DIVISION OF THE VICE-PRESIDENT (SERVICES AND RESOURCES)

THE UNIVERSITY OF ADELAIDE AUSTRALIA

PRIVACY MANAGEMENT PLAN FOR PERSONAL INFORMATION

The Privacy Management Plan for Personal Information applies the principles of the University Privacy Policy to the management of personal information in the University. It provides clarification on the practical application of the Policy, including guidelines on applying the Policy to inquiries.

PRIVACY MANAGEMENT PLAN FOR PERSONAL INFORMATION

The University's Privacy Management Plan for Personal Information has been developed in accordance with the University's Privacy Policy and applies to personal information on prospective, current and former students, current and former staff and associates of the University and should be read in conjunction with the University's Privacy Policy.

The Vice-President (Services and Resources) is responsible for the maintenance of the Privacy Policy and the Privacy Management Plan for Personal Information.

1. MANNER AND PURPOSE OF PERSONAL INFORMATION COLLECTION

Personal information pertaining to students and prospective students is required to administer academic program advice, applications, enrolment, academic progress and scholarship selection, and to provide services to students.

Personal information pertaining to staff is required for the selection, appointment, review, promotion and general administration and to provide services to staff.

Personal information is collected to meet the wider functional needs of the University including financial management, legal accountability, and national reporting requirements. Information may also be collected to facilitate communication between the University and students or staff and to meet the requirements of legislative or external government agencies.

1.1 Classes of personal information collected and held by the University

1.1.1 Staff information

The University's major hard copy records relating to University employees are the staff files used by Human Resources and managed by the Records Management Office (RMO). There are files on all current members of staff. The University Archives holds files on some former members of the University's staff. Faculties and departments may also hold records relating to staff members. The University creates files on people holding unpaid positions such as titleholders and visitors. There are also records of current and former staff of institutions with which the University has amalgamated, including the Roseworthy Agricultural College and the South Australian College of Advanced Education (and its predecessor bodies).

The major electronic record-keeping systems relating to current and former University staff are the Human Resources system and the PeopleSoft Campus Community module.

The Alumni Association holds records relating to current and former staff members who have registered with the Alumni.

There are publicly available sources of information regarding current and former staff members that are not subject to the University's Privacy Policy including:

(a) University *Calendars*;

(b) Handbooks and other publications (including web published documents); and
(c) the University's internal telephone directories.

1.1.2 Student information

The University holds extensive hard copy records relating to students of Adelaide University in the form of student files and student cards that are managed by the Student Services Branch of the Division of the Deputy Vice-Chancellor and Vice-President (Academic). In addition, the University Archives maintains records of former students of the University. There are also records of former students of institutions with which the University has amalgamated including the Roseworthy Agricultural College and the South Australian College of Advanced Education (and its predecessor bodies). At the Roseworthy and Waite Campuses there are records of current and former students. Faculties and departments may also hold records relating to students.

The major electronic record-keeping systems relating to current and former University students are the Student Information System (SIS), to be discontinued in 2001, the PeopleSoft Campus Community module and the TRIM records management system maintained by the RMO.

The Alumni Association holds records relating to graduates of the University.

There are publicly available sources of information regarding graduates of the University that are not subject to the University's Privacy Policy including:

(a) the University *Calendar* which included a list of present and former graduates until 1979. The *Calendar* also published pass lists of students up to 1948. From 1949-1950 the *Calendar* contained only pass list results of Honours Examinations before the practise ceased altogether;

(b) *Graduates and Diploma Holders of the University to July 1979* provides a list of graduates 1874-July 1979 (with some omissions); and

(c) *Commemoration Programs*, which list the graduates at each graduation ceremony, are deposited with the Barr Smith Library, the State Library of South Australia and National Library of Australia.

1.1.3 Other records

Barr Smith Library clients

The Adelaide University libraries have records identifying those persons entitled to use their services.

Research records

Records created by the University's academic staff and students may contain personal information in some instances.

Deposited records

Records that have been deposited with Special Collections in the Barr Smith Library, University Archives or elsewhere within the University, may contain personal information. Access restrictions pertaining to particular deposits are documented in the relevant finding aids or catalogues.

Event and publicity mailing lists

The University maintains VIP and publicity mailing lists containing names and contact details of people not employed or engaged by the University.

1.2 Implementation

1.2.1 Student enrolments

There is an enrolment declaration on all enrolment forms informing students how the personal information supplied will be used, and outlining the circumstances under which it might be disclosed. All students must sign the declaration and consent to the release of personal information before their enrolment is finalised.
[Responsibility: Student Services Branch]

1.2.2 Staff records

All new staff must be notified of procedures to store, process and use their personal information through the inclusion of the University Privacy Policy and Privacy Management Plan for Personal Information in their induction package.
[Responsibility: Human Resources]

All continuing staff must be notified of procedures to store, process and use their personal information through the distribution of the University Privacy Policy and Privacy Management Plan for Personal Information by their senior manager.
[Responsibility: Student Services Policy Branch, Executive Deans, Managers]

1.2.3 Community relations

All prospective students and community members who request that information be posted to them must be informed if their personal details are entered into a prospective students database and retained for future reference. The caller should be advised that their personal details may be added to a University mailing list accessed by authorised members of University staff for purposes related to the original query.
[Responsibility: Student Information and Services, International Student Centre, Graduate Studies, academic areas entering prospect data]

The University website disclaimer includes a statement informing prospective student visitors to the site that personal information provided by them via the website will be entered into a prospective students' database and retained for future reference. It makes clear that their personal details may be added to a University mailing list and accessed by authorised members of University staff for purposes related to the original query, but that personal details will not be collected indirectly through the site's technology.
[Responsibility: Student Information and Services, International Student Centre, Graduate Studies, academic areas entering prospect data]

1.2.4 Accuracy of personal information

The accuracy of personal information will be maintained by ensuring that it is collected from the student or staff member concerned (or authorised proxy) and in cases where the information collected is not consistent with existing information, a routine check will be undertaken.
[Responsibility: Student Centre, International Student Centre, Graduate Studies, Student Administrative Services, academic areas, Human Resources]

1.2.5 Promoting the University Privacy Policy

The University website will include a link to the University Privacy Policy.
[Responsibility: Media, Marketing and Publications]

2. SOLICITATION OF PERSONAL INFORMATION

When collecting personal information, University staff should ensure that the information collected:

(a) is relevant to the purpose
(b) is not excessive
(c) is as up to date and complete as possible
(d) does not unreasonably intrude into the personal affairs of the individual concerned.

The University's preferred source of personal information is the individual concerned. However there is a range of other sources of personal information, which may include the following:

For student personal information:

(a) schools, the South Australian Tertiary Admissions Centre (SATAC), its successors and equivalent interstate and overseas bodies; and
(b) other tertiary institutions.

For staff personal information:

(a) previous employers and referees nominated by prospective and current staff members;
(b) academic assessors;
(c) external and internal medical and rehabilitation documentation; and
(d) promotion and performance review assessments.

2.1 Implementation

2.1.1 Proxies

Personal information about a staff member or a student can only be collected from the proxy when the person acting in that role can present a signed authority from the student or staff member. The proxy will have to establish their own identity and may be asked to present photo identification of him or herself at the time of presenting the authorisation.
[Responsibility: Student Centre, Human Resources and academic areas]

3. STORAGE AND SECURITY OF PERSONAL INFORMATION

Personal information must be protected by all reasonable security measures against loss, unauthorised access, modification or disclosure, and other misuse. Electronic record-keeping systems must be maintained in accordance with best practice relating to security against unauthorised access and use, and in accordance with University IT security policies and procedures. Hardcopy staff and student files should be kept in locked furniture when not in use and protected from deliberate or accidental viewing by members of the public, students, or staff whose duties do not require them to have access.

Retention and disposal of personal information must be in accordance with University functional disposal schedules, which are themselves prepared in accordance with the *State Records Act 1997* and approved *General Disposal Authorities*.

3.1 Implementation

3.1.1 Disposal and destruction of records containing personal information

The University has a *Disposal Authority for Student Personal Information* and a *Disposal Authority for Staff Personal Information* prepared in accordance with the *State Records Act 1997*. These authorities provide guidelines for the lawful and timely destruction of personal information, and are available on the University website.
[Responsibility: Records and Archives Services and Student Administrative Services]

3.1.2 Logon screens

A privacy notice appears on the logon screens of the SIS and the Campus Community module of PeopleSoft to remind staff of their obligations with regard to student and staff personal information.
[Responsibility: Information Technology Services]

3.1.3 External service providers

When the University provides personal information to an external service provider (eg. mailing or distribution service) the contract of service must expressly state the use to be made of the information and that no other use whatsoever may be made of it. The contract should make provision for the information's confidential destruction or its return to the University at the conclusion of the contract. The service provider must certify in writing that no copies of the information have been made or retained by them other than with the written consent of the University.

[Responsibility: Division of Vice-President (Services and Resources) and any area contracting an external service provider]

4. ACCESS TO OWN RECORDS

4.1 Student access to student files

Subject to clause 4.4, the University will enable students to have access to their own student files (including electronic records).

4.2 Staff access to staff files

Subject to clause 4.4, the University will enable staff to have access to their own staff files (including electronic records).

4.3 Correction of personal information

An individual about whom the University holds personal information may request changes to that information. The University has administrative mechanisms for routine changes to personal information such as change of name and address. Applications for changes regarding the accuracy, relevancy, currency, completeness or alleged misleading nature of personal information should be referred to the relevant senior manager. In circumstances where the University is not prepared to make a requested amendment, a statement of the requested amendment may be attached to the student file or marked on the electronic student record as appropriate.

4.4 Limitations on access to personal information

The University will not enable individuals to see the personal information pertaining to them which is held by the University where the University deems:

(a) it would pose an imminent threat to life or health of any individual; or
(b) it would affect the privacy of another individual or individuals; or
(c) the request is frivolous or vexatious; or
(d) there are legal proceedings between the University and the individual concerned and the information would not be accessible by the process of discovery in those proceedings; or
(e) access would reveal the intentions of the University in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
(f) the University acts according to any law restricting the provision of information to the individual or where it would be against a law to provide the information to the individual;
(g) access would be likely to prejudice an investigation of possible unlawful activity; or
(h) access could prejudice or be likely to prejudice the prevention, detection, investigation, prosecution or punishment of criminal activity, or where there is any reasonably held suspicion of illegal or improper conduct.

4.5 Implementation

4.5.1 Student access

Students can make an appointment with the Manager, Administrative Services Branch, to view their student file in the presence of the Manager.
[Responsibility: Student Administrative Services]

4.5.2 Staff access

Staff can apply in writing to make an appointment with a staff member from Human Resources to view their staff file in the presence of an authorised staff member. Confidential referees reports may be removed from the file before it is made available, to protect the privacy of the referee in accordance with provision 4.4 above.
[Responsibility: Human Resources]

4.5.3 Correction of personal information

Students have the opportunity to correct personal information during the enrolment and re-enrolment process. They will be advised through the Student Guide and Timetable, or other appropriate publication, that they can apply to the Student Centre to make changes to their personal details, and make changes to their address on-line at other times.

Students requesting by telephone that staff change their personal details will need to establish identity by providing their name, student number, date of birth and PIN. None of these details will be released over the telephone, and staff will not make changes to personal information unless the student provides all the required details of identity.

If a staff member experiences difficulty communicating with a student over the telephone and is unable to establish identity or to ascertain the student's request, the staff member will not action the change but will request that the student attend the Student Centre in person to speak to a staff member or complete a change of personal details form.
[Responsibility: Student Centre, International Student Centre, Graduate Studies, Student Information and Services and academic areas]

Staff will be advised through their induction package that they may apply to make changes to their personal details through Human Resources. Staff members requesting by telephone that staff of Human Resources change their personal details will need to establish identity by providing their name, staff ID number and date of birth. None of these details will be released over the telephone, and staff will not make changes to personal information unless the staff member requesting the changes provides all the required details of identity.
[Responsibility: Human Resources]

5. USE AND DISCLOSURE OF PERSONAL INFORMATION

Personal information collected and held by the University will only be accessed and used by people employed or engaged by the University as required in the fulfilment of their duties and in a manner consistent with the original purpose stated at the time of collection. Information on staff and students may be disclosed in the following instances:

(a) with the individual's written consent; or
(b) to reduce or avoid a threat to an individual's life, health or safety or a serious threat to public health and safety; or
(c) when the use or disclosure is required or is specifically authorised by law; or
(d) if the individual is reasonably suspected of being engaged in current or past unlawful activity, and the personal information is disclosed as a necessary part of the investigation or reporting the matter; or

(e) as required by law to government departments and statutory bodies including the Department of Immigration and Multicultural Affairs, Department of Education, Training and Youth Affairs, Australian Tax Office, Centrelink and the Medical Board of South Australia.

In addition, the University may release students' personal information in the following instances:

(a) factual data (name, address, etc.) and financial standing information to the Adelaide University Union to enable the Union to manage its membership;
(b) academic progress information to another tertiary institution or related body as required in the course of a student's transfer to a new institution; and
(c) personal and enrolment information, including academic results, of students undertaking cross-institutional study to the relevant institution as required to confirm the student's enrolment or qualification.

5.1 Implementation

5.1.1 Disclosing student personal information on the telephone and in person

University staff will only disclose or discuss personal information with a student in person on the provision of photo identification or student number and PIN to establish identity. Staff will only reveal or discuss personal information with a student over the telephone on provision of student number and PIN. Personal or academic information will not be disclosed or discussed with any third party (including relatives) without written authority from the student.
[Responsibility: Student Centre, International Student Centre, Graduate Studies, and academic areas]

5.1.2 Disclosing staff personal information on the telephone and in person

Human Resources staff will only disclose or discuss personal information with staff in person on the provision of photo identification to establish identity. Staff will only reveal or discuss personal information with staff over the telephone on provision of staff ID number and date of birth. Personal information will not be disclosed or discussed with any third party (including relatives) without written authority from the staff member.
[Responsibility: Human Resources]

5.2 APPLICATION OF THE PRIVACY POLICY TO QUERIES

If a staff member receives a request for information and is unsure whether it should be provided, they should advise that legislation and policy restrict the disclosure of personal information and that they will seek advice and provide the enquirer with correct information as soon as possible. The staff member should consult their line manager initially and, if the situation is still unclear, consult the Manager, Records and Archives Services.

If any person making an inquiry should become angry or abusive when advised that personal information will not be disclosed, the staff member should refer the query to their line manager for resolution. If support is not available, the staff member should ensure they have provided a complete answer to the query and then politely inform the enquirer that they are terminating the conversation.

5.2.1 Examples of queries where information SHOULD NOT be released

(a) *Parents*
A parent telephones the University and asks to be informed of the results attained by their son or daughter. The parent argues that they pay the HECS and therefore have a right to know if academic progress is being made.

The parent must be advised that their payment of the HECS is a private arrangement between themselves and their son or daughter. The enrolment and results are between the student and the University. The University Privacy Policy and legislation prevents University staff from releasing that information to any third party. The parent should be advised to approach their son or daughter directly to discuss their academic progress.

(b) *Students*
(i) A student of the University advises that they need to contact a friend urgently and ask to be provided with the student's home telephone number.

The student must be advised that all students provide their personal details for access by University staff for purposes directly related to their study only, and that the University Privacy Policy and legislation prevents the University releasing telephone numbers to safeguard student privacy. The staff member can inform the student of the formula for student e-mail addresses and suggest that option for communication.

(ii) A student telephones to check whether their amendment to enrolment has been processed and asks to be advised by telephone of their current enrolment. The student cannot provide their student number.

The student must be advised that the student number is essential to establishing identity. To safeguard student privacy personal information will not be disclosed or discussed without provision of the student number.

(c) *Police*
The police telephone and advise that they are investigating a student and ask to be provided with the student's home address.

The police are to be advised that all requests for student personal information must be directed to the Deputy Vice-Chancellor and Vice-President (Academic). The staff member can offer to put the police through to the Deputy Vice-Chancellor and Vice-President (Academic) but should advise that all requests for information must be in writing and that without provision of a sealed subpoena, warrant or other legal order for the information, the personal details cannot be released. (This is subject to the University's considerations at clause 5.)

(d) *Government Departments*
(i) A staff member from a government department or agency authorised by legislation to access student personal information telephones and requests confirmation of a student's enrolment status.

The person must be informed that personal information will not be provided in response to a telephone request, and that the University will only supply personal information in response to a formal notice under the Department's legislation.

(ii) A staff member from the Department of Immigration and Multicultural Affairs telephones a member of academic staff and requests information on the attendance status of an international student.

The academic should advise the inquirer that all requests for information from that Department should be made in writing to the International Student Centre.

(e) *Employers*
(i) An employer telephones asking for the date of birth and results of a student who has applied for a position with their company.

The employer must be informed that the University has a legal obligation to protect the privacy of student personal information and will not release it to any third party without the written permission of the student. The employer should be advised to contact the applicant directly to solicit the information required.

(ii) An employer telephones asking a staff member who was not listed as a referee to provide a verbal reference for a colleague who has applied for a position with their organisation.

The employer must be informed that the University has a legal obligation to protect the privacy of staff personal information and staff members will only provide a verbal or a written reference when formally nominated as a referee.

5.2.2 Examples of queries where information SHOULD be released

(a) *Government Departments*
Centrelink telephones Adelaide University seeking confirmation of the enrolment status of a particular student.

The results should be provided in this circumstance. However the request should be put in writing and faxed to the University to verify the identity of the caller and to provide a record that can be placed on the student file for reference.

(b) *Employers*
An employer telephones asking whether a person who has applied for a position with their company is a graduate of the University.

The employer should be advised if the student is a graduate, as records of names of graduates are available in public documents. Academic results and dates of birth are personal information of the student but status as a graduate is a matter of public record and a legitimate interest of the University.

(c) *Other institutions*
(i) A staff member from another institution telephones and asks that the results of a student who undertook cross-institutional study be faxed to them.

The results should be provided in this circumstance. However the request should be put in writing and faxed to the University to verify the identity of the caller and to provide a record that can be placed on the student file for reference.

(ii) A staff member from another University telephones and asks that the results of a student who has applied to that institution be faxed to them.

The results should be provided in this circumstance. However the request should be put in writing and faxed to the University to verify the identity of the caller and to provide a record that can be placed on the student file for reference.

(d) *Adelaide University staff*
A member of academic staff telephones his or her faculty office or the Student Centre to request the contact details of a student who has not been attending tutorials.

The faculty office should release the information as it is required for the monitoring of the student's academic progress, and the identity of the staff member can be established. If the academic is known to the Student Centre staff the information should be released, if not the query should be referred to the relevant faculty office.

5.2.3 General queries

(a) *Students*
(i) A student refuses to sign the enrolment declaration agreeing that their personal and academic information might be released to a person or organisation outside the University.

The student should be advised that their enrolment will not be processed without the declaration signed because the University does not have any discretion over releasing personal information to authorised bodies and is legally obliged to make this clear to students before they provide such information.

(ii) A student objects to signing the enrolment declaration because they are concerned that information about their disability might be released to a person or organisation outside the University.

The student should be advised that information on disability is legally classified as 'sensitive' information rather than 'personal' information. The University has no legal obligation to routinely release sensitive information. Information on a disability will only be released to reduce or remove a threat to the life or health of any person.

(iii) A student signs the enrolment declaration but requests that they be personally notified if their personal information is released.

The student should be advised that, as thousands of students are enrolled at the University, there are a large number of requests for personal information from authorised agencies, and the University will not notify students individually when it releases personal information according to its legal obligations.

(b) *Members of the public*
(i) A researcher telephones the University requesting access to the student file of a famous graduate about whom they are writing a book.

The researcher should be advised to contact the Manager, Records and Archives Services, who will discuss the nature of the project and consider whether it is appropriate to release or discuss any of the information contained on the student file.

(ii) A member of the public telephones to ask if they access the University website whether their personal details will be collected for the purpose of sending them unsolicited information in the mail.

The caller should be advised that the University does not collect personal information indirectly through its website. The Internet address of the visitor will automatically be logged in the site's Internet access logs, and their server address, top level domain name (e.g. .com, .au), the date and time of the visit and the pages and documents accessed may be analysed through the use of small files of information called cookies, that save and retrieve information about the visit. This analysis is undertaken to determine the effectiveness of the site and to improve it for users. Users will only be identified where a law enforcement agency exercises a warrant to inspect the logs. The caller can be advised

that if they do not want their visit logged they should contact their Internet service provider to discuss disabling their cookies.

Meredith Strain, Kylie Percival, Kellie Toole 7 May 2001

Approved by Vice-Chancellor 22 August 2001
Amended 11 October 2001 (Section 5.2.1 (d) (ii) added)
Amended 12 December 2005 (Section 2.2.2 deleted)