Privacy Policy

Table of Contents

1. Purpose

a. The purpose of this policy is to support the University's commitment to the protection of the privacy of individuals' personal information, by stating the ways in which the University may collect, store, use, manage and protect personal information.

b. The University's commitment is as follows:

i. To apply best practice to the protection of individuals' privacy by:

- upholding the Australian Privacy Principles (APPs) as set out in the Privacy Act 1988 (Cth) (though neither this Act nor any State privacy legislation actually binds the University), and
- applying substantially the same processes and thresholds to data breaches as if it were bound by the Privacy Act.

ii. To comply with the requirements of Regulation EU (2016/679)–General Data Protection Regulation (GDPR) in respect of individuals located in the European Economic Area to the extent applicable to the University.

2. Scope

a. This policy is relevant to **any individual** who discloses personal information to the University, whether they are a part of the University community or any member of the public worldwide.

i. If you do not agree with any part of this policy, we recommend that you do not provide your personal information to us. However, our ability to provide services to you may be affected if you do not provide us with your personal information, or if you withdraw any consent we are legally required to have in order to process the personal information you have given us.

ii. For individual **students** who provide personal information to the University**,** this policy is supported by the Student Information Management Procedures.

b. This policy applies to all members of the University community who access, use, or deal with personal information on the University's behalf or possession, or handle questions or complaints about personal information, in the course of the University's activities.

3. Definitions

personal information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not, or as otherwise defined by applicable data protection laws
sensitive information	any personal information that is about a person's a. health, health treatment, or other medical needs b. race, ethnicity or religion c. professional or political affiliations and memberships d. criminal record e. sexuality f. disability status g. religious or philosophical beliefs h. trade union membership, or i. genetic or biometric data.
University community	For the purposes of this policy, University community includes: a. enrolled Flinders students, including cross-institutional students and students on exchange from another institution b. employees and exchange staff c. employees of controlled entities, Centres and Institutes, and affiliated clubs and associations d. contractors and consultants performing work on University sites or on behalf of the University e. visiting academics or persons with academic status f. the Council and its committees, and g. any volunteer in the workplace and study environment.
we (us, our, ours)	Flinders University
you (your, yours)	Any individual who discloses personal information to the University

4. Privacy Framework

a. The Privacy Framework is the mechanism by which the University implements its commitments to the privacy of individuals' personal information.

b. It includes the following elements:

i. this Privacy Policy

ii. the Student Information Management Procedures, setting out the processes for the collection, storage, use, management, protection and disclosure of student information

iii. the Personal Information Protection Procedures, setting out the processes for staff to follow so that the University can honour its commitments

iv. a Quick Guide to Privacy Management, for use by staff in support of the Personal Information Protection Procedures

v. the Personal Information Access Procedures, setting out the processes for individuals to access and correct their personal information, and

vi. internal business process documents within the office of the University's Privacy Officer, setting out the process for investigating and responding to unauthorised use or disclosure of personal information.

5. Kinds of personal information we collect

a. We might collect and hold different personal information depending upon how an individual interacts with us. For example:

i. if you access our website, we may collect information about how you have used our website, or

ii. if you contact us for any reason, we may collect your name, address, email address, phone number or contact details.

b. We may also collect information about:

i. your demographic
ii. your participation in research projects
iii. your studies and academic career, including teaching and learning interactions
iv. your grades and course feedback
v. your enrolments
vi. your preferences or opinions
vii. police checks, e.g., if required for your course of study
viii. your transactions with us
ix. your bank account details and financial records with us
x. your tax file number
xi. your records of donations
xii. your photograph or video recording (e.g., identity card, lecture capture, CCTV footage)
xiii. your vehicle registration and contact details
xiv. your health and your Medicare number
xv. the frequency of your enquiries
xvi. your location and your access to, and use of, our equipment and infrastructure (such as IT networks)
xvii. your employment status, professional history and reference check information
xviii. other information relating to your employment with Flinders
xix. the technology you use to access our services
xx. how and when you use our services, and
xxi. sensitive information.

6. Collecting personal information

a. We may collect personal information:

i. directly from you (e.g., when we contact you, when you contact us, when you enrol as a student, when you visit us or when we visit your premises, or when you participate in a research project, complete a survey or enter a competition)

ii. from third parties whom you have authorised to provide us with information

iii. from third parties who provide services to us or organisations of which we are a member, e.g., SATAC

iv. from third parties and publicly available sources, such as public web pages, published databases, social media and publications

v. from CCTV footage operated by us on or around our premises

vi. via routine monitoring of our information technology and telephone networks

vii. from audio and video recordings in public locations and other spaces identified as being subject to recording devices, or

viii. where generated by us in the course of our business activities (e.g., assessment results, grades or your Flinders Authentication Number).

b. We do not collect sensitive information, unless you consent to its collection and the information is reasonably necessary for our business or activities or the collection of sensitive information is otherwise permitted by the relevant privacy laws (for example it is required or authorised by law). By supplying us with sensitive information, unless you state otherwise, you consent to our collection and handling of that information in any of the ways and for any of the purposes described in this policy.

7. Holding and securing personal information

a. We may store your personal information in both hard copy format, digitally, on site and/orwith several third party providers. Generally, all hard copy material is secured using locked filing cabinets or office security and all digital material is secured using file access controls.

b. We use digital data storage providers located inside Australia and in the following countries:

i. United States

ii. Canada

iii. Singapore

iv. United Kingdom (and European Union).

c. We have agreements with our digital data storage providers to ensure the protection of personal information they store. Arrangements with these providers are reviewed and assessed periodically. Additional requirements apply in respect of individuals located in the European Union, as described in section 11.

d. We only keep your personal information for as long as it is required for the purpose for which it may be used or disclosed or as otherwise required by law. If we no longer need to hold your personal information for any reason, we will take reasonable steps to de-identify or destroy that information. These steps may vary depending on the nature of the information, the way it was collected and how it was stored.

8. Reasons for collecting, holding, using and disclosing personal information

a. We may collect, use and disclose personal information for a number of purposes, including:

i. providing you with goods or services, including processing payments
ii. providing you with information about our goods and services, our teaching and research activities, and other initiatives
iii. developing or refining our services, including for analysing, understanding and optimizing learning and educational outcomes
iv. internal business and administrative purposes (such as training staff, risk management; developing and marketing products and services, undertaking planning, research and statistical analysis)
v. providing you with marketing and fundraising material, and communicating with you generally
vi. providing information to prospective, current and former students and applicants about Flinders' courses, activities and programs

vii. better understanding your needs, including by engaging with you about your studies and providing you with information about any educational, recreational or support services, resources or programs that may be of interest to you
viii. tailoring our marketing, services, promotions, publicity, philanthropic activities, and other operations for you
ix. student retention initiatives
x. assessing your application for a role with us and taking references
xi. organising external activities related to your study, including Work Integrated Learning, study abroad and study exchanges
xii. confirming that you meet registration and/or accreditation requirements with external professional registration or accreditation bodies
xiii. reporting to Government agencies as required by law or Government policy
xiv. for your visa or immigration application and associated reporting obligations
xv. for performance review and assessment purposes
xvi. for the investigation of a complaint or allegation made by or against you
xvii. responding to, investigating and managing inquiries, complaints, feedback and claims
xviii. responding to legitimate inquiries from government agencies, including law enforcement agencies, upon request
xix. corporate governance, auditing and record keeping
xx. any other reason disclosed to you at the time of collection
xxi. to comply with other legal obligations, or
xxii. as otherwise permitted by privacy laws.

b. If we collect personal information from you, we may:

i. use and disclose that information, including to a third party, for any of the purposes outlined in section 8.a. This may include transferring your personal information to an overseas recipient as described in section 7.b.
ii. store that information in accordance with this policy
iii. pass that information amongst entities we work with
iv. disclose that information to third parties who provide products or services to us (including our accountants, auditors, lawyers, IT contractors, advertising and marketing providers, education providers, and other service providers)
v. pass that information to your home or host institution overseas, if you are involved in a mobility, exchange, cross-institutional or joint program
vi. provide that information to third parties as required by law and to law enforcement agencies upon receipt of an official request
vii. publish photographs of you that have been taken in the course of a University activity for informational, marketing and promotional purposes,
viii. ask you from time to time to confirm that the information is accurate, up-to-date, complete and relevant, or
ix. otherwise disclose the information as required or authorised by law.

c. Our use of personal information may extend beyond these uses, but will be restricted to purposes that we consider to be related to our functions and activities.

9. Direct marketing

a. We may use and disclose your personal information to identify a product or service that you may be interested in or to contact you about an event, important initiative, or fundraising activity. We may use and disclose your phone number, email address, mailing address and other contact details to contact

you from time to time to tell you about products or service offerings that we believe may be of interest to you.

b. In the event that you do not wish to receive marketing communications of this nature from us, you may at any time, unsubscribe from the mailing list, by contacting us at the details at the end of this policy, or by using the opt out mechanism in our marketing communications.

10. European Union – additional provisions

a. In addition to the protections given to you under this policy, if you are an individual located in the European Union (**EU**) (including the European Economic Area (**EEA**) and we offer or provide our products or services to you, your personal information will be subject to Regulation EU (2016/679)– General Data Protection Regulation (GDPR) and the following provisions apply.

b. Flinders University is the data controller for the purposes of processing your personal information.

c. Our Privacy Officer (see section 13) is our Data Protection Officer for the purposes of the GDPR.

d. **Legal grounds for processing**: We rely on the following legal grounds to process your personal information:

   i. *contract performance* – we may collect and process your personal information to enter into a contract with you or to perform our obligations under a contract to which you are a party

   ii. *if it is necessary to pursue our legitimate interests and does not override your rights and interests* – this is the usual basis on which we carry out our business for the purposes set out above and includes when we carry out research, conduct direct marketing or otherwise communicate with you

   iii. *with your consent* – where required, we will only use your personal information for the purposes for which you have given your valid or explicit consent. For instance, we need your consent to collect and use your sensitive information or to send you direct marketing, and

   iv. *to comply with laws that apply to us including exercising our rights* – we may use and process your personal information where we are legally required to do so.

e. **Transfer of information outside Europe**: If we or our service providers or one of our controlled entities transfers your personal information outside the European Union or onwards to a third country from Australia, we will ensure that it is protected and transferred in a manner consistent with the GDPR. We will do this by:

   i. sending it to a recipient in a country approved by the European Commission as having an adequate level of protection for personal information, or

   ii. sending it to a recipient which has signed a contract, based on standard "model contractual clauses" approved by the European Commission, requiring it to protect your personal information, or

   iii. sending it to a recipient located in the US, if they are a certified member of the EU-US Privacy Shield scheme or another valid scheme, or

   iv. obtaining your explicit and informed consent to the proposed transfer.

f. **Time we retain your personal information for:** We retain your personal information for as long as necessary to provide our services and products that you have requested, comply with our legal obligations, resolve disputes, and enforce our rights and policies.

g. **Your additional rights and choices:** In addition to the above, an individual located in the European Union has the following rights:

i. **Erasure:** You can ask us to erase your personal information without undue delay in certain circumstances such as if you withdraw your consent and we otherwise have no legal reason to retain it.

ii. **Restrictions of processing:** You can object to, and ask us to restrict, our processing of your personal information in certain circumstances, such as while we verify your assertion the information is inaccurate or if we are processing your information for our legitimate interests or for direct marketing purposes (we may be legally entitled to refuse that request).

iii. **Data portability:** You can, in some circumstances such as where we are processing your information with your consent, receive some personal information you have given us in a structured, commonly used and machine-readable format and/or ask us to transmit it to someone else if technically possible feasible.

iv. **Right to object:** You can withdraw your consent (but we may be able to continue processing without your consent if there is another legitimate reason to do so).

v. **Right to complain:** You can lodge a complaint with the relevant European data protection authority if you think that any of your rights have been infringed by us.

h. If we refuse any request you make in relation to your personal information rights, we will write to you to explain why and how you can make a complaint about our decision.

11. Accessing or correcting personal information

a. In most cases you can gain access to your personal information held by us. You are encouraged to use the University's self-service systems, where available, to access, correct, or update your personal information.

b. You may otherwise request access or correction to the personal information that we hold about you by contacting the following areas:

Person making the request	Submit to:
Alumni or donor	Alumni and Advancement
Research participant	the relevant researcher
Student	Flinders Connect
Staff	People & Culture
Not listed above	the area which holds your personal information.

c. We will respond to your access or correction request within 30 days.

d. An administrative fee may be charged to cover our costs in providing you with access to your personal information. This fee will be explained to you before it is incurred.

e. If we deny your access or correction request, we will provide you with reasons.

f. If we refuse to correct your personal information, you can ask us to attach a statement to it stating that you believe the information is incorrect and why.

g. In some cases, you may be asked to submit a formal application under the Freedom of Information Act 1991 (SA) in order for us to process your request.

12. Questions or complaints

a. The General Counsel and University Secretary, Governance, Legal & Risk is the University's Privacy Officer, responsible for promoting awareness of this policy and for ensuring we comply with this policy and any applicable laws about the protection of personal information. The General Counsel and University Secretary is also the University's Data Protection Officer for the purposes of the GDPR.

b. If you have a question or complaint about how we have handled your personal information, you can raise it with us at any time by:

   i. e-mailing privacy@flinders.edu.au

   ii. calling us on 08 8201 7721, or

   iii. writing to us via post to:
   Privacy Officer
   Governance, Legal and Risk Division
   GPO Box 2100
   ADELAIDE SA 5001

c. We take all questions and complaints seriously and will generally acknowledge receipt of your question or complaint, in writing, within 5 working days and will investigate and respond to you within 30 days.

d. If you aren't satisfied with the way we have handled your matter, you may write to the Privacy Committee of South Australia. This committee has no formal responsibility with respect to universities but is willing to assist in the resolution of privacy complaints involving South Australian universities.

13. Changes to this policy

This policy is current as at the Approval Date shown below. It may be amended in light of new laws and technology, changes to our operations and practices, and changes in the business environment. The most up to date version of this policy is always posted on our website.

14. Supporting procedures

Supporting procedures are part of this policy and provide additional detail to give practical effect to the policy principles.

Personal Information Protection Procedures

Personal Information Access Procedures

Student Information Management Procedures

Approval Authority	General Counsel and University Secretary
Responsible Officer	General Counsel and University Secretary
Approval Date	2 May 2023
Effective Date	2 May 2023
Review Date*	May 2026
Last amended	
CM file number	CF14/374
* Unless otherwise indicated, this policy or procedures still apply beyond the review date.	

Printed versions of this document are not controlled. Please refer to the Flinders Policy Library for the latest version.