THE UNIVERSITY of ADELAIDE

Privacy Policy

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. The University is also committed to comply with the requirements of applicable privacy laws in other jurisdictions including Regulation EU (2016/679)–General Data Protection Regulation ("**GDPR**") regarding individuals located in the European Union (including the European Economic Area).

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.

If an individual does not agree with any part of this Policy then Personal Information should not be provided to the University. However the University's ability to provide services may be affected if Personal Information is not provided, or if any consent is withdrawn that is legally required by the University in order to process the Personal Information provided.

POLICY PRINCIPLES

1. The University's collection of Personal Information

1.1. The University collects Personal Information that is reasonably necessary for one or more of the University's functions or activities.

1.2. The University will collect Sensitive Information only:
- (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.

1.3. 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 but not limited to:

(i) from correspondence and submitted forms (including via online 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 and events;
(v) in the course of recruitment and appointment processes;
(vi) from third parties with which the University collaborates;
(vii) from third parties whom you have authorised to provide us with information, such as SATAC;
(viii) monitoring and logging of metadata from individuals' use of IT and online services and facilities provided by the University;
(ix) from CCTV cameras on University premises;
(x) from publicly available sources, such as webpages, databases, social media and publications.

1.4. At the time the University collects Personal Information (or, if not practicable, as soon as practicable afterwards), the University will take reasonable steps to provide a Privacy Statement to the individual.

1.5. If the University receives unsolicited Personal Information, the University will determine whether there is a lawful basis to retain the information (in full or in de-identified form) or if it should be destroyed.

1.6. 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.

2. How the University may use Personal Information

2.1. The University may use Personal Information for many different purposes depending on the nature of the association between the individual and the University including but not limited to:

(i) Personal Information of students
The Personal information of students will be collected, used, disclosed and managed in accordance with the Student Privacy Statement.

(ii) Personal Information of prospective students
The University may use this information to provide prospective students with information and marketing material about the University; assess admission applications; respond to enquiries; undertake internal planning, improvement and development; complaints handling; assess education agent performance.

(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.

If employees and applicants 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 and related purposes, including 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 reasonable 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.

(viii) *People who enter University grounds/premises*
All individuals entering the University's grounds/premises should expect Personal Information in their images will be captured by CCTV cameras. If individuals enter the University grounds by vehicle, the Personal Information collected includes the vehicle registration details.

CCTV images are recorded to facilitate the safety and security of the University and members of the University community; for investigative and legal purposes; and for planning purposes,

CCTV images may be released to third parties including organisations and law enforcement bodies in accordance with this Policy, the Privacy Management Plan and the University of Adelaide Security Services CCTV Guidelines.

(ix) *University website users*
The University may use this information to improve user experience on the website, analyse website traffic and usage to improve website service, re-targeting, and to provide services, in accordance with the Privacy Statement available on the University website (https://www.adelaide.edu.au/legals/privacy)

3. How the University may disclose Personal Information

3.1. The University may disclose Personal Information to the following types of third parties:

(i) Government departments and agencies to satisfy reporting requirements;
(ii) Regulators and law enforcement bodies for the purpose of conducting investigations and enforcement related activities;
(iii) 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;
(iv) 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
(v) 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);
(vi) third parties impacted by investigations into student 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;
(vii) third parties impacted by investigations into research integrity complaints, such as research publishers, funding bodies, and affiliated organisations in accordance with the Research Misconduct Procedure;
(viii) Adelaide University, as the future successor of the University by operation of the *Adelaide University Act 2023*, for purposes related to the transition of the University to Adelaide University;
(ix) as required or authorised by Australian law or court/tribunal order.

3.2. Some third parties to whom the University discloses Personal Information may be located outside of Australia, most commonly USA, Canada, UK, European Union, Singapore and Hong Kong.

3.3. 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 and/or other applicable privacy laws; 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.

3.4. The University will not use Personal Information for the purpose of direct marketing unless such use is contemplated under this Policy, the Privacy Management Plan, a Privacy Statement, or the University has obtained consent from the individual, the use is permitted by the Privacy Act, or is required or authorised by law. 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.

4. How the University manages Personal Information

4.1. 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.

4.2. Other than the purposes stated in this Policy, the Privacy Management Plan 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.

4.3. 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.

4.4. 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.

4.5. 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 by undertaking a privacy impact assessment as set out in the Privacy Management Plan.

5. How individuals may seek access to or correction of Personal Information

5.1. 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.

5.2. The procedure for employees, titleholders and students to request access is set out in the Privacy Management Plan.

5.3. Individuals may also 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).

5.4. The University relies on and 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.

5.5. The University encourages Personnel, 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

5.6. 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 & Vice-President.

6. European Union – General Data Protection Regulations (GDPR)

6.1. Where the University handles Personal Information from individuals located in the European Union the Personal Information will be subject to the GDPR and the following provisions apply.

6.2. **Lawful bases:** The University will rely on the following lawful bases for processing the Personal Information:

(i) if it is necessary to pursue the University's legitimate interests and does not override the individuals' rights and interests;
(ii) it is necessary to enter into a contract with the individual or to perform obligations under a contract to which the individual is a party;
(iii) with the consent of the individual; and/or
(iv) to comply with applicable laws.

6.3. **External data processors:** If the University engages an external service provider to process Personal Information on the University's behalf, it will only do so if that data processor has provided the University with sufficient guarantees that it will implement appropriate technical, contractual and organisational measures that ensure compliance with the GDPR, and the protection of the Personal Information. The University will ensure that it enters into a written agreement with external data processors which record the data protection obligations.

6.4. **Overseas disclosures:** If the University or external service providers or one of the University's Controlled Entities transfers Personal Information outside the European Union or onwards to a country outside of Australia, the University will ensure that the Personal Information protected and transferred in a manner consistent with the GDPR.

6.5. **Additional rights of individuals:** In addition to the other rights of individuals under this Policy, an individual located in the European Union has the following rights in certain circumstances:

(i) Erasure of their Personal Information;
(ii) Restrictions on processing of their Personal Information;
(iii) Receive Personal Information in a structured, commonly used and machine-readable format and/or having the University transmit it to someone else if technically feasible (data portability);
(iv) Object to the processing of their Personal Information;
(v) Complain to the relevant European data protection authority if the individual thinks any of their rights have been infringed by the University.

6.6. For the purposes of GDPR the University's Data Protection Officer is the General Counsel, Legal Services.

7. Breaches

7.1. 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. The University will comply with mandatory data breach notification requirements.

8. Complaints

8.1. 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, Audit & Compliance
Risk Services Branch
The University of Adelaide SA 5005
email: legalcompliance@adelaide.edu.au

8.2. 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.

8.3. 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.

8.4. Staff or students of the University who are dissatisfied with the decision or action taken pursuant to Policy Principle 8.3 may lodge a further complaint under the relevant staff or student complaint process.

8.5. The University will comply with any applicable mandatory data breach notification requirements.

9. Authorities

Key	***Authority Category***	***Authority***	***Delegation Holder***	***Limits***
Information Management	Personal Information	Review refusal to make corrections to Personal Information	Chief Operating Officer 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.

Responsibility: Personal Information Stewards

(i) Manage local area Personal Information relevant to its activities;
(ii) Ensure the local area has appropriate Privacy Statements available to inform individuals who providing Personal Information about how their Personal Information will be handled;
(iii) Accountable for implementing and complying with this Policy and the Procedures;
(iv) Promote privacy awareness and requirements for their local area;
(v) Report privacy related issues to Heads of School/Branch and Executive Directors.

Responsibility: Heads of School/Branch and Executive Directors

(i) Promote, at the local level, an organisational culture that values and manages Personal information as an important asset and an enabler of University business;
(ii) Nominate a Personal Information Steward in their local area considering who has responsibility for the business systems used to manage Personal Information;

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 means 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 (e.g. IP address)
p. metadata from use of online services and facilities (e.g. cookie identifiers)
q. records of donations and transactions

Personal Information Steward means University Personnel nominated by their local area Head of School / Branch or Executive Director to be responsible for the management of local area Personal Information relevant to its operational purpose.

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 means:

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.

RMO File/Document Number	2022/6252
Policy Custodian	Chief Operating Officer
Responsible Officer	General Counsel and Executive Director, Legal Services Branch
Endorsed by	Vice-Chancellor's Executive on 20 March 2024
Approved by	Vice-Chancellor and President on 22 April 2024
Related Documents and Policies	Privacy Management Plan Student Privacy Statement Data Breach Response Plan Information Management Policy Freedom of Information Policy IT Acceptable Use and Security Policy Responsible Conduct of Research Policy & related procedures Managing Customer / Student Credit / Debit Card Data Procedures (under Financial Management Policy) University Security Services CCTV Guidelines University website Privacy Statement
Related Legislation	Privacy Act 1988 (Cth) South Australian Cabinet Administrative Instruction 1/89 (Information Privacy Principles Instruction) *Higher Education Support Act 2003* (Cth) Privacy (Tax File Number) Rule 2015 (Cth) Telecommunications (Interception and Access) Act 1979 Freedom of Information Act 1991 (SA) Regulation (2016/679) EU General Data Protection Regulations
Superseded Policies	Privacy Policy Version: D2018/130893
Date Effective	22 April 2024
Next Review Date	21 April 2027
Contact for queries about the Policy	Contact Legal Services Branch by email: helpdesklegal@adelaide.edu.au