

## Purpose and Scope

Murdoch University is committed to protecting the privacy of individuals and responsibly managing information in accordance with the Privacy and Responsible Information Sharing Act 2024 (WA) (PRIS Act). This procedure outlines how the University collects, uses, stores, shares, and safeguards personal information to support education, research, and community engagement while ensuring compliance with Western Australian law and other impacted legislation.

Supporting the [Privacy Policy](#), this procedure applies to students, employees, other members of the University community and the public and includes information collected through teaching, research, administration, and community services and information shared with external entities under the Responsible Information Sharing Principles (RSPs) and core Information Privacy Principles (IPPs) governing collection, use, integrity, storage, security, and access to information as set out in the PRIS Act.

## Overarching Policies

[Privacy Policy](#)

## Procedure

### 1. Privacy Officer

- 1.1 The Vice Chancellor will appoint a Privacy Officer for the University who will hold responsibilities under the Privacy and Responsible Information Sharing (PRIS) Act 2024 (WA).

### 2. Collection

- 2.1 The University will collect personal information only by lawful and fair means.
- 2.2 So long as it is reasonable and practicable to do so, personal information will be collected directly from the individual.
- 2.3 If it is necessary to collect personal information from a third party, reasonable steps will be taken to inform the individual of the circumstances of this collection.

- 2.4 If it is necessary to collect any sensitive information, specific consent will be sought at the time of collection and the purpose for which the sensitive information is being collected will be provided.

### 3. **How the University collects and holds personal information**

- 3.1 Personal Information Collection Notices are generally provided at the time of personal information collected. These Collection Notices:

- 3.1.1 Notify an individual:

- 3.1.1.1 Whether the information is being collected under an Australian law or court/tribunal order;

- 3.1.1.2 of any collection which an individual might not otherwise be aware of; or if it is being collected from someone else; or any secondary purposes for which it is being collected; and

- 3.1.1.3 The main consequences for the individual if all or some of the personal information is not collected.

- 3.1.2 Inform an individual:

- 3.1.2.1 of any other entity to which the University usually discloses this kind of information; and

- 3.1.2.2 Whether the University is likely to disclose the information to overseas recipients, and if so, advise, if possible, the countries in which those recipients are likely to be located.

- 3.2 Where practicable, access to personal information will be restricted to those staff members who may need the information to carry out their responsibilities.

- 3.3 Information collected may be held in any form including:

- 3.3.1 Paper based

- 3.3.2 Audio or videotape

- 3.3.3 Microfilm or microfiche

- 3.3.4 Computer chip-based memory

- 3.3.5 Cloud storage system

- 3.3.6 CCTV camera footage

- 3.3.7 Any electronic, magnetic or optical medium, such as computer disks or computer tape.

### 4. **Access to and correction of personal information**

- 4.1 All efforts will be taken to ensure that the information collected and held is complete, accurate and up to date. It is expected that an individual will assist by informing the University of any relevant changes.

- 4.2 If personal information is not provided in full, or not kept up to date, then there may be serious consequences, including (by way of example only):
  - 4.2.1 the withdrawal of an offer to a student of a place at the University;  
or
  - 4.2.2 if admitted to the University, the cancellation of a student's enrolment; or
  - 4.2.3 an adverse impact on the student/staff record.
- 4.3 Upon request, and subject to applicable exceptions, the University will provide access to the personal information it holds about an individual within 30 days, at no cost. Personal information may be reviewed and depending on its nature, may be updated or corrected in accordance with relevant procedures. This applies, for example, to information held on Callista (MyInfo) for students and Workday for staff. Access may be denied to information where this may impact the privacy of other individuals or involve the disclosure of trade secrets, confidential information, ongoing research data or information about the business, commercial or financial affairs of the University; or where the request is frivolous or vexatious; or the information is subject to legal professional privilege.
- 4.4 If any personal information held by the University is inaccurate, out of date, incomplete, irrelevant, or misleading, the University will take reasonable steps to correct it. If a correction is refused, an individual will receive a written explanation, and upon request, a statement disputing the information will be attached to the record.
- 4.5 Unless impracticable or unlawful, the University will notify any third party to whom personal information was previously disclosed of a correction, if requested.

## 5. **Use and disclosure of personal information**

- 5.1 The University will not use or disclose personal information other than for the primary purpose for which it was collected.
- 5.2 The University may disclose information in the following specific situations:
  - 5.2.1 **Authorised Contractors:** To contractors engaged by the University, such as IT service providers, where required to fulfil contractual obligations.
  - 5.2.2 **Academic Verification:** In response to a legitimate request from another university regarding a student's academic record and disciplinary history, provided reasonable steps are taken to confirm the legitimacy of the request.
  - 5.2.3 **Graduate Register:** Publication of graduate details, including name, conferral date, and award title, on the University's Graduate Register to enable third parties to verify qualifications.
  - 5.2.4 **Surveys:** For the purpose of conducting student and graduate surveys, either directly by the University or through an authorised third party. Any third party engaged will be required to comply with

the Australian Privacy Principles when handling personal information.

- 5.2.5 Where there is a request from another university to obtain information on the academic record and performance of a student, including whether the student was expelled or suspended for disciplinary reasons and the University has taken reasonable steps to confirm the legitimacy of the request.
- 5.3 Information may be disclosed/used for reasons other than the primary purpose of collection where the provider of the information has consented or that secondary purpose is related to the primary purpose; or in relation to sensitive information, it is directly related to the primary purpose.

## 6. **Automated Decision-Making**

- 6.1 The University may use automated systems or tools to assist in decision making processes. These may include analysing personal information to support administrative, educational, research, or service-related functions.
- 6.2 Where an automated decision-making process is used, the University will:
  - 6.2.1 ensure the use of personal information complies with the PRIS Act, including the IPPs;
  - 6.2.2 take reasonable steps to ensure that any automated decision is fair, accurate, and based on reliable and up to date information;
  - 6.2.3 provide individuals with information about the use of automated decision making where it forms a substantial part of a decision that affects them;
  - 6.2.4 ensure that a meaningful human review is available upon request where an automated process has materially influenced an outcome; and
  - 6.2.5 maintain appropriate oversight, auditability, and safeguards to prevent unlawful discrimination, bias, or adverse impacts arising from automated processes.
- 6.3 Biometric information will not be used for automated decision making that has a significant effect on an individual's rights or access to the university services without appropriate human oversight.
- 6.4 Automated decision making will not be used as the sole basis for decisions that may significantly affect an individual's rights, access to services, or opportunities without appropriate human involvement.

## 7. **Disclosure to overseas recipients**

- 7.1 If the University is likely to disclose personal information to an overseas recipient, reasonable steps will be taken to notify the individual at the time of collection and, where practicable, specify the countries in which such recipients are likely to be located.

- 7.2 However, from time to time, as part of carrying out functions and activities of the University, there may be a need to disclose certain personal information to individuals or organisations located overseas, including, but not limited to the following countries:
  - 7.2.1 Dubai and Singapore (where the University has transnational educational centres)
  - 7.2.2 US (where certain IT platforms are hosted).
- 7.3 Every reasonable effort will be taken in the circumstances to ensure that any overseas recipient of personal information is aware of and agrees to uphold the privacy standards and principles outlined in the Privacy Policy before any disclosure occurs, unless:
  - 7.3.1 The overseas recipient is in a jurisdiction with similar laws which can be enforced; or
  - 7.3.2 Consent for the disclosure has been provided; or
  - 7.3.3 The overseas transfer is required, authorised or permitted by law.

## **8. Disclosure to WA government agencies**

- 8.1 Murdoch University is subject to Western Australia's responsible information sharing framework established under the PRIS Act, consequently:
  - 8.1.1 Information sharing requests are assessed against the PRIS Act criteria.
  - 8.1.2 Sharing is permitted only when it improves community outcomes (e.g., health, education, research) and aligns with privacy protections.
  - 8.1.3 Aboriginal data governance principles are respected, ensuring culturally appropriate handling of Indigenous information.

## **9. Security of personal information and breach notification**

- 9.1 Reasonable technical and organisational measures will be taken to protect the personal information held by the University from misuse, interference, and loss, as well as from unauthorised access, modification, or disclosure.
- 9.2 As part of the security measures, the University has developed a range of policies and standards, available on the website, which should be read in conjunction with this Privacy Policy and Privacy Procedure in the context of personal information. These policies relate to:
  - 9.2.1 Privacy collection notice of personal information
  - 9.2.2 Information security Incident Management Policy
  - 9.2.3 IT conditions of use policy
  - 9.2.4 Email and electronic messaging policy
  - 9.2.5 Information Management Policy

9.2.6 Emerging Digital Technologies Policy

9.2.7 ICT Security Policy

9.3 Personal information will be retained in accordance with the Western Australian University Sector Disposal Authority established under the State Records Act (WA) and disposed of lawfully and securely.

9.4 In the event of a serious data breach, Murdoch University will notify the Western Australian Information Commissioner and affected individuals, as required under the PRIS Act.

## 10. **Unsolicited personal information**

10.1 If the University receives personal information about an individual that was not solicited, information will be assessed whether it is a part of a public record or could have been lawfully collected. If not, and if lawful and reasonable, steps will be taken to destroy or de-identify the information.

10.2 If any personal information is uploaded to the University's Facebook page or other social media channels, no steps are taken by the University in relation to that information. If a specific enquiry or complaint is received, steps considered necessary in the circumstances will be taken to investigate and address the matter within a reasonable time.

## 11. **Direct Marketing**

11.1 As a general rule, personal information will not be disclosed (including any sensitive information) for direct marketing purposes.

11.2 Subject to clause 11.5, the University may use personal information (excluding sensitive information) collected to send direct marketing material that an individual would reasonably expect to receive. A "reasonable expectation" includes situations where there is a past or existing relationship with the University, or an individual has expressed interest in the functions or activities of the University. Such material may include, but is not limited to, invitations or information about the University's events and activities.

11.3 Subject to clause 11.5, the University may also use personal information (excluding sensitive information) collected from a third party to send direct marketing material to individuals which may or may not be reasonably expected, but only where there has been consent or it is impracticable to obtain that consent.

11.4 Sensitive information will only be used for direct marketing purposes with prior consent.

11.5 All direct marketing material will include an opt-out mechanism. If an individual decides at any time that they do not wish to receive certain promotional material, they may request removal from the mailing list, and this will be actioned without charge.

11.6 Subject to clause 11.5, the University may share personal information (excluding sensitive information) with a third party to send direct marketing

material or serve advertising related to the University products and services, but only where the individual has consented or it is impracticable to obtain that consent.

11.7 These third parties may use cookies, pixel tags and similar tracking technologies to collect certain information about online activities and deliver relevant advertisements as well as help to monitor advertising effectiveness.

11.8 If the University intends to use personal information for direct marketing purposes outside the scope of its activities, consent will be sought unless it is impracticable to do so.

## 12. Responsibilities for the management of personal information

12.1 The University will manage personal information by:

12.1.1 Proactively protecting it from unauthorised access or invasive events;

12.1.2 Embedding privacy principles into the design of processes and systems;

12.1.3 Establishing clear accountabilities and responsibilities for information management.

12.2 Information Stewards must ensure reasonable steps are taken to manage the University's information assets, regardless of media format.

12.3 Information Custodians are responsible for implementing and monitoring all reasonable measures to manage the University's information assets in accordance with this Policy.

12.4 Information Users must ensure that the collection, use, storage, disclosure, and correction of personal information is carried out in compliance with this Policy.

## 13. Governance and accountability

13.1 The University's Privacy Officer oversees compliance with the Privacy Policy.

13.2 Staff are trained in privacy and responsible information sharing obligations.

13.3 Regular audits and reviews ensure ongoing compliance with the PRIS Act.

## 14. Privacy inquiries and complaints

14.1 Contact:

Privacy Officer  
University Secretary's Office  
90 South Street, Murdoch, Western Australia, 6150  
+61 (8) 93607647

[universitysecretary@murdoch.edu.au](mailto:universitysecretary@murdoch.edu.au)

## Governance

<b>Approval Authority</b>	Senior Leadership Team
<b>Owner</b>	Vice Chancellor
<b>Legislation mandating compliance</b>	<i>Privacy and Responsible Information Sharing Act 2024 (WA)</i>
<b>Category</b>	Primarily a function of Management
<b>Related University Legislation and Policy Documents</b>	<a href="#">Privacy Policy</a> <i>Personal Information Collection Notice</i> <a href="#">Information security Incident Management Policy</a> <a href="#">IT conditions of use policy</a> <a href="#">Email and electronic messaging policy</a> <a href="#">Information Management Policy</a> <a href="#">Emerging Digital Technologies Policy</a> <a href="#">ICT Security Policy</a>
<b>Date effective</b>	27/01/2026
<b>Review date</b>	27/01/2029

## Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Approved by SLT	27/01/2026	

*Please refer to the electronic copy in the Policy and Procedure Manager to ensure you are referring to the latest version.*