PRIVACY MANAGEMENT PLAN

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Commitment to Privacy

The collection and management of Personal Information is an integral part of the University's function and purpose. The University recognises that it has a responsibility to respect and protect Personal Information and to develop, encourage and implement sound organisational practices around the collection, use, disclosure and management of Personal Information.

The University has, through its *Privacy Policy*, adopted practices that are consistent with the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth).

The University is also committed to complying with the requirements of EU General Data Protection Regulation 2016/679 (**GDPR**) ***which may apply when the University handles / processes Personal Information of individuals who are located in the European Economic Area*** (**EEA**). Generally the GDPR sets higher compliance requirements than the Australian Privacy Principles regarding:

- Pre-activity risk assessments
- Privacy statements and consents
- Lawful basis for handling information
- Disclosures to third parties
- Rights of individuals
- Data breach notifications

1.2 Overview of Privacy Management Plan

The main section of this Privacy Management Plan provides detailed guidance to University Personnel on how the principles under the *Privacy Policy* should be applied when GDPR does not apply.

Appendix 1 provides guidance where GDPR applies.

1.3 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. place of birth
h. citizenship
i. passport number
j. banking and credit card details
k. tax file number
l. health information
m. emergency contact details
n. photographs or video recordings (including CCTV footage)
o. criminal history
p. academic record
q. IT access logs (e.g. IP address)
r. metadata from use of online services and facilities (e.g. cookie identifiers)
s. 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 (that is also Personal Information) 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; or
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
[Privacy Policy principle 1.1]

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 1.4]

Written Privacy Statement

General

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 purpose of [insert specific purpose] and otherwise be handled in accordance with the University of Adelaide's Privacy Policy. 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, how the University will manage a data breach, 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 Services if they require assistance with drafting the Privacy Statement.

Research

Where Personal Information is collected for research purposes the University's Human Research Ethics Committee has a template Participant Information Sheet, which assists participants in their decision to take part in research and addresses privacy and confidentiality, security, storage, sharing, and future use of data/information for research purposes.

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.

A written record must be retained of the verbal Privacy Statement provided to an individual and the consent given by the individual.

2.3 Sensitive information

[Privacy Policy principle 1.2]

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. The key elements of informed consent are:

- the individual is adequately informed before giving consent;
- the individual gives consent voluntarily;
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

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 Services 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 1.4]

Where possible, University Personnel must collect Personal Information only from the individual concerned. If Personal Information about an individual is collected from another source, unless the circumstances where consent is not required (see section 2.3 above) 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). Personal Information on social media platforms may not be considered publicly available. For example if the Personal Information is only accessible by other users of the platform (and not non-users) then it is generally not considered publicly available and should not be collected / used.

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 1.6]

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 1.5]

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 9, 4.1]

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 4.2]

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 subpoenaed 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 → Disclosure permitted
Example: 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 (updated 2018),* G*uidelines under Section 95 and 95A of the Privacy Act 1988 (2014),* 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 Services 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 11]

The University may disclose Personal Information to:

a) Government departments and agencies to satisfy reporting requirements;

b) regulators and law enforcement bodies for the purpose of conducting investigations and enforcement related activities;

c) 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;

d) 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;

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

f) third parties impacted by investigations into misconduct complaints such as student accommodation providers, clubs, societies, or placement providers in accordance with the Sexual Misconduct Policy and the Sexual Misconduct Response Procedures. Section 7.3 of the Sexual Misconduct Response Procedures permits the University to:

- share information (including Personal Information) relating to a complaint related to the Complaint and the investigation for the purposes of conducting a joint investigation; and
- share the outcome of its investigation, including any investigation report, with the third party.

g) third parties impacted by investigations into research misconduct complaints, such as research publishers, funding bodies, and affiliated organisations in accordance with the Research Misconduct Procedure;

h) Adelaide University, as the successor of the University by operation of the Adelaide University Act 2023, for purposes related to the transition of the University to Adelaide University;

i) third parties as required or authorised by Australian law or court/tribunal order; and

j) third parties the individual has consented to or would reasonably expect.

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(d) or (e) 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 3.2]

Prior to disclosing Personal Information to a third party located outside Australia ("overseas recipient"), University Personnel should consult with Legal Services.
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 3.4]

"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 the Privacy Policy, this Plan, a Privacy Statement, or consent has been obtained from the individual, the use is permitted by the Privacy Act, or is required or authorised by law.

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.

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 5.1]

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 OnLine) 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.

The University may update Personal Information using publicly available sources.

4.2 Correction of Personal Information

[Privacy Policy principle 5.5, 5.6]

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 OnLine 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 4.4]

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 are authorised 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 unauthorised staff, students or members of the public.

5.2 Destruction of Personal Information

[Privacy Policy principle 4.4]

If the Personal Information is no longer needed for the purposes permitted at the time of collection it can , 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 5.3]

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, the Privacy Policy and Procedures.

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

[Privacy Policy principle 5.5]

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 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.

If students are unable to physically attend the University, the University will seek to provide alternative arrangements as appropriate.

Limitation on access

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

a) unreasonable impact on the privacy of other individuals (e.g. personally identifying information of referees on a staff appointment file)

b) the request for access is frivolous or vexatious or would require an unreasonable diversion of University resources

c) documents are subject to confidentiality obligations or legal professional privilege

d) 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 access to Personal Information, the University may release the Personal Information where the University has a reasonable belief that the use or disclosure is reasonably necessary for law enforcement related activities, 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.

If the police request involves Personal Information in CCTV images the University may release the CCTV images in accordance with the University of Adelaide Security Services CCTV Guidelines. Generally releasing CCTV images to third parties requires prior approval from General Counsel, Legal Services.

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, Independent Commission Against Corruption)

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 the Office of General Counsel Legal Services 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 Services 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 4.5]

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.

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, a Privacy Impact Assessment should be completed to assess the privacy risks for that project or activity. The University's Privacy Impact Assessment (**PIA**) form should be used to undertake that privacy risk assessment. The University PIA form is available on the Legal Services – Self Service Resources webpage under the '*Forms'* tab.

Undertaking a PIA should be seen as a process that does not end with the completion of the PIA form. A PIA may be useful more than once during the project's development and implementation. It should be revisited and updated when changes to the project are considered. If there are substantial changes to how Personal Information will be handled or changes to an existing project, it may be necessary to undertake another PIA.

Other areas of the University involved in the proposed Processing activity should also be consulted with as part of completing the PIA.

Consult with Legal Services if:

- the PIA results in a privacy risk rating of ***high*** (according to the University's Risk Matrix); or
- the activity involves **Sensitive Information** (see definitions).

There are additional requirements for PIAs if GDPR applies. Please refer to paragraph 3 of Appendix 1.

8. DATA BREACH

8.1 Data breach

[Privacy Policy principle 7.1]

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
- uploading spreadsheets containing Personal Information to shared drives
- University systems containing Personal Information are compromised by cyber attack
- 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 7.1]

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 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 other stakeholders, having regard to any mandatory data breach reporting requirements under legislation, contract or binding code.

Appendix 1 – GDPR Privacy Management

1. INTRODUCTION

Where Personal Information concerns individuals who reside or are located in the European Union, the privacy management approach adopted must be consistent with the guidance below.

1.1 Key concepts under GDPR

"***Consent***" means 'any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

"***Data Controller***" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of personal information. Generally the University will be a Data Controller.

"***Data concerning health***" means 'Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.'

"Data Protection Officer" means the General Counsel, Legal Services.

"***Data Subject***" means an individual who is physically located in the European Economic Area at the time that their personal information is collected by the University. A person does not need to be a citizen of a European country in order to considered a Data Subject.

"***Personal Data***" means 'information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' The types of Personal Data that the University collects and holds will depend on the circumstance and relationship between the individual and the University. Personal Data that is commonly collected by the University includes:

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

*"**Personal Data Breach**"* means 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.'

"***Privacy by Default***" means data Processing with the standard settings of products and services set in such a way that it provides maximum protection of the privacy of Data Subjects. This means – among other things – requesting and Processing as little data as possible.

"***Privacy by Design***" means the management of the entire life cycle of Personal Data, from the collection to the Processing and erasure, with mechanisms that are designed to take as much account of the privacy of Data Subjects as possible. This involves systematically paying attention to comprehensive safeguards with regard to accuracy, confidentiality, integrity, physical security and erasure of the Personal Data.

"***Privacy Statement***" means a notification to Data Subjects about the nature of a proposed collection and Processing of their Personal Data, and that complies with the requirements set out in paragraph 5.

"***Processing***" means 'any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

"***Processor***" means 'a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.'

*"**Special Categories of Personal Data***" means 'Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'

*"**Supervisory Authority**"* means 'an independent public authority which is established by a Member State pursuant to Article 51.'

*"**Third Party**"* means 'a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.

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

2. GDPR PRINCIPLES FOR PROCESSING PERSONAL DATA

GDPR contains overarching Processing principles that the University must adhere to in relation to all Processing of Personal Data. These Processing principles are as follows:

a) Personal Data must be Processed based on one of the statutory bases of Processing (**lawfulness of Processing**) (see paragraph 4 below);

b) Personal Data must be processed fairly and in a transparent manner in relation to the Data Subject (**fairness and transparency**);

c) Personal Data can only be collected for specified, explicit and legitimate purposes that has been communicated to the Data Subject prior to the Processing. Personal Data cannot be further processed in a manner that is incompatible with those purposes (**purpose limitation**);

d) Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (**data minimisation**);

e) Personal Data must be accurate and, where necessary, kept up to date. Reasonable steps must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is to be processed, is erased or rectified without delay (**accuracy**);

f) Personal Data can only be kept in a form permitting identification of Data Subjects for as long as required for the purposes for which the Personal Data is processed (**storage limitation**);

g) Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

Prior to collecting and Processing any Personal Data, University Personnel should ensure that the collection and Processing of Personal Data is compliant with the above Processing principles. Please see below for further guidance on how to do so.

3. PRIVACY PLANNING

[Privacy Policy principle 4.5]

3.1 Data protection by design and by default

When determining the means of Processing Personal Data, and at the time of Processing itself, the University shall implement the principles of 'Privacy by Design' and 'Privacy by Default'. This involves the University implementing appropriate technical and organisational measures (such as pseudonymisation to minimise the data collected) to ensure safeguards are built into the Processing of Personal Data.

The appropriate technical and organisational measures are determined with reference to the cost of implementation, the nature, scope, context and purposes of Processing as well as the risks posed by the Processing to Data Subjects.

3.2 Data protection impact assessment

Prior to commencing a project or activity that involves Processing Personal Data that impact the rights and freedoms of natural persons the responsible University Personnel must assess the privacy risk using the University's **Privacy Impact Assessment** or **PIA**. The University PIA form is available on the Legal Services – Self Service Resources webpage under the '*Forms'* tab.

Some examples of the activities that require a PIA include:

a) using new technologies;
b) tracking people's behaviour or location;
c) systematically monitoring a publicly accessible place on a large scale;
d) Processing Special Categories of Personal Data;
e) if the Processing is used to make automated decisions about people that could have an impact on their rights and freedoms;
f) Processing Personal Data about children.

Other areas of the University involved in the proposed Processing activity should also be consulted with as part of completing the PIA.

Consult with Legal Services if:

- the PIA results in a privacy risk rating of ***high*** (according to the University's Risk Matrix); or
- the activity involves **Special Categories of Personal Data** (see definitions).

4. LAWFUL BASIS OF PROCESSING

[Privacy Policy principle 6.2]

4.1 Personal Data

The University should only process Personal Data if one of the following lawful bases applies:

a) the Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into a contract;

c) Processing is necessary for the University to comply with a legal obligation;
d) Processing is necessary in order to protect the vital interests of the Data Subject or another person;
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University; or
f) Processing is necessary for the purposes of the legitimate interests pursued by the University or a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

However, despite any legal basis which may apply, the Processing of Personal Data relating to criminal convictions and offences shall only be carried out under the control of official authority or when the Processing is authorised by Union or Member State law which provides for the appropriate safeguards for the rights and freedoms of Data Subjects.

4.2 Special Categories of Personal Data

The University is dedicated to ensuring that all Processing of Special Categories of Personal Data is lawful under GDPR. As Processing of Special Categories of Personal Data is prohibited at first instance, the University should only process Special Categories of Personal Data where one of the following exceptions applies:

a) the Data Subject has given explicit Consent to the Processing of those Personal Data for one or more specified purposes;
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the University or of the Data Subject in the field of employment and social security and social protection law;
c) Processing is necessary to protection the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
d) Processing relates to Personal Data which is manifestly made public by the Data Subject;
e) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; and
f) Processing is necessary for reasons of substantial public interest.

Tips:

- The lawful basis must be determined before the Processing begins, and you should document it.
- Take care to get it right the first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from Consent to a different basis.
- Consent can be withdrawn at any point and if it is withdrawn the Personal Data can no longer be processed and as a result will usually have to be deleted. For this reason, where possible and valid, a lawful basis other than Consent should be relied upon.

4.3 Conditions for Consent

Where the University is Processing based on the Consent of the Data Subject, the University shall adhere to the following additional conditions of Consent:

a) the University shall only process the Personal Data where the University can demonstrate that the Data Subject has Consented to the Processing;
b) if the Data Subject's Consent is given in the context of a written declaration which also concerns other matters, the request for Consent shall be presented in a manner which is clearly distinguishable from the other matters;
c) the Data Subject shall have the right to withdraw their Consent at any time and shall be notified of that right prior to giving Consent. Such withdrawal shall not affect the lawfulness of Processing based on Consent before its withdrawal;
d) it shall be as easy to withdraw Consent as it is to provide Consent; and
e) when assessing whether Consent is freely given, utmost regard will be given to whether performance of a contract (including the provision of a service) is conditional on the Data

Subject Consenting to the Processing of Personal Data that is not necessary for the performance of that contract.

5. COLLECTION OF PERSONAL DATA

5.1 Principles of collection

The University should only collect Personal Data where one of the lawful bases of Processing applies as outlined in paragraph 4 of this Appendix. When collecting Personal Data, the University will adhere to the GDPR principles (outlined in paragraph 2) including collecting the Personal Data for specified, explicit and legitimate purposes and limiting the Personal Data collected to what is adequate and relevant for the purpose for which it is to be processed.

5.2 Collecting directly from the Data Subject

When collecting the Personal Data directly from that Data Subject, the University should at the time of collection provide the Data Subject all of the following information in a Privacy Statement:

a) the identity and the contact details of the University and (where applicable) the University's Third Party representative;
b) the lawful basis for the Processing;
c) the purposes for which the Personal Data is intended;
d) the legitimate interests pursued by the University or by a Third Party (only where 4.1(f) applies);
e) the intended recipients or categories of recipients of the Personal Data;
f) whether the University intends to transfer Personal Data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission or appropriate or suitable safeguards and how to obtain a copy of them;
g) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
h) the rights of the Data Subject;
i) where the Processing is based upon Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal;
j) the right to lodge a complaint with a Supervisory Authority;
k) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract;
l) whether the Data Subject is obliged to provide the Personal Data and of the possible consequence of failure to do so;
m) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and envisaged consequences of such Processing for the Data Subject.

When collecting Personal Data in writing from a Data Subject to whom the information relates, the University may either provide a copy of the University's Privacy Policy to the Data Subject, direct the Data Subject to the Privacy Policy available on the University's website or provide the information orally (where the Data Subject has requested that the University do so).

Please contact Legal Services for more information and/or assistance with creating appropriate Privacy Statements that cover the above information.

Where Personal Data 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, the lawful basis of Processing and the availability of the University's Privacy Policy on the University's website.

5.3 Collecting from a Third Party

When collecting the Personal Data of a Data Subject from a Third Party, the University will provide the Data Subject (to whom the data relates) with the following information in a Privacy Statement in addition to the information outlined in 5.2:

a) The categories of Personal Data concerned; and
b) From which source the Personal Data originates and, if applicable, whether it came from publicly available sources.

However, the University is not required to include in the Privacy Statement provided to the Data Subject the following information from 5.2:

a) Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract; and
b) Whether the Data Subject is obliged to provide the Personal Data and of the possible consequence of the failure to do so.

The University will provide the Data Subject with the above information the earlier of:

a) the first communication with the Data Subject;
b) when the Personal Data is first disclosed to another recipient; or
c) within a reasonable period after obtaining the Personal Data having regard to the specific circumstances in which the Personal Data is being processed (but no later than one month).

The Privacy Statement may be provided in writing (electronic and otherwise) or orally upon request of the Data Subject. However, the University is not required to provide the above information to a Data Subject (when their Personal Data has been collected from a Third Party) where the Data Subject already has the information or the provision of such information proves impossible or would involve a disproportionate effort. For further information, please contact Legal Services.

5.4 Obligation to be transparent

The University shall ensure that the information above under 5.2 and 5.3 of this Appendix is provided to the Data Subject in a concise, transparent, intelligible and easily accessible form using clear and plain language. Such information will also be provided free of charge to the Data Subject.

6. PROCESSING OF PERSONAL DATA

[Privacy Policy principle 6.3]

6.1 General principles of Processing

The University will only process Personal Data where one of the lawful bases of Processing applies as outlined in paragraph 3. At first instance, the University may process the Personal Data for a purpose for which the Personal Data has been collected (as communicated to the Data Subject).

When collecting Personal Data, the University will adhere to the GDPR principles (outlined in paragraph 2) including Processing the Personal Data in a fair and transparent manner (for example, Processing in the manner disclosed to the Data Subject) and Processing the Personal Data in a manner that ensures appropriate security for the Personal Data.

6.2 Processing beyond the purpose for which it was collected

The University must not process Personal Data for a purpose other than what the Personal Data was originally collected for (**additional purpose**) unless:

a) The University obtains Consent from the Data Subject for the additional purpose;

b) The additional purpose is compatible with the purpose for which the Personal Data was initially collected, taking into account:

   i. any link between the original purpose and the additional purpose;
   ii. the context in which the Personal Data was collected, in particular regarding the relationship between the Data Subject and the University;
   iii. the nature of the Personal Data (for example whether the data attracts higher protections under GDPR due to being a special category of Personal Data or criminal convictions and offences);

iv. the possible consequences of the intended further Processing for Data Subjects; and
v. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the additional purpose is compatible, a new lawful basis for the further Processing is not required. However, you should remember that if you originally collected the data on the basis of Consent, you usually need to get fresh Consent to ensure your new Processing is fair and lawful.

c) There is a clear legal provision requiring or allowing the new Processing in the public interest,

Where the University has collected the Personal Data of Data Subjects from third parties, the University may also process such data for an additional purpose. However, prior to doing so, the University is required to provide the Data Subject with information on the additional purpose and with any relevant further information as outlined in sections 5.2 and 5.3 of this Appendix.

6.3 Security of Processing

The University shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. When determining the appropriate level of security, the University shall take into account the state of the art technology, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk posed to the rights and freedoms of natural persons.

When assessing the appropriate level of security to implement, the University shall take into account the risks presented by Processing from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Examples of appropriate technical and organisational security measures to implement include:

a) pseudonymisation and encryption of Personal Data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the Processing systems and services;
c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

Tip: Do the easy things right:

1. double check the recipient of your email;
2. double check that you have attached the right document;
3. double check that attached spreadsheets do not contain extra tabs or hidden columns;
4. keep filing cabinets and offices locked.

6.4 Storage of Personal Data

The University will ensure that all Personal Data stored is accurate and up to date. Where Personal Data is inaccurate or out of date (having regard to the purposes for which it is to be processed), the University will take reasonable steps to erase or rectify the Personal Data without delay.

Please see paragraph 5.1 (Security measures) of this Plan for further information regarding security measures.

6.5 Deletion of Personal Data

The University is obliged to delete Personal Data without undue delay where one of the following grounds applies:

a) When the Personal Data is no longer required for the purposes for which the Personal Data was collected or otherwise processed;
b) the Data Subject withdraws Consent on which the Processing is based and there is no other legal ground for the Processing;
c) the Data Subject objects to the Processing and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing;
d) the Personal Data has been unlawfully processed;
e) the Personal Data has to be deleted to comply with a legal obligation in Union or Member State law that applies to the University; or
f) where the Personal Data relates to a child (15 and under) and the Processing is without the Consent of the holder of parental responsibility over the child.

7. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

[Privacy Policy principle 6.4]

Under the GDPR there is a general prohibition on transfers of Personal Data outside of the EEA unless the transfer is subject to particular conditions and safeguards. These conditions and safeguards are more onerous that those under the Australian Privacy Act.

The University has many arrangements with other institutions and organisations in the EEA and elsewhere in the world. The GDPR does not prevent the University from transferring Personal Data outside of the EEA as part of these activities, but it does require the University to implement the required conditions and safeguards beforehand.

Examples of situations that can give rise to transfers of Personal Data include:

- Sharing Personal Data as part of a collaborative research arrangement
- Using an international cloud-based service such as DropBox to store Personal Data
- A researcher taking Personal Data for a research project from an EEA based institution to the University

University Personnel who are engaging in activities that will involve the transfer of Personal Data from the EEA to Australia or another country outside of the EEA should contact Legal Services to ensure that the appropriate conditions and safeguards are in place for that transfer.

This will generally involve the University putting in place a suitable data protection agreement that has sufficient provisions included for the University to comply with its GDPR obligations, and particular provisions that have been approved by the European Commission.

Terms and conditions that are provided by third parties contracting with the University may not be sufficient for the University to cover off on its obligations under the GDPR or the Australian Privacy Act (see paragraph 3.4 *Disclosure to third parties outside Australia* of this Plan in relation to overseas transfers under the Australian Privacy Act) and should be reviewed by Legal Services.

8. DIRECT MARKETING

Generally, direct marketing will require the Data Subject's Consent. Though depending on the circumstances there may be other grounds upon which the University can process Personal Data for direct marketing.

Under the GDPR the Data Subject has the right to object at any time to the Processing of their Personal Data for direct marketing purposes and upon receipt of the objection, the University will no longer process the Personal Data of that Data Subject for such purposes.

The University will communicate the Data Subject's right to object to the Processing of their Personal Data for direct marketing purposes clearly and explicitly in the first communication the University has with the Data Subject (including the Privacy Policy and Privacy Collection Statement).

University Personnel also need to be aware that there are other European laws that may apply to the University's direct marketing activities in certain circumstances, particularly email and other electronic marketing and use of website cookies.

> Examples of situations where the GDPR and other European laws may apply to the University's direct marketing activities:
>
> - Establishing a webpage that will use cookies to monitor the activities of users who will include users in the EEA
> - Marketing new University courses and services to Data Subjects in the EEA by email

University Personnel should contact Legal Services before establishing websites, webpages or engaging in direct marketing activities directed to Data Subjects who may be in the EEA.

9. RECORDS OF PROCESSING

The University will maintain a record of all Processing activities undertaken by the University (including University Personnel) or within the responsibility of the University. For every Processing activity, the University shall record:

a) the name and contact details of the University and (where applicable) the joint Data Controller, the University's representative and Data Protection Officer;
b) the purposes of Processing;
c) a description of the categories of Data Subjects and of the categories of Personal Data;
d) the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures.

10. RIGHTS OF DATA SUBJECTS

[Privacy Policy principle 6.5]

10.1 Data Subjects exercising their rights

The following applies to Data Subjects exercising their rights:

a) All information provided to the Data Subject, and all communications to the Data Subject, from the University shall be in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The language will be adjusted to the target group.
b) All information and communications from the University to the Data Subject must be in writing or by other means, including where appropriate, by electronic means.
c) The University will respond to a request from a Data Subject exercising their rights without undue delay and in any event, within one month of receipt of the request. If it is necessary to do so, the response period may be extended by a further period (taking into account the complexity and number of the requests). Where an extension is necessary, the University will inform the Data Subject within one month of receipt of the request and provide reasons for the delay.

d) The University will only provide the information requested if the identity of the Data Subject has been properly established. The University may request additional information as a part of this process.

10.2 Right of Access

Data Subjects have the right to obtain access to Personal Data about themselves from the University that originated from the EEA. Data Subjects who request access will be provided with a copy of their Personal Data free of charge. The University may charge a reasonable fee (based on administrative costs) to fulfil any further requests from the Data Subject for copies of their Personal Data.

Upon receiving a query as to whether or not the Personal Data of a Data Subject is being processed by the University, the University shall provide the Data Subject with confirmation either way. Where Personal Data is being processed, the University shall also provide the Data Subject with access to the following information:

a) the purposes of the Processing;
b) the categories of Personal Data concerned;
c) the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations (and the appropriate safeguards in place);
d) where possible, the period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the Data Controller rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing;
f) the right to lodge a complaint with a Supervisory Authority;
g) where the Personal Data are not collected from the Data Subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and likely consequences of such Processing for the Data Subject.

Limitation on access

The right to access should not adversely affect the rights and freedoms of other Data Subjects. Consideration should be given to:

a) the unreasonable impact on the privacy of other individuals (e.g. personally identifying information of referees on a staff appointment file);
b) whether documents are subject to confidentiality obligations or legal professional privilege; and
c) whether documents contain trade secrets, intellectual property or copyright.

The University cannot use the rights and freedoms of others as justification to refuse access to all information. Redaction should be undertaken where appropriate.

> **Tip**: Where a Data Subject exercises their right of access, at first instance an extraction of their Personal Data from the database should be attempted in order to protect the privacy of other Data Subject. Where an extraction is not possible, the Personal Data of other Data Subjects is required to be redacted.

10.3 Right to rectification

Data Subjects have the right to obtain from the University without undue delay the rectification of inaccurate Personal Data concerning themselves.

Where the University has rectified Personal Data at the request of a Data Subject, the University is required to communicate the rectification to each recipient of the Personal Data to who the University disclosed the Personal Data to.

10.4 Right to erasure (right to be forgotten)

Data Subjects have the right to ask for their Personal Data erased where one of the following grounds apply:

a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the Data Subject withdraws Consent on which the Processing is based according to certain requirements[1], and where there is no other legal ground for the Processing;
c) the Data Subject objects to the Processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing pursuant to Article 21(2);
d) the Personal Data have been unlawfully processed;
e) the Personal Data have to be erased for compliance with a legal obligation in Union or Member State law to which the University is subject;
f) the Personal Data have been collected in relation to the offer of information society services referred to in Article 8(1) of GDPR.

In addition to the above requirements, the University is not required to comply with such a request if:

a) the Personal Data the University holds is needed to exercise the right of freedom of expression;
b) there is a legal obligation to keep the Personal Data;
c) for reasons of public interest (for example public health, scientific, statistical or historical research purposes).

Where one of the grounds set out in (a)-(f) applies, at the request of the Data Subject, the University is required to erase the Personal Data concerning the Data Subject without undue delay. This includes taking reasonable steps to pass on the request to the recipients of the Personal Data to whom the University disclosed the Personal Data to.

With regard to the right to be forgotten online, the University is expected to take reasonable steps (for example technical measures) to inform other websites that a particular individual has requested the erasure of their Personal Data.

Data can also be kept if it has undergone an appropriate process of anonymisation (e.g. the Data Subject concerned is no longer identifiable by any means).

> **Tip:** Generally, the right to erasure requires that the Personal Data of the requesting Data Subject is deleted from all storage devices to the extent that it is no longer accessible by the University.

10.5 Right to restriction of Processing

The Data Subject has the right to require the University to restrict the Processing of their Personal Data in particular circumstances. Where such a request has been made, the University is required to communicate the restriction of the Processing to each recipient of the Personal Data to whom the University disclosed the Personal Data to. Please contact Legal Services for more information.

10.6 Right to data portability

The Data Subject has the right to receive from the University the Personal Data about themselves that the Data Subject provided to the University. The Personal Data shall be provided to the Data

[1] GDPR point (a) of Article 6(1), or point (a) of Article 9(2)

Subject in a structured, commonly used and machine-readable format and the University will not hinder the transmission of such data to an entity other than the University.

This right arises where the Processing of the Personal Data is based on the legal grounds of Consent or contract and Processing is by automated means. Consequently, this right generally does not cover paper files.

The University's compliance with this right shall not adversely affect the rights and freedoms of others.

10.7 Right to object

The Data Subject has the right to object to the Processing of their Personal Data. This right arises only where the Processing of the Personal Data is based upon the legal grounds of public interest and the legitimate interests of the University (including any profiling based on these legal grounds).

Upon receiving an objection from the Data Subject, the University shall no longer process the Personal Data unless the University can demonstrate compelling legitimate grounds for the Processing which overrides the interests, rights and freedoms of the Data Subject.

The University will communicate the Data Subject's right to object to the Processing of their Personal Data on the grounds of public interest and the legitimate interests of the University clearly and explicitly in the first communication the University has with the Data Subject (including the Privacy Policy if applicable).

10.8 Automated individual decision-making

The Data Subject has the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects or significantly affects the Data Subject.

This right shall not apply if the decision is necessary for entering into, or performance of, a contract between the Data Subject and the University, is authorised by Union or Member State law to which the University is subject, or is based on the Data Subject's explicit Consent.

> **Be Aware:** For research, there are a number of exemptions to these rights and the lawful basis used affects the rights people have, therefore you should seek advice if a research participant wishes to exercise one of their rights.

11. PERSONAL DATA BREACH

[Privacy Policy principle 7.1]

If there is a Personal Data Breach the University may have an obligation to notify the relevant Supervisory Authority and may have an obligation to notify affect individuals.

The threshold to report a Personal Data Breach is lower that the threshold to report a data breach under the Australian Privacy Law. The University also has a much shorter time period in which to notify the relevant authority. The University has a Data Breach Response Plan which sets out procedures if a University Personnel becomes aware of an actual or suspected Personal Data Breach which includes requirements under GDPR.

See section 8 (*Data Breach*) in the main section of the Plan for more information.