Flinders UNIVERSITY

INSPIRING ACHIEVEMENT

Personal Information Protection Procedures

Table of Contents

1. Governing Policy

Privacy Policy

2. Purpose

To implement the University’s commitments to the protection of the privacy of individuals’ personal information as set out in the Privacy Policy.

3. Scope

These procedures apply to all University personnel, students, academic status holders, volunteers, contractors, University agents and associated third parties, who have reason to access, use or deal with any personal information possessed by the University or gained in the course of University activity.

4. 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.
personnel	For the purposes of these procedures, **personnel** includes staff, students, academic status holders, volunteers, contractors, University agents and associated third parties

5. Collection of personal information on behalf of the University

5.1. General

All personnel who collect personal information on behalf of the University must:

a. ensure that personal information requested from individuals is the minimum needed for one or more of the University's functions or activities

b. collect the information in a way that is transparent and not intrusive

c. collect personal information about an individual only from the individual unless it is unreasonable or impracticable to do so, and

d. if the information is being collected for the purposes of undertaking research, ensure that appropriate research ethics approval is obtained.

> ***Example:*** *If you manage an email list of people who ask to receive information by email, e.g., a newsletter, record only their name and email address. Do not ask for or record unnecessary information such as their home address or phone number.*

5.2. Consent

When collecting personal information, personnel must:

a. obtain express consent (e.g., signed consent forms) wherever possible

b. collect sensitive information only with informed consent, and

c. seek advice from the Privacy Officer before relying on implied consent or on any of the following exemptions from collecting personal information without the person's consent:

   i. the collection is required or authorised by Australian law or a court

ii. it is unreasonable or impracticable to obtain consent and there is evidence that the information is needed to lessen or prevent a serious threat to the life, health or safety of an individual or the public

iii. there is evidence that the information is needed in order to take action on suspected unlawful activity or misconduct of a serious nature

iv. the information is reasonably necessary for a legal defence or claim by the University

v. the information is health-related and is required for the provision of a health service to the person and the information is collected in accordance with professional confidentiality, or

vi. the information is health-related and
- is necessary for the University to undertake research or statistical analysis relevant to public health or public safety, and
- it is impracticable for the University to obtain the individual's consent, and
- the information is collected in accordance with relevant NHMRC guidelines.

Examples: *The University wishes to use information about successful students in a course for promotional purposes. Information on their success is available from the Student Information System, but you must* ***not*** *identify any students in such promotions without their* ***consent****. Photos of students in class or on field trips also must not be used for promotional purposes without consent. To obtain consent, you must invite the student/s to be identified in the promotional activity, and they must consent to it in writing and be given a Privacy Statement. See also Procedure 5.3 below.*

You are on an interview panel for a personnel vacancy and you make a note that an applicant appears to have a physical disability. Making such a note would amount to the collection of Sensitive Information without the consent of the individual.

If you collect personal information that is to be sent on to another organisation, such as another university, be sure to inform students prior to collection that this is the intention.

If a student joins a University club, they must provide their personal details to the club themselves. You should not release information to the club without the student's consent.

5.3. Anonymity and Pseudonymity

When collecting personal information, personnel must:

a. consider whether individuals can be dealt with on an anonymous or pseudonymous basis. This cannot be the case if there is a legal requirement to verify identity or it is impracticable to deal with individuals if they have not identified themselves, and

b. de-identify personal information if statistical information only is required.

Examples of a.: *The name field on survey forms should not be mandatory unless it is intended to make follow-up contact with the individual.*

The University must enrol a student and award their degree using the true name of the student.

Note: *the fact that a student graduated, the name of their particular degree and year of graduation are public knowledge, but their results are not.*

Example of b.: *The University collects health information from a student through an application for supplementary assessment on medical/compassionate grounds. The information must only be used to assess the application and not for any other purpose. Any summary of the number or nature of such applications must not include information that might identify individuals.*

5.4. Privacy Statement

a. When collecting personal information, personnel must ensure that individuals are made aware of or are able to access an appropriate Privacy Statement relating to the collection of that personal information, at or before the time of personal information collection (or as soon as practicable after).

b. The Privacy Statement must include:

i. the University's full name and the contact details of the area that is collecting the personal information
ii. the purpose/s for which the information is collected
iii. the link to the University's Privacy Policy for further information
iv. any law that requires the individual's personal information to be collected
v. any third parties to which the University may disclose the individual's Personal information and whether any such party is located overseas, and
vi. any consequences for the individual if all or part of the personal information is not provided.

Example:

"This information is being collected by or on behalf of Flinders University's [University College/Division..., contact:…].

The information you provide will be used for [state purpose here…], and in accordance with the purposes set out in the University's Privacy Policy. Please refer to the University's Privacy Policy for more information, including the types of external entities to which the University may need to disclose personal information; how you can seek access to your personal information held by the University and how you can make a complaint if you feel your privacy has been breached."

***Additional text depending on the circumstances:*

If there is a law requiring the Personal information to be collected:

The information is being collected in accordance with [state relevant legislation here…]

If you know 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 purpose of collection, third party name and contact/ location]".

If there will be significant consequences if personal information is not provided:

If you do not provide the information, [insert consequence:...]."

Example: *A researcher wants to survey persons in a specific area for a research project. The researcher obtains names and addresses from the electoral roll. The researcher must ensure that the survey sent to the individual explains where the researcher has obtained their details from and includes a Privacy Statement.*

Example: *Where you are collecting personal information through personal contact (e.g. phone, over the counter), you must inform the individual of the information that is being collected and the purpose of collection, and direct them to the Privacy Policy.*

Example: *Where you use a form on a webpage to collect information, ensure that the webpage provides a Privacy Statement and requires the user to tick a box agreeing to the terms and conditions of the Privacy Statement.*

6. Data security

6.1. Unsolicited personal Information

When unsolicited personal information is received, personnel must determine whether it could have been collected for one or more of the University's functions or activities. If not, it must be destroyed or de-identified.

Examples:

- *emails sent in error*
- *unsolicited correspondence*
- *extra information provided in a job application*

6.2. Security of personal information

Once personal information is collected, personnel must:

a. Take reasonable steps to protect any personal information that is held from misuse, interference, loss, unauthorised access, modification or unauthorised disclosure, by:

   i. using locked filing cabinets and office security for hard copy personal information

   ii. using file access controls for personal information in digital form

   iii. using encryption (contact the IDS Helpdesk for assistance) for digital transfer of personal information outside the University

   iv. ensuring that appropriate data handling and security measures are in place, where personal information is disclosed to recipients overseas

   v. reviewing existing agreements with third parties overseas whom we engage to handle personal information, to ensure those third parties meet appropriate privacy and security management standards, and

   vi. reviewing existing agreements with third parties whom we engage to handle personal information, to ensure that those contracts impose appropriate privacy obligations and data breach response procedures.

b. Consult with Central Records about destruction or de-identification of personal information if it is no longer needed for any purpose for which it may be used or disclosed, and that is not required by law to be retained.

Related references:

- Records Management Policy and Overview of retention of personal information.
- Information Classification Framework and document handling Quick Reference Guide.

Example: *Staff in Colleges must not keep their own files of student information that is already stored on the Student System. Student information not retained on the Student System must be lodged with Enrolment Services for storage in the central student file.*

6.3. Disclosure to third parties

Personal information must only be disclosed to third parties for the purpose/s for which the personal information was collected, as set out in Procedure 3. Permitted disclosures to a third party include:

a. to government departments and agencies, where necessary to satisfy statutory reporting requirements;

b. to the University's controlled entities or subsidiaries, to the extent such personal information is required by the controlled entity or subsidiary to provide services to or on behalf of the University;

c. to external advisers and service providers to the extent such personal information is required for that party to provide services to the University;

d. to collaborating parties (e.g. other education institutions) where personal information is required for the collaborative activity to be undertaken; or

e. to IT service providers to enable the provider to establish user accounts for University personnel, students and others connected with the University, or to enable information storage or processing.

Example: *Where students' details are given to an outside organisation that provides work placements for students, the students must be informed. Only information essential for providing the placement may be provided to the organisation; refer to the Work Integrated Learning policy and procedures.*

Centrelink can require the University to provide enrolment information about a student.

The University must provide the Australian Health Professional Regulation Authority with details of students in certain medical, nursing and health sciences courses to enable those students to be registered by AHPRA.

The University must report any student visa breaches to the Department of Home Affairs.

The Law Society of SA is authorised to inquire whether a person who has applied for admission to legal practice has been guilty of dishonest conduct or any other conduct relevant to whether the applicant is a fit and proper person to be admitted as a legal practitioner.

6.4. Overseas disclosure

a. Before personal information is disclosed to an overseas recipient, steps must be taken to ensure that the overseas recipient does not breach the University's Privacy Policy or Australian Privacy Principles.

***Examples** of overseas disclosure include:*

- *The provision of courses of study or student support services by overseas educational institutions*
- *Sharing research data containing personal information with an overseas collaborating institution for a specific purpose*
- *Storing electronic files of personal information on a server located overseas (e.g using a cloud service).*

b. At least one of the following conditions must be met before there is any disclosure of personal information to third parties overseas:

i. there is a contract between the University and the third party that binds the third party to privacy obligations that are consistent with the Australian Privacy Principles

ii. the third party is subject to a law or binding scheme consistent with the Australian Privacy Principles and there are mechanisms to access and enforce the protection of that law or binding scheme, or

iii. written consent is obtained from the persons concerned to the disclosure of their information to the third party and the persons concerned are made aware that the University's Privacy Policy might not apply in this instance.

c. In determining the acceptability of disclosure to offshore third parties, personnel must also consider the types of information to be disclosed, the location of the provider's facilities and the provider's data security protocols. The provisions of the University's Information Classification & Handling Procedures must be applied.

d. A risk assessment must be completed and the business owner must accept any identified risks prior to any arrangement or contract is entered into with a provider. Where the arrangement with the overseas third party is for information management, IDS must complete the risk assessment and provide recommendations. Where the arrangement is with an overseas educational institution, or relates to a course of study (for example overseas student placement), the International Centre should be asked to provide the risk assessment.

***Example:** Where a contract with an overseas university is being negotiated, ensure you obtain advice on the terms of the contract concerning information privacy from Legal Services and the International Centre.*

***Example:** If you want to use a third party cloud provider to store personal information, you should contact IDS. Any agreement or formal contract with a cloud service provider must be assessed to ensure the provider securely stores and transmits personal information. All such contracts must be approved by IDS.*

Be careful also with storing personal information in Dropbox (or similar services such as OneDrive, Box, Google Drive etc). These services do not guarantee the privacy or security of your data. Sensitive University data must not be stored using these services unless approved by IDS.

***Example:** The privacy of the personal information of international students enrolling at Flinders on campus, whether they are exchange students here for a semester or completing a whole course, must be treated in the same way as for domestic students. Contracts with offshore universities that provide for exchange agreements or articulated programs must require adherence to the University's Privacy Policy.*

7. Purpose of collection, use and disclosure

7.1. Primary Purpose

a. The use and disclosure of personal information is restricted to purposes related to the University's functions and activities. The purpose for which you collect personal information is the **primary purpose** and you must not use or disclose the information for a **secondary purpose**.

b. Exceptions include where:

i. consent is obtained

ii. use or disclosure is authorised or required by law

iii. certain health situations or law enforcement situations arise

iv. in the case of personal information that is not Sensitive Information: if the individual would **reasonably anticipate** the secondary purpose, and the secondary purpose is **related** to the primary purpose, and

v. in the case of sensitive information, if the individual would **reasonably anticipate** their Sensitive Information being used or disclosed for the secondary purpose, and the secondary purpose is **directly related** to the primary purpose.

Examples:
Students
- *Primary: provision and management of education services*
- *Secondary: collating student statistics*

Alumni
- *Primary: providing interactive Flinders community/networking services*
- *Secondary: targeting alumni for research*

Donors
- *Primary: facilitating donations/gifts to Flinders*
- *Secondary: invitations to guest lectures/unrelated events*

Staff
- *Primary: management of employment, recruitment processes*
- *Secondary: statistics*

7.2. Direct marketing

a. Direct marketing must only occur if a simple opt-out mechanism is provided and the individual has not asked to opt out. You must have each individual's express or implied consent, and the individual should reasonably expect the University to use or disclose the personal information for that purpose.

b. Ensure direct marketing processes and mail out lists, including opt-outs, are carefully managed.

7.3. Government related identifiers

c. Government related identifiers such as Tax File Numbers and Medicare numbers must not be adopted by the University to identify individuals.

d. Do not use or disclose Government-related identifiers unless required or authorised by law, or where it is:
i. reasonably necessary to verify the person's identity for the purpose of the University's business
ii. required to fulfil obligations to a Government agency, or
iii. reasonably necessary for law enforcement.

8. Access to and correction of personal information

a. Before personal information is used or disclosed, as per the Personal Information Access Procedures, consider whether it is accurate, up-to-date, complete and relevant.

b. At least annually, remind individuals whose personal information is held on an ongoing basis to confirm the accuracy of their personal information.

> ***Example:*** *Include in newsletters a reminder to notify changes of address etc. and include a blank form, email address or link to a web-page for doing so.*

9. Data breaches

9.1. What is a data breach?

a. A ***data breach*** occurs when there is **unauthorised access** to or **disclosure** of personal information about an individual, or where such information is **lost** and unauthorised access or disclosure is likely to occur.

b. A data breach may be identified by way of a report from University personnel, an individual whose personal information is held by the University, or a person or entity external to the University.

c. Some forms of data breach require mandatory notification to either the Office of the Australian Information Commissioner (OAIC) or, where the data breach is related to individuals located in the European Union (EU), to the relevant EU supervisory authority.

d. To avoid serious consequences for the University, and to ensure data breaches are promptly managed, the procedures below must be followed whenever a suspected or actual data breach is detected.

> ***Examples of a data breach include*:**
>
> *A personnel member accidentally posts a spreadsheet on Flinders Learning Online, which contains personal information about students and their academic performance.*
>
> *A tutor loses a USB which contains personal information about students and their academic performance.*
>
> *A researcher accidentally sends an email to the wrong recipient, which contains the personal information of research participants.*
>
> *A payroll officer misplaces a bundle of payslips, which contains personal information about employees including their tax file number information.*
>
> *A personnel member accesses student records containing personal information without authority to do so and/or for an inappropriate or fraudulent purpose.*
>
> *A hacker gains access to the University's ICT systems containing personal information (e.g. email accounts, student databases or payroll software).*
>
> *A laptop is stolen from a personnel member's office, which contains personal information about students.*
>
> *A contractor who holds personal information on behalf of the University suffers a data breach.*

9.2. Reporting data breaches

a. Any personnel who becomes aware of a suspected or actual data breach must report it **immediately** to their supervisor/manager in person or by email, and no later than 24 hours after identifying the breach.

b. The supervisor/manager must:

i. notify the Privacy Officer of the data breach by emailing privacy@flinders.edu.au, as soon as reasonably practicable but no later than 24 hours after the report was received

ii. take immediate action to contain any real or suspected breach where possible (e.g., by stopping the unauthorised practice, recovering the records, advising persons who have received the information by mistake to destroy that information etc.), and

iii. if the real or suspected data breach affects electronic records, immediately notify the IDS Service Desk so that they can assist with containing the data breach.

c. The supervisor/manager and the person who reported the data breach must keep the incident confidential and not discuss it with any other person within or outside of the University, except for the Privacy Officer and other personnel involved in the investigation.

9.3. Investigating and responding to data breaches

a. The Privacy Officer will lead the investigation and the response, and all University personnel must provide assistance, as required.

b. Responses to a data breach may include:

i. notifying authorities where this is mandatory

ii. notifying affected individuals where this is appropriate

iii. undertaking a review of personal information handling and security practices, with a view to improving current practices, systems, other processes, policies and procedures.

10. Complaints about the University's handling of an individual's personal information

10.1. On receipt of a complaint

a. Any personnel who receives a complaint must refer it to the Privacy Officer in the first instance.

b. The Privacy Officer will check that the individual making the complaint is the individual whose personal information has been affected. If not, the Privacy Officer will clarify the complainant's authority to act for the individual whose privacy is the subject of the complaint.

c. The Privacy Officer will determine whether the complaint involves any of the following:

i. Inappropriate collection of personal (including sensitive) information

ii. Inappropriate use and/or disclosure of personal information

iii. Inaccuracy of personal information

iv. A breach of security of personal information

v. Refusal to give access to personal information

vi. Refusal to correct personal information

vii. Any other privacy issues.

d. If the complaint relates to a data breach, the Privacy Officer will take immediate action to remediate, investigate and assess the data breach in accordance with Procedure 9.

e. If there has been a breach of electronic information security, the Privacy Officer will notify Information and Digital Services immediately.

f. If the Australian Privacy Principles are not relevant to the complaint, the Privacy Officer will consider whether the complaint can be dealt with under the University's other complaint handling procedures.

g. The Privacy Officer will acknowledge all complaints in writing within 5 working days and clarify their understanding of the complaint.

h. If the complaint cannot be resolved through this initial contact with the Privacy Officer, the Privacy Officer will refer the matter to the appropriate area for investigation.

10.2. Investigation of complaint

a. Where investigation of the complaint is required, the Privacy Officer will refer the complaint promptly to the appropriate senior officer for investigation, as follows:

i. Portfolio Head with respect to information and records managed within the Portfolio

ii. Director of College Services or Vice President and Executive Dean with respect to information and records managed by a College

iii. Chief Executive Officer of a controlled entity or subsidiary with respect to information and records managed by the controlled entity or subsidiary

—together with their understanding of the privacy obligations at issue, with reference to the relevant clauses of the Australian Privacy Principles or the GDPR.

b. The senior officer must undertake the investigation of the complaint and prepare a response, or nominate an officer to do so. The investigating officer must be independent of the person/s responsible for the alleged conduct.

c. Where the complaint is referred for investigation, the Privacy Officer will notify the complainant of the name, title, and contact details of the investigating officer handling the complaint.

d. Where the complaint involves a breach of electronic information security, the investigation of the complaint will be coordinated by Information Digital Services (IDS), Information Security, Quality and Risk.

e. When investigating the complaint, the investigating officer must consider:

   i. whether there is evidence that the alleged conduct occurred

   ii. which privacy obligation/s may be relevant and why

   iii. whether it appears that the conduct complied with the University's privacy obligation/s (taking into account any legal exceptions or exemptions)

   iv. whether, if it appears that the University has not complied with its obligations, the complainant's requests regarding outcomes (if any) can be met.

f. Where a complaint is found to have been substantiated, the senior officer handling the matter will take steps to redress the concerns raised by the complainant and notify the complainant of the actions taken. Examples of outcomes include any or all of: an apology; a review and revision of policy, forms and procedures; staff training; improvement of security safeguards; or initiation of disciplinary procedures.

g. Where it appears that personnel has deliberately or maliciously disclosed or given unauthorised access to information or breached confidentiality or engaged in misconduct as a result of the misuse of information, a recommendation may be referred to the Deputy Vice-Chancellor (Students) (in respect of a student) or the Director, People & Culture (in respect of any other personnel), to initiate investigatory/disciplinary procedures.

h. The senior officer and/or the investigating officer must consider any systemic issues raised by the complaint and possible responses, such as:

   i. privacy training in the area

   ii. amendment of policies, forms and/or collection notices

   iii. providing additional accessible information

   iv. improvement of security and storage measures

   v. steps to improve data accuracy.

10.3. Communication with the complainant

a. The investigating officer must reply to the complainant in writing within 30 calendar days of the complaint being lodged, informing the complainant of:

   i. what progress has been made and when the next report to the complainant will be made, and

   ii. how the investigating officer is independent of the person/s responsible for the alleged conduct.

b. Once the investigation is complete, the investigating officer must:

   i. notify the complainant in writing of the outcome of the complaint, including a summary of the information relied on in developing the response

   ii. invite the complainant to reply to the response, including, if appropriate, an invitation for the complainant to discuss the response

iii. arrange for the issuing of an apology if the University did not comply with the relevant privacy obligation/s, and

iv. consider whether any additional outcomes may be appropriate.

c. The apology must be issued by the appropriate senior officer, as specified in Procedure 10.2.a.

10.4. Complainant's response

a. If the complainant seeks further action or is not satisfied with the outcome, the senior officer must:

i. assess any reply or further information from the complainant

ii. consider, if the outcome was that the University did comply with its privacy obligation/s, whether the complainant's response alters this view

iii. attempt to resolve the matter informally, through discussion and mediation and in accordance with the principles of natural justice and procedural fairness.

b. The investigating officer and/or the complainant can seek mediation from the Privacy Committee of South Australia—although it has no formal responsibility with respect to universities, it is willing to assist in the resolution of privacy complaints involving South Australian universities.

10.5. If the complainant is still not satisfied with the outcome

a. If still not satisfied, a complainant who has made a complaint which has been substantiated may seek, where applicable, to have the matter resolved through a process consistent with clause 17 of the University's Grievances procedures.

b. The senior officer or investigating officer must ensure that all records of the complaint and the investigation and outcome are confidentially secured and, following completion of the investigation, submitted to the Privacy Officer. All complaint records must be stored securely and in accordance with the Records Management Policy.

11. Failure to comply

Failure to comply with these procedures may result in disciplinary action in accordance with the relevant disciplinary procedures. These are:

a. for students: Student Academic Integrity Policy and/or Statute 6.4: Student Conduct, or

b. for personnel: the discipline procedures of the relevant industrial agreement.

12. Further advice

- Contact University Records (central.records@flinders.edu.au) for advice about secure disposal of personal information in accordance with the Records Management Policy
- Contact Legal Services (legal@flinders.edu.au) for advice on template agreements/privacy clauses.
- Contact the Privacy Officer (privacy@flinders.edu.au) for questions about access or complaints.

13. Related Policies and Procedures

Payment Card Data Protection
Records Management Policy

Approval Authority	University Secretary
Responsible Officer	General Counsel, Governance, Legal & Risk
Approval Date	3 December 2018
Effective Date	3 December 2018
Review Date*	December 2021
HPRM file number	CF/1064
* Unless otherwise indicated, this procedure will 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.