torres Straight Islander descent indicator
Existing educational Qualifications and results form other institutions.
Details of student assessment and course progress are also held by individual course coordinators.

The university is obliged to collect and forward to the Australian Taxation Office:

Tax File Numbers (TFN) of students

These details are entered into encrypted fields of the database and not retrievable.

The university also provides some student personal information to related entities for the conduct of their business. These are

- The University Union
- The University Sports Union
- The University Students Union
- The University Postgraduate Student Association
- The New England Conservatorium of Music

Supporting document and the audit trail are collected in paper based systems to further assist in managing specific students. These documents include student correspondence, medical certification, and complaints or grievances.

Purpose of collecting the information

The collection of personal information is essential for the University in administering student enrolment, related financial management, student welfare and student performance. Specific uses are detailed in Appendix 2.

Purpose of supplying the information to related entities

Specific subsets of personal student information are supplied to unincorporated related entities of the University. These related entities exist only to supply university students and other members with services.

Storage, security and disposal of personal information

The files holding this information are subject to strict security and are only accessible by authorised staff. The varied functional nature of the files collected about students requires that specific files are dedicated to each student only if the function is required.

Personal information held in databases is accessible only to authorised staff and can only be altered by staff with the appropriate delegation. An audit trail of every transaction exists to validate any staff action. Student records are to be disposed of in accordance with Draft *General Disposal Authority : University Records*.

5.2 The University is required to collect the following personal information on staff

Name	Date of Birth
Gender	Country of Citizenship
Addresses Details	Contact telephone numbers
Position Description	Tax File Number
Salary Records	Superannuation Details
Existing educational Qualifications	
Medical Examination Records	
Workers Compensation claims records	
Internet Access logs	

Purpose of collecting the information

The collection of personal information is essential for the University in administering human resources, financial services, office services, information technology management and staff recruitment. Specific uses are detailed in Appendix 2.

Storage, security and disposal of personal information

The files holding this information are subject to strict security and are only accessible by authorised staff. Personal information held in Management Information Systems is accessible only to authorised staff and can only be altered by the Human Resources Officer with appropriate delegation.

Personnel records are disposed of in accordance with *General Disposal Authority 3: Personnel Records*.

The university also provides services that other individuals or organisations that requires personal information for the conduct of their business. These are

- Special Users of the UNE Information Technology Services
- The University Union
- The University Sports Union
- The University Students Union
- The University Postgraduate Student Association
- New England Regional Art Museum

6. Compliance with the IPPs

6.1 Collection – principles 1 to 4

The University of New England collects all personal information directly from the individual in relation to teaching, the administration of students, the administration of staff and the conduct of associated business activities. Where personal information collected in the conduct of research may not be directly collected from the individual in some circumstances. When not collected directly from the individual, the information is collected from publicly available sources or in accordance with the Code of Conduct for Research.

Students are made aware the information is being collected by notification on the applications form and associated documentation in the UNE Handbook. The University of New England will modify the 2001 application form to advise students specifically why the information is required.

Address and contact information is collected from all inquiries regarding potential enrolment.

6.2 Retention and security – principle 5

Compliance with the security principle is being addressed by a complete survey of personal information of official record collections on campus. This includes physical location checks to ensure compliance with the Standard on Physical Storage of State Records. This program is also ensuring the application of Disposal and Retention practices in accordance with the General Records Disposal Schedules on State Records.

6.3 Notification, access and correction – principles 6 to 8

As The University of New England collects most personal information directly from the individual and the accuracy of this information is required to conduct the business of teaching, existing notification, access and correction procedures are in place. The University of New England will further alert clients of the existence of the IPP's regarding the correction of information by publishing the Privacy Management Plan on its Web site.

6.4 Use – principles 9 to 10

The University of New England does not use personal information for a purpose other than for the reason it was collected unless the individual concerned consents, the new purpose relates to the original purpose, to prevent death and illness or it is otherwise permitted under an exemption under the Act. Personal information supplied to sub-contractors is protected by contractual obligations and the insertion of dummy addresses to ensure compliance.

6.5 Disclosure – principles 11 to 12

State Records does not disclose personal information, including the ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless it is to prevent a threat to the life or health an individual, and unless otherwise exempted under the Act.

(need to include similar notes on NPPs)

7. Compliance with the Public Register Provisions

The University of New England is responsible for the public register of Graduates of the institution. The register details the student name, conferral date and details of degree awarded by the institution. The register does not contain any other personal information.

8. Internal Review at The University of New England

If an individual has a complaint about the conduct of The University of New England or a member of its staff in relation to the collection, storage, use or disclosure of personal information, a written request should be made to the Vice-Chancellor so that an internal review may be undertaken. An application for an internal review can address any breach under the Privacy and Personal Information Protection Act.

Under s. 53(3) of the Act, an application for an internal review must:

- be in writing
- be addressed to The University of New England
- specify an address in Australia to which a notice may be sent
- be lodged within six months (or such later date as the Vice-Chancellor may allow) from the time the applicant first became aware of the conduct the subject of the application, and
- comply with such other requirements as may be prescribed by the regulations to the Act.

8.1 Internal review procedure

An internal review will be managed by the Privacy Officer, who will delegate matters for investigation in the following manner:

- Academic Registrar for student matters,
- Director Human Resource Services for staff matters,
- Director, Financial Services for financial matters,
- another nominated person as appropriate.

This individual investigating the complaint shall not have any substantial involvement in the matter that is the subject of the application.

The report of the individual investigating the complaint will be reviewed by the University's Privacy Officer prior to action

The review will be completed as soon as is practicable in the circumstances and within 60 days from the day on which the application was received.

Reviews will be treated in strictest confidence. A separate file under the control of the Records Management Officer, will be created, they will contain documents received or created as part of reviews.

As a result of the review The University of New England may:

- take no further action on the matter; or
- make a formal apology to the applicant; and/or
- take such remedial action as thought appropriate; and/or
- provide undertakings that the conduct will not occur again; and/or

- implement administrative measures to ensure that the conduct will not occur again.

The University of New England is also required to:

- notify the NSW Privacy Commissioner of an application for internal review
- provide reports to the Privacy Commissioner on the progress of the internal review
- inform the Privacy Commissioner of the findings of the review and of the action to be taken by The University of New England in relation to the matter.

The University of New England reserves the right to request that the Privacy Commissioner undertake the internal review if applicable.

8.2 Obligations of the Privacy Officer in an internal review.

The Privacy Officer will acknowledge the receipt of an application and write to an applicant within 14 days after completing the review and advise the applicant of:

- the findings of the review (and the reasons for those findings)
- action proposed to be taken (and the reasons for taking that action), and
- the right of the applicant to have the findings, and The University of New England's proposed action, reviewed by the Administrative Decisions Tribunal in NSW.

9. UNE Implementation

9.1 Staff Development – Privacy Management

All staff will be notified of the Privacy Management Plan through the staff electronic newsletter (UNE-Official). The plan itself will be available to staff on the corporate intranet site.

Specific groups of staff who are responsible for the initial gathering of personal information from staff and students eg. Human resource Services, Admissions, will be required to undertake a short training program on the legislation and its implications for their work.

Staff obligations under the Privacy and Personal Information Protection Act will be included in the existing Records Management training program. The briefings will also remind them of their responsibilities under the Staff Code of Conduct.

A short Powerpoint presentation of the key elements of the policy will be developed for Web delivery. Designated staff will be required to view this and to indicate that they are aware of their responsibilities under the legislation eg. Heads of School, Deans.

This information will also be part of the induction process for new staff and will be included in the UNE Procedures Manual.

Equal Opportunity Advisers, Union officials and other key personnel who may receive enquiries or complaints from students or staff will also be given training re the legislation.

UNE staff have been previously trained in the older IPP's devised by the Federal Government. The nature of universities being State organisations funded by and reporting to the Federal Department of Training and Youth Affairs, means that a significant cross-over of federal procedures occurred in the past. Updating the knowledge of these staff will be a primary objective.

Students will be informed of the legislation through articles in student magazines and University publications eg. Updates (T&LC), UNE Handbook, Help Book.

9.2 Effective Date

The University Privacy Management Plan will come into effect immediately, upon being approved by the Vice-Chancellor in accordance with the Administrative Policy Development procedure.

9.3 Operational Plan

Details of actions to be taken to implement this plan are shown in Appendix 3.

9.4 Review

This policy is to be reviewed at least on an annual basis to reflect changes in legislation, technologies, programs and resources available to the University.

APPENDIX 1

Information Protection Principles

(Part 2, Division 1, *Privacy and Personal Information Protection Act 1998*)

8. 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.

9. 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.

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.

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.

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.

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, 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.

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.

15. 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.

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 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.

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.

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.

19. 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 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.

APPENDIX 2

University Purposes for Collecting Personal Information

Staff records are collected and created for:

- recruitment purposes
- payroll purposes
- leave purposes
- superannuation purposes
- to assess staff promotions
- to record academic performance
- to record job performance
- to determine the eligibility of staff as electors or candidates for office within the University
- for other lawful purposes identified from time to time so as to fulfil accountability standards and promote the educational, cultural, social and community related activities of the University

Student records are collected and created:

- to identify students who are eligible to attend courses;
- to record students' academic performances and grades and determine the conferral of degrees, diplomas and certificates;
- to determine student eligibility for grants, awards, prizes;
- to determine the eligibility of students as electors or candidates for office within the University;
- to record financial obligations which students have to the University and designated affiliated bodies;
- for other lawful purposes identified from time to time so as to fulfil accountability standards and promote the educational, cultural, social and sporting activities of the University and designated affiliated bodies.

APPENDIX 3

Operational Plan

IPP 1 Collection of personal information for lawful purposes

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure that the University is not collecting information other than for lawful purposes eg. for super schemes or bodies such as the Union	Records surveys, privacy audits and communication strategy	Manager RMO		audit of information collected is proceeding;

IPP 2 Collection of information directly from the individual

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure that alumni bodies who may supply personal information to the University inform their members of this activity	Liaise, in writing and in person, with office bearers of alumni bodies	Director, Development Office		Notices included by Development Office where personal data is being collected.
Confirm that UAC and QTAC applications include personal information collection statement	Seek confirmation	Academic Registrar		UAC application form checked and appropriate notice is included in the terms signed by the applicant.
Ensure all University forms distributed by Shafston College, Blue Mts Hotel Mangt etc. include authorisation for the information to be collected	Include provision for authorisation on all forms	Academic Registrar		Letter sent to A/Registrars and I/national Office requesting them to review arrangements with third parties (17/1/02).

IPP 3 Requirements when collecting personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
<p>Ensure that enrolling and re-enrolling students are notified of procedures to store, process and use the information provided on the enrolment forms, or in a notice early in 2002 if already enrolled.</p> <p>Include notification that academic record information may be supplied to UAC/QTAC and other universities; statistical data to DETYA</p>	<p>Include statement on enrolment forms</p>	<p>Academic Registrar</p>		<p>Written notice being mailed with Undergraduate External Admission forms. Similar notice on web.</p>
<p>Ensure staff are notified of procedures to store, process and use their personal information</p>	<p>a) Include on application and forms collecting information b) Induction material to advise staff</p>	<p>Director, Human Resource Services</p>		
<p>Ensure that staff notify callers requesting information that their contact details will be entered into a database for mail outs of University related matters</p>	<p>Prepare standard statement to be read to callers</p>	<p>Academic Registrar</p>		
<p>Ensure that collection procedures for SEU and SET surveys do not allow respondents to be 'identified'</p> <p>Ensure that CEQ and GDS questionnaires include or are accompanied by a notice informing respondents that personal information</p>	<p>a) Amend current collection procedures for external student surveys and amend information notice in teaching material . b) Amend survey covering</p>	<p>Director, Teaching and Learning Centre Planning and</p>		<p>Revised letter drafted.</p>

is being collected	letter	Institutional Research		
Ensure international students and students of the Language Training Centre are notified of procedures to store, process and use the information provided on University data collection forms	Include statements on forms	Manager, IO, Director, LTC		LTC and I/national Office both have included notice re personal info in the conditions provided when students receive letter of offer.
Ensure that University Web sites include a link to a Privacy Statement.	a) Draft privacy Statement b) Include on UNE Web pages	Director, Mkting and Public Affairs		Link to UNE Privacy Statement provided on UNE Home Page

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

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure that personal information about staff is relevant, not excessive, up to date and accurate	Review data sets held on staff	Director, Human Resource Services		

IPP 5 Retention and security of personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure 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	Manager, RMO		

Ensure that personal information about staff and students is protected against loss, unauthorised access, use, modification disclosure of other misuse	Review and revise guidelines for access to and use of personnel and student files	RMO, Academic Registrar, Director, Human Resource Services		
	Review security procedures for access to electronic systems eg. Banner Student	Chief Information Technology Officer		
	Design and incorporate privacy module into all training and manuals for use of all University admin systems	Manager, ODU		
	Add privacy notice into logon screens for all University admin systems where necessary	System owners		
	Prepare privacy agreement to be signed by all staff	Director, Human Resource Services		
	Require all new staff (academic, general and casual) to sign privacy agreements as part of the appointment process	Director, Human Resource Services		
	Progressively require all existing staff (academic, general and casual) to sign privacy agreements	Director, Human Resource Services		
	Establish and promulgate standards for security of all electronic systems containing	Chief Info Technology Officer		

	personal information			
Ensure 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, partner education service providers	Require all external providers to sign, as appropriate, form of Confidentiality Agreement	Exec. Director (Business & Admin); A/Registrars; Manager, IO		
Ensure that where personal information is given by the University to external examiners or assessors of higher degree theses the examiner or assessor is aware of the University's Privacy Policy	a) Draft leaflet for inclusion with information sent to examiners and assessors b) enclose leaflet with information for examiners and assessors	PVC, (I & R) Research Services		

IPP 6 Information about personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
Make public information about the University's holdings of personal information.	Include statement regarding holdings of personal information in the University Handbook and Annual Report	Director, Mkting and Public Affairs	Feb 2002	Statement to appear in 2001 Annual Report

IPP 7 Access to personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure mechanisms exist for students to have access to their student file	a) Review existing policies regarding student access to student records b) Develop a schedule of staff whom students should contact to access their personal information	PVC (Academic)		
Ensure mechanisms exist for staff to have access to their staff file	a) Review existing policies regarding staff access to staff records b) Develop a schedule of staff whom staff should contact to access their personal information	Director, Human Resource Services		
	Implement FOI awareness program	RMO/ODU		

IPP 8 Alteration of personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure mechanisms exist for staff to apply to alter or amend their personal files	Review existing policies and procedures regarding correction of personal information on staff	Director, Human Resource Services		procedures informally in place, yet to be documented
Ensure mechanisms exist for students to apply to alter or amend their personal files	Review existing policies and procedures regarding correction of personal information on students	PVC (Academic)		Staff aware of requirement, procedures awaiting documentation

IPP 9 University must check accuracy of personal information before use

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure students are aware of 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	Academic Registrar		Article provided to TLC for inclusion in Updates (newsletter to all external students)
Ensure staff are aware of personal information held by the University about them, and the mechanisms that exist for correction		Director, Human Resource Services		

IPP 10 Limits on use of personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure 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 holdings of personal information and identify and correct potential difficulties	Privacy Officer		
	Ensure understanding of the Act and Privacy Management Plan through awareness program	RMO/ODU		Powerpoint information presentation available on Web (Privacy pages)

IPP 11 Limits on disclosure of personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
Ensure mechanisms exist for the exchange of personal information regarding students engaged in cross institutional study	Notify all students engaged in such arrangements that a condition of their mode of study includes the exchange of personal information with the other institutions	PVC (I & R)		International Office requested to review this area.
Ensure mechanisms exist for the exchange of limited personal information to the major student bodies	Establish working party to determine process	PVC (Academic)		
Ensure that all students are aware that the University may disclose personal information to the University Admission Centre	Include notice on enrolment form	PVC (Academic)		
Ensure Library users applying for authorisation as a borrower through the reciprocal rights scheme are aware that some personal information will be disclosed to other libraries	Include statement on application form	University Librarian		Notice included on form.

IPP 12 Special restrictions on disclosure of personal information

Objectives	Strategy	Responsibility	Timeframe	Outcome
------------	----------	----------------	-----------	---------

<p>Ensure understanding of and adherence to, the Act</p>	<p>a) Implement awareness program</p> <p>b) Adopt and implement relevant Codes of Practice</p>	<p>a) Privacy Officer</p> <p>b) VC</p>	<p>a) - Powerpoint presentation available on Web. - Info session conducted for Reference Group staff (18/12/01)</p> <p>b) Privacy policy 28 November, 2001. Implementation Guidelines and Procedures detailed on Privacy Web site.</p>
--	--	--	--