

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 policy 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.

This policy and the supporting Privacy Procedure apply 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.

Policy

1. **Murdoch University adheres to the Information Privacy Principles (IPPs) and Responsible Information Sharing Principles (RSPs) established under the PRIS Act.**
 - 1.1 Lawful and fair collection: Information is collected only for legitimate University purposes.
 - 1.2 Transparency: Individuals are informed about how their information will be used.
 - 1.3 Data minimisation: Only necessary information is collected and retained.
 - 1.4 Security: Personal information is protected against loss, misuse, and unauthorised access.
 - 1.5 Access and correction: Individuals have the right to access and correct their personal information.
 - 1.6 Responsible sharing: Information is shared only when it serves a clear public interest, is authorised under the PRIS Act, and safeguards privacy.

2. **The purposes for which personal information is collected and held:**
 - 2.1 To undertake and support the activities of the University including the following:
 - 2.1.1 Student enrolment, teaching, and assessment.
 - 2.1.2 Research activities and compliance with ethics requirements.
 - 2.1.3 Employment and human resources management.
 - 2.1.4 Community engagement, alumni relations, and fundraising.
 - 2.1.5 Compliance with legal and regulatory obligations.
 - 2.1.6 Safeguarding staff, students and the University's physical assets using CCTV camera footage.
 - 2.2 Whenever personal information which is also sensitive information is collected, prior consent will be sought unless the law requires or permits collection without first obtaining consent.

3. **Types of personal information that may be collected:**
 - 3.1 Personal information is information or an opinion, whether true or not and whether recorded in a material form or not, about an individual whose identity is reasonably apparent.
 - 3.2 Personal information collected may comprise:
 - 3.2.1 Full name
 - 3.2.2 Address – postal or residential
 - 3.2.3 Contact details such as telephone numbers and email addresses
 - 3.2.4 Photograph
 - 3.2.5 Date of birth
 - 3.2.6 Gender
 - 3.2.7 Academic results
 - 3.2.8 Academic record
 - 3.2.9 Disciplinary record
 - 3.2.10 Student fee liability to the University
 - 3.2.11 Bank account details
 - 3.2.12 Credit card details
 - 3.2.13 Tax file numbers for Commonwealth supported students
 - 3.2.14 Visa information for overseas students
 - 3.2.15 Emergency contact details
 - 3.2.16 Information about opinions and preferences.
 - 3.3 Sensitive information is a subset of personal information and may comprise information or an opinion about relating to such matters as:

- 3.3.1 Racial or ethnic origin
 - 3.3.2 Political opinions
 - 3.3.3 Membership of a political association
 - 3.3.4 Religious beliefs or affiliations
 - 3.3.5 Philosophical beliefs
 - 3.3.6 Membership of a professional or trade association
 - 3.3.7 Membership of a trade union
 - 3.3.8 Sexual orientation or practices
 - 3.3.9 Criminal record
 - 3.3.10 Health information, including disability information
 - 3.3.11 Genetic information
 - 3.3.12 Biometric information or templates.
- 3.4 Biometric information is a form of sensitive information and includes data derived from biological or behavioural characteristics that can be used to identify an individual. This may include, but is not limited to:
- 3.4.1 facial images or facial recognition templates
 - 3.4.2 fingerprints or palmprints
 - 3.4.3 iris or retinal scans
 - 3.4.4 voiceprints
 - 3.4.5 keystroke patterns or other behavioural identifiers
 - 3.4.6 biometric identifiers used for identity verification, access control, examination integrity, or security purposes.

4. How the University collects and holds personal information.

- 4.1 Personal Information Collection Notices are generally provided at the time of personal information collection.
- 4.2 The University's website uses essential cookies to ensure core functionality. The University also uses non-essential analytics and target cookies to improve performance and show more relevant content. These cookies do not identify an individual. Non-essential cookies can be disabled in browser settings, but doing so may limit some site features.

5. Use and disclosure of personal information:

- 5.1 The general rule is that the University will not use or disclose personal information other than for the primary purposes for which it was collected.
- 5.2 The information may be used/disclosed for reasons other than the primary purpose of collection where the provider of the information has consented; and/or there is a reasonable expectation of disclosure.

- 5.3 There may also be use/disclosure for reasons of law, order, enforcement and safety in the following circumstances:
 - 5.3.1 If required or authorised by law or court/tribunal order;
 - 5.3.2 When it is unreasonable or impracticable to obtain consent and the University reasonably believes it is necessary to prevent or lessen a serious threat to the life, health or safety of any person; or public health or public safety.
 - 5.3.3 If the University has reason to suspect that unlawful activity or misconduct of a serious nature that relates to the University's functions or activities has been, is being, or may be engaged in, and the University reasonably believes that it is a necessary part of its investigation and action in relation to the matter to disclose it, including in the reporting of its concerns to relevant persons or authorities;
 - 5.3.4 If it is reasonably necessary either to establish, exercise or defend a legal (or equitable) claim, or for the purposes of a confidential alternative dispute resolution process;
 - 5.3.5 When the University believes that the use or disclosure is reasonably necessary for one or more enforcement related activities conducted by an enforcement body (e.g. the police), in which case a written note will be kept with details of the disclosure.
- 5.4 There may also be use/disclosure for health-related situations -. Health information may be disclosed for purposes other than the primary purpose of collection as outlined in clauses 5.2 and 5.3, and in the following circumstances:
 - 5.4.1 Research
 - 5.4.1.1 Disclosure is necessary for research or for compiling and analysing statistics relevant to public health or safety;
 - 5.4.1.2 It is impracticable to obtain consent;
 - 5.4.1.3 The research is conducted in accordance with all applicable guidelines; or
 - 5.4.1.4 The University reasonably believes the recipient will not disclose the information or any personal information derived from health information.
 - 5.4.2 Incapacity to give consent
 - 5.4.2.1 If a health service has been provided; and
 - 5.4.2.2 The recipient is a responsible person for the individual; and
 - 5.4.2.3 The individual is physically or legally incapable of giving consent or cannot communicate consent; and
 - 5.4.2.4 The carer providing the health service for the University is satisfied that the disclosure is necessary for appropriate care or treatment, or is made for compassionate reasons; and

5.4.2.5 The disclosure does not contradict any prior expressed wishes of the individual; and

5.4.2.6 The disclosure is limited to what is reasonable and necessary in the circumstances.

5.5 The University may use or disclose this genetic information if:

5.5.1 This has been obtained while providing a health service; and

5.5.2 The University reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another person who is a genetic relative; and

5.5.3 It is conducted under all applicable guidelines relating to this use or disclosure; and

5.5.4 In the case of disclosure – the recipient of the information is a genetic relative.

5.6 Holders of Murdoch University email addresses

5.6.1 Names and email addresses are accessible via the University's Microsoft 365 Global Address List. A staff member may access student contact details in this manner only for purposes related to the University's functions. Students may access the contact details of other students only in connection with University activities.

5.6.2 Students able to hide their contact details from the other users. Students may opt to remove their contact details from the database. In doing so, they should first enquire as to whether, and to what extent, the removal of their contact details may adversely impact their involvement with University activities.

6. Integrity of personal information

6.1 The University will take reasonable steps to ensure that the personal information that is collected, used, stored, and shared is accurate, up to date and complete with the individual having a responsibility to inform the University of any relevant changes.

7. Rights of Individuals

7.1 An individual has the right to:

7.1.1 Request access to their personal information.

7.1.2 Seek correction of inaccurate or incomplete information.

7.1.3 Make complaints to the West Australian Information Commissioner if there is a belief that privacy rights have been breached.

8. Direct Marketing

8.1 As a general rule, the University will not use or disclose personal information (including any sensitive information) for direct marketing purposes.

9. Overseas data subjects

9.1 In some circumstances, the University may have privacy obligations under the laws of jurisdictions other than Australia. These are legislated through general data protection legal instruments and apply when personal information about an individual resident in the relevant jurisdiction is processed by the University as part of a service offering.

9.2 It is the individual's responsibility to determine whether they believe rights exist under such legislation.

9.3 Where these rights which are binding on the University exist, the University will manage the personal information accordingly.

Governance

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

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Approved by SLT	27/01/2026	
SLT Rescinded Approved 31/01/2023 version	27/01/2026	
Administrative Amendment	31/01/2023	
Administrative Amendments	13/01/2023	
Approved	09/01/2023	
Approved	13/11/2020	
Approved	26/02/2020	
Clause 8 amended	06/02/2018	
Approved	14/09/2016	
Approved	11/03/2014	
Approved	20/03/2012	
Approved	21/03/2012	

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