PRIVACY MANAGEMENT PLAN

Table of Contents

1. INTRODUCTION

1.1 Commitment to Privacy

The University recognises that it has a responsibility to develop, encourage and implement sound organisational practices around the collection, use, disclosure and management of Personal Information. Although the University is not subject to the Commonwealth *Privacy Act 1988* (the Privacy Act) and no State privacy legislation currently exists, the University has, through its *Privacy Policy*, undertaken to adopt practices that are consistent with the Australian Privacy Principles contained in the Privacy Act.

This Privacy Management Plan provides detailed guidance to University Personnel on how the principles under the *Privacy Policy* should be applied.

1.2 Key concepts

"***Australian Privacy Principles****"* are contained in the Privacy Act.

"***Consent***" means express consent or implied consent

"***Health information***" means:

a. information or an opinion about:
   (i) the health or a disability (at any time) of an individual; or
   (ii) an individual's expressed wishes about the future provision of health services to him or her; or
   (iii) a health service provided, or to be provided, to an individual;
   that is also personal information; or

b. other Personal Information collected to provide, or in providing, a health service; or
c. other Personal Information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
d. genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

"***Personal information***" is defined in the Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.' The types of Personal Information that the University collects and holds will depend on the circumstance and relationship between the individual and the University. Personal information that is commonly collected by the University includes:

a. name
b. address (residential, postal and email)
c. phone number
d. date of birth
e. gender
f. ethnic origin
g. passport number
h. banking and credit card details
i. tax file number
j. health information
k. emergency contact details
l. photographs or video recordings (including CCTV footage)
m. criminal history
n. academic record
o. IT access logs
p. metadata from use of online services and facilities

q. records of donations and transactions

*"**Privacy Statement**"* means a notification, in the format specified under paragraph 2.2, that is required to be provided to an individual at or before the time (or, if that is not practicable, as soon as practicable after) the University collects Personal Information.

"***Sensitive information***" is defined in the Privacy Act as:

a. information or an opinion about an individual's:
   (i) racial or ethnic origin; or
   (ii) political opinions; or
   (iii) membership of a political association; or
   (iv) religious beliefs or affiliations; or
   (v) philosophical beliefs; or
   (vi) membership of a professional or trade association; or
   (vii) membership of a trade union; or
   (viii) sexual orientation or practices; or
   (ix) criminal record
   that is also Personal Information;

b. health information about an individual; or
c. genetic information about an individual that is not otherwise health information; or
d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
e. biometric templates.

*"**University Personnel**"* means all employees, titleholders, consultants, contractors and volunteers of the University.

2. COLLECTION OF PERSONAL INFORMATION

2.1 Information must be reasonably necessary or directly related
[Privacy Policy principle 1.1, 1.3]

University Personnel must not collect Personal Information unless it is reasonably necessary or directly related to the University's functions or activities. Personal information should not be collected 'just in case' it may be useful in the future.

Personal information must only be collected by lawful and fair means. Collection must not be unreasonably intrusive.

Example: If you are compiling a mailing list of people who want to receive information about the University and you only intend on sending that information by email, do not ask for their home address or phone number.
Example: External organisations hosting students for work experience or internships may require students to have a criminal history check. This is a requirement of the placement host, not the University. The School may need to sight the police certificate or DCSI clearance letter to confirm the student has fulfilled the requirement, but the School should not retain a copy unless it is necessary.

2.2 Notifying individuals of collection
[Privacy Policy principle 1.5]

Written Privacy Statement

Where Personal Information is collected or solicited from forms or websites, University Personnel must ensure that a Privacy Statement in the following format is included.

Privacy Statement

"The information you provide will be used for the primary purposes set out in the University of Adelaide's Privacy Policy and [insert any other specific purposes]. Please refer to the University's Privacy Policy (www.adelaide.edu.au/policies/62/) for more information, including the types of other entities to which the University may need to disclose Personal Information; how you can seek access to your Personal Information held by the University and how you can make a complaint if you feel your privacy has been breached."

****Additional text depending on the circumstances:*
If you know that there is need for the Personal Information to be disclosed to a third party:
"The University will need to disclose your personal information to [insert third party name and location (if overseas)]".

If there will be significant consequences if Personal Information is not provided:
"If you do not provide the information, [insert consequence, e.g. the University will be unable to process your application].

Additionally, the form or website must clearly identify the relevant School / Branch / Faculty and provide a contact email or phone number.

University Personnel should contact Legal and Risk if they require assistance with drafting the Privacy Statement.

Verbal Privacy Statement

Where Personal Information is collected through personal contact (e.g. phone, over the counter, photographing at University events), University Personnel must inform the individual of the information that is being collected; the purpose of collection and the availability of the University's Privacy Policy on the University's website.

2.3 **Sensitive information**
[Privacy Policy principle 1.3]

Consent required

University Personnel must generally only collect Sensitive Information with the individual's consent and when the information is reasonably necessary for one or more of the University's functions or activities.

Limited circumstances where consent not required

University Personnel may collect Sensitive Information without the individual's consent in the following limited circumstances:

a) the collection is required or authorised by Australian law or court / tribunal order; or

b) it is unreasonable or impracticable to obtain consent and the University has a reasonable belief that the information is needed to lessen or prevent a serious threat to the life, health or safety of an individual or the public; or

c) the University has a reasonable belief that the information is needed in order to take action on suspected unlawful activity or misconduct of a serious nature; or

d) the information is reasonably necessary for a legal defence or claim; or

e) the information is health information and is required for the University to provide a health service to the individual and the information is collected in accordance with obligations of professional confidentiality; or

f) the information is health information and:

   i. is necessary for the University to undertake research or statistical analysis relevant to public health or public safety;

   ii. it is impracticable for the University to obtain the individual's consent; and

   iii. the information is collected in accordance with relevant NHMRC guidelines (*National Statement on Ethical Conduct in Human Research 2007* and the *Australian Code for the Responsible Conduct of Research 2007)*.

University Personnel should seek advice from Legal and Risk before relying on any of the above exemptions in order to collect Sensitive Information without the individual's consent.

2.4 Collection of information from a third party

[Privacy Policy principle 1.3, 1.5]

Where possible, University Personnel must collect Personal Information only from the individual concerned. If Personal Information about an individual is collected from another source, University Personnel must take reasonable steps to ensure that the individual is or has been made aware:

a) that the University has collected the information and the circumstances of the collection;

b) of the matters that would have been contained in a Privacy Statement provided to the individual had the information been collected directly from the individual.

This applies even if the information is collected from publicly available source (e.g. internet, telephone directory, electoral roll).

Example: Applications into University programs are processed by SATAC. SATAC then provides the applicant details to the University. The University should ensure that SATAC notifies applicants that their Personal Information will be collected by the University and the purposes for which it will be used.
Example: A researcher wants to survey persons in a specific electorate for a research project. The researcher obtains names and addresses from the electoral roll. The researcher should ensure that the survey sent to the individuals explains where the researcher has obtained their details from, and includes a Privacy statement.

2.5 Anonymity and pseudonymity

[Privacy Policy principle 1.7]

Areas collecting Personal Information from individuals must provide individuals with the option of not identifying themselves, or of using a pseudonym, except where:

a) the University is required or authorised by Australian law or a court / tribunal order, to deal with individuals who have identified themselves

Example: In order for the University to satisfy its reporting requirements to the Commonwealth, the University requires students to enrol using their real names.

OR

b) it is impracticable for the University to deal with individuals who have not identified themselves or who have used a pseudonym

Example: A library user submits an inter-library loan request. The Library will need to know the individual's true identity in order to be able to verify that the individual is a registered library user entitled to make such request, and also to contact the individual once the item becomes available.
Example: The 'name' field on survey forms should not be mandatory unless the University intends to make follow-up contact with the individual

2.6 **Unsolicited Personal Information**
[Privacy Policy principle 1.6]

Unsolicited Personal Information is information that the University receives but has not taken active steps to collect, e.g.

- emails sent to the University in error
- unsolicited correspondence
- additional information provided as part of a job application but was not actually required for that application (e.g. photograph, copy of passport)

If unsolicited Personal Information is received, and such information is not reasonably necessary or directly related to the University's functions or activities, that information must be destroyed or de-identified, unless it is necessary to preserve the document in order to comply with the University's recordkeeping obligations (refer to Records and Archives Management Manual).

If a decision is made to retain the unsolicited Personal Information for use by the University (e.g. a CV sent 'on spec' is to be retained on file for consideration for future job opportunities), the individual must be provided with a Privacy Statement.

3. **USE AND DISCLOSURE**

3.1 **Primary purpose**
[Privacy Policy principle 2.1, 2.2]

University Personnel may use or disclose Personal Information for a purpose ("Primary purpose") set out in Policy Principle 2.1 of the Privacy Policy or in the Privacy Statement provided to the individual.

3.2 **Secondary purpose**
[Privacy Policy principle 2.3]

University must not use or disclose Personal Information for another purpose ("Secondary purpose") except in the following circumstances:

a) the individual has consented to use or disclosure for the Secondary purpose; or

b) both of the following apply:

i) the individual would reasonably expect the University to use or disclose the Personal Information for the Secondary purpose; and

ii) the Secondary purpose is related to the Primary purpose (or in the case of Sensitive Information, directly related to the Primary purpose)

Example: A student applies to enrol in a program that is clearly advertised as being jointly delivered by the University with other universities and that applications will be considered by all collaborating universities. → It is reasonable for the University to share the student's application details to the other universities so that they can assess the application.
Example: An individual submits an entry to a University-run competition. The competition rules clearly state that entries will be judged by an independent panel. → It is reasonable for the University to share the individual's entry with the panel members.

c) the use or disclosure is required or authorised by Australian law or court/tribunal order;

Example: Under the Health Practitioner Regulation National Law (South Australia) Act 2010, the University is required to provide to the Australian Health Professional Regulation Authority details of students enrolled in certain Health Sciences programs to enable those students to be registered by AHPRA. → Disclosure permitted
Example: The University is subpoenad to produce personnel records of a staff member who is involved in a motor vehicle accident case. → Disclosure permitted
Example: Centrelink, acting under the Social Security (Administration) Act 1999, has the power to request the University to provide enrolment information about a student. → Disclosure permitted
Example: The University has received a Freedom of Information request and has determined that certain information should be exempted from disclosure for reasons of privacy. The Ombudsman has, upon external review, reversed the University's determination and requires the University to release that information. → Disclosure permitted
Example: The Board of Examiners of the Law Society of SA is authorised under law to make inquiries with the University's Law School as to whether a person who has applied for admission to legal practice has been guilty of dishonest conduct or any

other conduct relevant to the determination of the question whether the applicant is a fit and proper person to be admitted as a practitioner. → Disclosure permitted
Example: The University is required to report any student visa breaches to the Department of Immigration and Border Protection. → Disclosure permitted
Example: Staff who are subject to mandatory reporting requirements under the Children's Protection Act are required to notify any suspected child abuse or neglect to the Department for Communities and Social Inclusion. → Disclosure permitted

d) the University has a reasonable belief that the use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

Refer to paragraph 6.3.1 below for how requests from police should be handled.

e) It is unreasonable or impracticable to obtain the individual's consent to the use or disclosure and the University reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;

Example: The University's Early Intervention Group has formed a reasonable belief that a student is at risk of self-harming. → The University can notify the State's Mental Health Triage Service so that Mental Health Triage Service can determine whether to take action to locate the student and provide intervention.

f) The University has a reasonable belief that the use or disclosure is needed in order to take action on suspected unlawful activity or misconduct of a serious nature;

Example: The University has a reasonable suspicion of fraudulent activity by a staff member and engages an investigator. → The University may disclose personal information to that investigator for the purposes of the investigation.

g) The University has a reasonable belief that use or disclosure is reasonably necessary to assist an organisation or person to locate a person who has been reported as missing;

h) The use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim;

i) The information is health information and:

i. use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety;
ii. it is impracticable to obtain the individual's consent;
iii. the use or disclosure is conducted in accordance with relevant NHMRC guidelines (*National Statement on Ethical Conduct in Human Research 2007* and the *Australian Code for the Responsible Conduct of Research 2007);*
iv. in the case of disclosure, the recipient of the information has undertaken not to disclose the information.

Example: The Department of Health engages the University to undertake research into an urgent issue of public health using health information that was collected under

previous projects. → The University is permitted to use the previously collected health information however any Ethics requirements must still be adhered to.

University Personnel should seek advice from Legal and Risk if they wish to rely on paragraphs 3.2(e) to (i) above.

Requests from third parties for disclosure under paragraphs 3.2(c), (d) and (g) should be handled in accordance with paragraph 6.3 below.

3.3 **Permitted disclosure to third parties**
[Privacy Policy principle 2.4]

As stated in the University's Privacy Policy, the University may disclose Personal Information to:

a) Government departments and agencies to satisfy reporting requirements;

b) the University's Controlled Entities, to the extent such Personal Information is required by the Controlled Entity to provide services to the University or undertake activities for the University;

c) external advisers and service providers to the extent such Personal Information is required for that party to provide services to or on behalf of the University;

d) collaborating parties to the extent such Personal Information is required for the collaborative activity to be undertaken.

Example: An externally hosted software provider requires student names and email addresses in order to establish user accounts to enable the student to have access to internet-based education resources and assessment tools. → Disclosure permitted (but refer to paragraph 3.4 below if software provider or server is located outside Australia)
Example: A Faculty organises clinical placements for students and the placement host requires names and emergency contact details of the attending students. → Disclosure permitted.
Example: The University offers a double degree with another university. The University needs to be able to share student details and results with the other university to facilitate enrolment and maintain student records. → Disclosure permitted

Where disclosure is made to a third party under paragraphs 3.3(c) or (d) above, University Personnel must ensure that there is a contract in place with the third party that contains obligations on the third party to maintain privacy of the Personal Information.

3.4 **Disclosure to third parties located outside Australia**
[Privacy Policy principle 2.5, 2.6]

Prior to disclosing Personal Information to a third party located outside Australia ("overseas recipient"), University Personnel should consult with Legal & Risk.
Examples of overseas disclosure include:

- Providing an externally hosted software provider with student names and email addresses in order for the provider to establish user accounts

- Sharing research data containing Personal Information with an overseas collaborating institution

- Storing electronic files of personal information on a server located overseas

In determining the acceptability of disclosure to offshore third parties, University Personnel must consider the reasonableness of the types of Personal Information to be disclosed; the location of the overseas recipient (or its servers) and the overseas recipient's data security protocols must be considered.

Additionally, at least one of the following must be met:

a) there is a contract between the University and the overseas recipient that binds the overseas recipient to privacy obligations that are consistent with the Australian Privacy Principles; or

b) the overseas recipient is subject to a law or binding scheme that has the effect of protecting the Personal Information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information, and that individuals are able to access mechanisms to enforce the protection of the law or binding scheme; or

c) express consent is obtained from the individuals to the disclosure of their Personal Information to the overseas entity and that subclause 8.1 of the Australian Privacy Principles will not apply to the disclosure.

3.5 Direct marketing

[Privacy Policy principle 2.7]

"Direct marketing" means issuing marketing or promotional materials about the University or other parties directly to an individual (e.g. by post, email, SMS)

University Personnel must not use Personal Information for the purpose of direct marketing unless such use is contemplated under Policy Principle 2.1 of the University's Privacy Policy or consent has been obtained from the individual.

Hardcopy direct marketing material must contain a contact point for the individual to opt out of receiving further direct marketing communications from that area of the University issuing the direct marketing communication. Once an individual has made such a request, that area must not issue any further direct marketing communications to the individual.

Direct marketing material sent by email and SMS must comply with the *Spam Act 2003* (Cth) which also requires an opt-out mechanism. Refer to
http://www.adelaide.edu.au/its/it_policies/email/spam.html

3.6 Government related identifiers

The University must not adopt a government related identifier (e.g. Tax File Number, Medicare number, Passport number, Driver's Licence number) as the identifier of an individual.

Tax File Numbers must only be used or disclosed for a purpose authorised by taxation law, the *Higher Education Support Act 2003* (Cth) or superannuation law. Collection, use and storage of Tax File Numbers must be compliant with the *Privacy (Tax File Number) Rule 2015*.

The University must not use a government related identifier of an individual unless the use is reasonably necessary for the University to verify the identity of the individual for the University's activities or functions.

4. ACCURACY OF INFORMATION

4.1 Ensuring accuracy of Personal Information

[Privacy Policy principle 3.1, 4.4, 4.5]

University Personnel must take such steps as a reasonable in the circumstances to ensure that Personal Information they collect, use or disclose is accurate, up-to-date, complete, relevant and not misleading.

The University provides online portals (Staff Services Online, Access Adelaide, Adelaide OnLion) for employees, students and alumni to update their Personal Information themselves.

In the case of other individuals with whom the University deals with on a repeated basis, where practicable, those individuals should be issued with reminders to notify the University of any changes to their Personal Information.

If University Personnel become aware or are notified that Personal Information in the University's possession is not accurate, the University Personnel must notify the area responsible for managing the Personal Information, and other areas that may have copies of the Personal Information, so that steps can be taken to correct the information.

Example: A School sends a letter to a student using the address within Peoplesoft but the letter is returned to sender and marked "Not at this address". → The School should notify Student Administrative Services so that the address in Peoplesoft can be removed and an email can be sent to the student reminding them to update their details in Access Adelaide.

4.2 Correction of Personal Information

[Privacy Policy principle 4.5, 4.6]

Students, employees and alumni have the opportunity, and are encouraged, to correct or update their Personal Information via the Access Adelaide, Staff Services Online or Adelaide OnLion systems respectively.

All individuals may submit a request to the University to correct or update Personal Information about them held by the University. Requests must be submitted as follows:

Requestor	**Submit request to:**
Student	Ask Adelaide
Employee / Titleholder	HR Service Centre
Research participant	The relevant researcher
Alumni or Donors	External relations
Others	The area of the University to which the individual provided their Personal Information

Areas receiving correction requests should respond within 30 days of receipt of the request and must not impose any charges for the request.

If the area refuses to make the requested correction, that area must provide the individual with a written notice setting out the reasons for refusal and that the individual may apply to the Manager,

Compliance to seek review of the decision. Requests for review will be referred to the relevant Deputy Vice-Chancellor or Vice-President.

5. SECURITY OF PERSONAL INFORMATION

5.1 Security measures

[Privacy Policy principle 3.1]

The University must take such steps as are reasonable in the circumstances to protect Personal Information in its possession from misuse, interference, loss, and unauthorised access, modification or disclosure.

Personal information must only be made accessible to, and must only be accessed by, those University Personnel who have a need to access it to perform their duties.

Example: Student files in HPRM should only be accessible by University Personnel within the security group established by Records Management Office

Personal information in electronic format must be stored and managed securely – refer to guidelines at http://www.adelaide.edu.au/secureit/.

Credit card information must be handled in accordance with the *Managing Customer / Student Credit / Debit Data* Procedures under the *Financial Management Policy.*

Hardcopy records containing Sensitive Information should be stored in locked furniture when not in use. Hardcopy staff or student files should not be left on desks when offices are unattended, or in places where they are visible to students or members of the public.

5.2 Destruction of Personal Information

[Privacy Policy principle 3.1]

If the Personal Information is no longer needed for the purpose it was collected, and the University is not otherwise required to retain the information under any law, regulation or code (e.g. State Records Act and General Disposal Schedules (http://www.adelaide.edu.au/records/services/disposal-schedule/); ARC / NHMRC Research Code), that information must be destroyed in a secure manner or de-identified.

6. DEALING WITH REQUESTS FOR ACCESS TO PERSONAL INFORMATION

6.1 Individuals seeking access to their own Personal Information

[Privacy Policy principle 4.1, 4.3]

Individuals (other than employees, titleholders and students) who request access to Personal Information about themselves held by the University should be directed to submit their request to the University's Freedom of Information officer. The Freedom of Information officer will process requests in accordance with the *Freedom of Information* policy.

6.2 Employee, titleholder or student seeking access to their own Personal Information

[Privacy Policy principle 4.2]

Employee and Titleholder access to appointment files

Employees and titleholders are entitled to request access to their appointment files without the need for a formal application under the *Freedom of Information Act*.

Employees and titleholders can contact the HR Service Centre to make an appointment to view their centrally-held appointment file in the presence of a Human Resources officer.

Where personnel files are maintained by the local area to which the employee or titleholder is appointed, the employee or titleholder may submit a request to their Head of School / Branch to view their local personnel file in the presence of a School / Branch officer.

Student access to student files and student records

Current and former students are entitled to request access to their student file and records without the need for a formal application under the *Freedom of Information Act*.

Students can apply in writing or email to Ask Adelaide to view their student file in the presence of a Student Administration officer.

Students can apply in writing or email to their Head of School to view any of their student records held by the School, in the presence of a School officer.

Students who have utilised Counselling or Disability Services can apply in writing or email to the Manager, Counselling & Disability Services to view their counselling file, in the presence of a counsellor or disability advisor.

Limitation on access

Documentation may be withheld or redacted if the University determines that access would not be appropriate. Reasons may include:

- unreasonable impact on the privacy of other individuals (e.g. personally identifying information of referees on a staff appointment file)
- the request for access is frivolous or vexatious
- documents are subject to confidentiality obligations or legal professional privilege
- granting access would compromise the University in anticipated legal proceedings or commercially sensitive decision-making processes

Staff or students who have been refused access under this procedure are still entitled to submit a Freedom of Information application for that document.

6.3 Third parties seeking access to Personal Information

Personal Information may only be disclosed to third parties if permitted under paragraph 3.1, 3.2 or 3.3 above. The procedures and examples listed below address some common scenarios and set out how University Personnel should deal with such requests for access from third parties.

6.3.1 Requests from police

Requests from police for access to staff Personal Information must be referred to the HR Service Centre and requests for access to student Personal Information must be referred to the Associate Director, Student Administration.

Except as provided below, University Personnel must not release Personal Information unless the police provide a warrant.

In circumstances where the police request urgent access to Personal Information, the University may release the Personal Information on the basis of the exemption under paragraph 3.2(d), however University Personnel releasing the information must ensure that:

a) the request has been made or authorised by Sergeant rank or higher; and

b) the request identifies that the information is necessary for the police's law enforcement activities; and

c) the request is either made in writing on official letterhead or from a recognised email address; or in person with their identity badge.

A record of the access granted must be retained.

6.3.2 Requests from Government agencies

Various Government agencies are empowered by legislation to request Personal Information in order to undertake their functions (e.g. Australian Tax Office, Centrelink, Workcover, Ombudsman, Australian Health Professional Regulation Authority, Safework SA)

If such a request is made, University Personnel must require that it is in writing and cite the authority upon which the request is made. If uncertain about the bona fides of the request, University Personnel should consult with Legal and Risk before releasing any information.

A record of the access granted must be retained.

6.3.3 Requests from family members

The University often receives inquiries from parents of students about the student's academic progress or attendance at class. University Personnel who receive such inquiries must advise the inquirer that the University is not entitled to disclose or discuss the information without the student's consent.

The University may release Personal Information of students to family members in circumstances under paragraph 3.2(e) or 3.2(g) above. University Personnel receiving such requests should consult with Legal and Risk before releasing any information.

6.3.4 Requests from lawyers (other than the University's lawyers)

Lawyers do not have a special right to access information held by the University. Personal information must not be disclosed in response to a lawyer's request unless with consent of the person to whom the information relates, or if required by law or court/tribunal order.

Example: A lawyer is representing a student in a motor vehicle accident claim. The lawyer issues a written request for the student's academic records and copies of WNF requests submitted by the student. → These may only be provided if a disclosure consent form signed by the student has been attached.
Example: A lawyer requests certain records pertaining to a former staff member. The lawyer is representing an individual who is suing that former staff member. → These records should not be released. If the lawyer requires the documents for a trial, it is up to the lawyer should obtain a subpoena from the court. Documents ordered under a subpoena are to be delivered to the Court Registrar's office stated in the subpoena.

6.3.5 Other examples of requests

Example: A company seeks confirmation from the University on whether a person who has applied for a position with that company is in fact a graduate of the University. *→ The University is able to provide confirmation, as names of graduates are made publicly available. However, the University must not provide details of academic results.*
Example: Some students have established a student association for a particular discipline. The President of the student association asks the Faculty for the names and email addresses of all students in that discipline so it can contact those students to encourage them to join. *→ The Faculty should not provide this information to the association. Instead, the Faculty can offer to disseminate information about the student association to students (e.g. via a bulletin board or email) and students can elect to initiate contact with the association if they are interested.*

7. PRIVACY PLANNING

[Privacy Policy principle 3(b)]

The best way of ensuring privacy compliance is to adopt a 'privacy by design' approach, whereby privacy compliance is considered and addressed from the start of a project, rather than being retrofitted.

The University's Risk Management Handbook requires that any proposed partnership, project or initiative should actively consider risk and document the assessment formally. When planning a new partnership, project or initiative that may involve collection or handling of Personal Information, or any changes to existing practices regarding the collection or handling of Personal Information, the following should be considered in the overall risk assessment for that project or activity.

7.1 Collection

- What personal or sensitive information will be collected?
- Why are the particular types of personal information necessary for the project / activity?
- Can de-identified or anonymous data be used instead?
- How will the information be collected? How will you notify the individuals?

7.2 Use

- How do you intend to use the personal information?
- If the personal information has already been collected and you are now planning to use it for a secondary purpose (i.e. other than a purpose set out in Policy Principle 2.1 of the Privacy Policy or in the Privacy Statement provided to the individual), should additional consent be obtained?
- Will your project / activity involve any data linkage or matching? What safeguards will be in place to ensure data linkage accuracy and that the individuals will not be adversely affected by incorrect data matching?

7.3 Disclosure

- To whom, how and why will the personal information be disclosed? Can you ensure the disclosed information will have the same privacy protections?
- Will personal information be disclosed to overseas recipients?

7.4 Information quality

- What are the consequences for individuals if the personal information is not accurate or up-to-date?
- How can individuals have their personal information corrected, or annotations made, if necessary

- How will personal information updates be given to others who have previously been given personal information about an individual?

7.5 Security

- Where will the personal information be stored? Who will have access?
- What security measures will be in place to protect the personal information from loss, unauthorised access, use, modification, disclosure or other misuse?

7.6 Compliance with other privacy laws

- Will the project / activity be subject to a contract requiring the University to comply with other privacy laws (e.g. if funding is from an interstate Government department, the contract may require compliance with that State's privacy legislation)
- Will the project / activity involve offering goods / services to individuals living in the European Union – this may cause the University to be subject to the *European Union General Data Protection Regulations*

8. DEALING WITH LOSS OR UNAUTHORISED DISCLOSURE OF PERSONAL INFORMATION

8.1 Data breach

Loss or unauthorised disclosure of Personal Information ("data breach") may occur in a variety of ways. It may be inadvertent or deliberate or malicious, for example:

- mistakenly emailing Personal Information to the wrong person
- loss or theft of laptops, removable storage devices or physical files
- hacking of University systems containing Personal Information
- staff accessing Personal Information outside the requirements of their employment

Data breaches have the potential to result in harm to the individuals affected and expose the University to legal, financial or reputational risk.

8.2 Responding to a data breach

[Privacy Policy principle 5.1]

The University has a Data Breach Response Plan which sets out procedures if a University Personnel becomes aware of an actual or suspected data breach. A Flowchart which forms part of the Data Breach Response Plan outlines the process for reporting, assessing, and responding to data breaches.

8.3 Data Breach Response Group

The University's Data Breach Response Group will be established in accordance with its Terms of Reference. The purpose of the Data Breach Response Group is to contain, assess and respond to significant data breaches in a timely and consistent manner. The Data Breach Response Group will determine if there is a need to notify affected individuals, the Office of the Australian Information Commissioner or others, having regard to any mandatory data breach reporting requirements under legislation, contract or binding code.