



[Overview](#)

[Scope and Application](#)

[Policy Principles](#)

1. [Collection of Personal Information](#)
2. [Use and Disclosure](#)
3. [Management of Personal Information](#)
4. [Access to and Correction of Personal Information](#)
5. [Breaches and Complaints](#)

[Procedures](#)

[Definitions](#)

[Appendix 1](#)

OVERVIEW

The University respects the privacy of individuals and is committed to the collection, use, disclosure and management of, and provision of access to, Personal Information in a manner consistent with the standards contained in the Commonwealth *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles.

SCOPE AND APPLICATION

This Policy applies to all areas of the University and all University activities. All employees, titleholders, volunteers, consultants, contractors and agents of the University must comply with this Policy and the [Privacy Management Plan](#) when collecting Personal Information on the University's behalf and when using or dealing with Personal Information in the University's possession. Failure to comply with this Policy or the Privacy Management Plan may constitute misconduct and may result in disciplinary action being taken by the University.

POLICY PRINCIPLES

The University's approach to collection of Personal Information

1. The University will not collect Personal Information unless the information is reasonably necessary, or directly related to, one or more of the University's functions or activities.
2. The University will not collect Sensitive Information unless:
 - (i) with the individual's consent; or
 - (ii) if required or authorised by Australian law or court/tribunal order; or
 - (iii) an exemption exists under the Privacy Act.
3. The University will collect Personal Information by lawful and fair means and, where possible, directly from the individual. The University collects Personal Information in a number of ways including:
 - (i) from correspondence and submitted forms (including via on-line portals);
 - (ii) as part of any enrolment, registration or subscription process;
 - (iii) in the course of undertaking research;
 - (iv) direct contact in the course of providing services or administration of University activities;
 - (v) from third parties with which the University collaborates;
 - (vi) monitoring and logging of metadata from individuals' use of IT and online services and facilities provided by the University;
 - (vii) from CCTV cameras on University premises.
4. Personal Information collected by the University may be held in hardcopy format, or electronic format stored on the University's computing equipment or on third party servers.
5. At or before the time (or, if that is not practicable, as soon as practicable after) the University collects Personal Information about an individual, the University will take reasonable steps to provide a Privacy Statement to the individual.

-
6. If the University receives unsolicited Personal Information, and the University has no lawful basis on which to retain the information, the University will destroy that information or ensure that it is de-identified.
 7. The University will provide individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with the University, except where:
 - (i) the University is required or authorised by Australian law or a court/tribunal order, to deal with individuals who have identified themselves; or
 - (ii) it is impracticable for the University to deal with individuals who have not identified themselves or who have used a pseudonym.

How the University may use and disclose Personal Information

8. The purposes for which the University collects, uses and discloses Personal Information will vary depending on the nature of the association between the individual and the University.

(i) Personal Information of students

The University may use this information in assessing admission applications; administration of a student's course of study (including enrolment, scholarships, prizes, timetabling, visa requirements); delivery of teaching, educational resources, email and other services related to the student's enrolment at the University; monitoring a student's progress in their course of study; fulfilling external reporting requirements; internal planning, improvement and development; management of health, safety and wellbeing; communicating to students about the University and other parties or activities relevant to the student's course of study; administering University Council electoral rolls.

Personal information of students will be collected, used and managed in accordance with the [Student Privacy Statement](#).

Photographs of students taken in the course of a University activity may be published by the University for informational, marketing and promotional purposes.

(ii) Personal Information of prospective students

The University may use this information to provide prospective students with information about the University; assess admission applications; undertake internal planning, improvement and development.

(iii) Personal Information of employees, job applicants, contractors, volunteers or titleholders

The University may use this information in assessing applications; administration and management of the employee, contractor, volunteer or titleholder; management of health, safety and wellbeing; fulfilling external reporting requirements; internal planning, improvement and development; creating a publicly available University staff contact directory; administering University Council electoral rolls.

In the case of employees and applicants who agree to be added to the University's recruitment database, the information may be used for follow up contact for future job vacancies.

University personnel names and expertise, and photographs of University personnel taken in the course of a University activity may be published by the University for informational, marketing and promotional purposes.

(iv) Personal Information of alumni and donors

The University may use this information to maintain communication and promote University activities and events; undertake fundraising; publicly acknowledge donors (unless otherwise requested by the donor); administer University Council electoral rolls; internal planning, improvement and development; profile building to evaluate prospective donors.

The names of all graduates and their conferred awards will be published in graduation booklets. The University may confirm a person's graduate status in response to inquiries from third parties.

(v) Personal Information of research participants

Subject to any human research ethics committee restrictions, the University may use this information for research purposes; follow up contact for future related projects.

-
- (vi) *Personal Information of clients of health or counselling services offered by the University*
The University uses this information to provide health or counselling services. In the case of students who use Disability Services, Personal Information (including health information) will be used to assess and respond to requests by the student for additional support or adjustments.
- (vii) *Personal Information of customers, users or attendees of University facilities, services, events or activities*
The University may use this information for the provision of the facilities or services; administration and monitoring of the use of or attendance at such facilities, services, events or activities; internal planning, improvement and development; ensuring the security of University facilities or premises; promoting other University events or activities
9. If the University collects or discloses Personal Information other than for those purposes stated above, such other purposes will be notified to the individual in a Privacy Statement.
10. Other than the purposes stated in this Policy or in a Privacy Statement, the University will only use or disclose Personal Information for purposes which are in reasonable contemplation or are permitted under the Privacy Act.
11. The University may disclose Personal Information to the following types of third parties:
- (i) Government departments and agencies to satisfy reporting requirements;
 - (ii) 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;
 - (iii) external service providers, to the extent such Personal Information is required for the service provider to provide services to or on behalf the University (e.g. mailing house services; email services; externally hosted software and databases; surveys); and
 - (iv) collaborating parties, to the extent such Personal Information is required for the collaborative activity to be undertaken (e.g. collaborative research; jointly delivered courses or programs; student exchange; vocational placements).
12. Some third parties to whom the University discloses Personal Information may be located outside of Australia. Appendix 1 to this Policy lists the countries in which recipients of the disclosed Personal Information may be located.
13. If the University discloses Personal Information to an overseas recipient, the University will:
- (i) enter into a contract with the overseas recipient that binds the overseas recipient to privacy obligations that are consistent with the Australian Privacy Principles; or
 - (ii) ensure that 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
 - (iii) obtain express consent of the individual to the disclosure of their Personal Information to the overseas entity.
14. The University will not use Personal Information for the purpose of direct marketing unless such use is contemplated under Policy Principle 8(i) or the University has obtained consent from the individual. The area of the University issuing the direct marketing will ensure the direct marketing communication contains a simple means by which the individual may easily opt out of receiving direct marketing communications from that area of the University.

How the University will manage Personal Information

15. The University will take such steps as are reasonable in the circumstances to:
- (i) ensure that Personal Information it collects is accurate, up-to-date and complete;
 - (ii) ensure that Personal Information the University uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant;
 - (iii) protect Personal Information in its possession from misuse, interference, loss, and unauthorised access, modification or disclosure;
 - (iv) destroy or de-identify Personal Information if the Personal Information is no longer needed or required to be retained under any law, regulation or code applicable to the University.
16. For any new project or activity that may involve collection or handling of Personal Information, or when contemplating any changes to existing practices to the collection or handling of Personal Information, University Personnel must take privacy considerations into account in the risk assessment for that project or activity as set out in the [Privacy Management Plan](#).

How individuals may seek access to or correction of Personal Information

17. The University will, upon request by an individual, give the individual access to Personal Information about them held by the University, unless the University has a legitimate reason for refusal.
18. The procedure for employees, titleholders and students to request access is set out in the Privacy Management Plan.
19. Other individuals may request access to Personal Information about themselves held by the University by contacting the Freedom of Information Officer, The University of Adelaide, South Australia 5005 or email to foi@adelaide.edu.au. In some cases, the Freedom of Information Officer may request that individual submits a formal application under the Freedom of Information Act 1991 (SA).
20. The University encourages University Personnel, students and other individuals with whom the University has regular dealings to notify the University of any changes to their Personal Information. If individuals do not disclose changes or update their Personal Information, this may affect the University's ability to administer records or provide services for those individuals.
21. The University encourages employees, students and alumni to use self-serve systems provided by the University (e.g. Staff Services Online, Access Adelaide, online Alumni community) to update their Personal Information. Individuals may also submit requests to the University to correct or update Personal Information about them held by the University by contacting:

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

22. The University will respond to requests for correction within a reasonable period after the request is made and will not impose any charges for the request. If the University refuses to make the requested correction, the University will provide the individual with a written notice setting out the reasons for refusal. Individuals who are dissatisfied with the decision may apply in writing for a review. Requests for review will be referred to the relevant Deputy Vice-Chancellor or Vice-President.

Breaches and Complaints

23. University Personnel who become aware of any actual or suspected loss or unauthorised access, use, modification, disclosure or other misuse of Personal Information ("data breach") must follow the data breach procedures contained in the [Data Breach Response Plan](#) referred to in the [Privacy Management Plan](#). A Data Breach Response Group will be established for the purposes of responding to data breaches.
24. If an individual believes that their Personal Information has not been handled by the University in accordance with this Policy, the individual may make a complaint in writing or by email to:

Manager, Compliance
Legal and Risk
The University of Adelaide
SA 5005
email: helpdesklegal@adelaide.edu.au
25. In order to enable prompt processing, individuals are encouraged to lodge complaints within six months of the individual becoming aware of the conduct the subject of the complaint.
26. Complaints will be processed in a reasonable time (usually 30 days from the date on which the complaint was received). Individuals will be advised in writing of the University's decision and any action taken.

27. Staff or students of the University who are dissatisfied with the decision or action taken pursuant to Policy Principle 026 may lodge a further complaint under the Complaints by Staff Policy & Procedure or Student Grievance Resolution Process respectively.
28. The University will comply with any applicable mandatory data breach notification requirements.

Authorities

Key	Authority Category	Authority	Delegation Holder	Limits
Information Management	Personal Information	Review refusal to make corrections to Personal Information	Deputy Vice-Chancellor / Vice-President	

PROCEDURES

Responsibility: All University Personnel

The Privacy Management Plan contains procedures and guidelines on how these Policy principles should be applied. All University Personnel must comply with the Privacy Management Plan.

DEFINITIONS

Australian Privacy Principles are contained in the Privacy Act.

Controlled Entity has the same meaning as in the University's *University-Owned Entities Policy*.

Personal Information is defined in the *Privacy Act 1988* (Cth) 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 Act means the *Privacy Act 1988* (Cth).

Privacy Statement means a notification to an individual at or before the time (or, if that is not practicable, as soon as practicable after) the University collects Personal Information, that addresses the following points, as are reasonable in the circumstances:

- a. the full name of the University and the contact details of the area of the University responsible for the collection of the individual's Personal Information;
- b. the purposes for which the individual's Personal Information is collected;
- c. any law that requires the individual's Personal Information to be collected;
- d. any third parties to which the University may disclose the individual's Personal Information and whether any such party is located overseas;
- e. any consequences for the individual if all or part of the Personal Information is not provided;
- f. that the University's Privacy Policy is available on the University's website.

Sensitive Information is defined in the *Privacy Act 1988* (Cth) 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 employees, titleholders, consultants, contractors and volunteers.

APPENDIX 1

Locations of overseas recipients of Personal Information (refer Policy

Principle 2(b))

United States of America

Canada

United Kingdom

European Union

Singapore

Hong Kong

RMO File/Document Number	2017/3065
Policy Custodian	Chief Operating Officer
Responsible Officer	General Counsel
Endorsed by	Vice-Chancellor's Executive on 5 July 2017
Approved by	Interim Vice-Chancellor and President 17 July 2017
Related Documents and Policies	Privacy Management Plan Records Management Policy Freedom of Information Policy IT Acceptable Use and Security Policy Responsible Conduct of Research Policy Managing Customer / Student Credit / Debit Card Data Procedures (under Financial Management Policy) Student Privacy Statement Data Breach Response Plan
Related Legislation	Privacy Act 1988 (Cth) South Australian Cabinet Administrative Instruction 1/89 (Information Privacy Principles Instruction) <i>Higher Education Support Act 2003</i> (Cth) Privacy (Tax File Number) Rule 2015 (Cth) Telecommunications (Interception and Access) Act 1979 Freedom of Information Act 1991 (SA)
Superseded Policies	None
Date Effective	17 July 2017
Next Review Date	17 July 2020
Contact for queries about the Policy	Contact Legal and Risk Branch by email: helpdesklegal@adelaide.edu.au