**Policy Title: Privacy**

This is a draft policy/procedure under development and is subject to review. It should not be construed as an approved University policy/procedure or acted upon as such. Any template or branding updates will be made and finalised before publication. Any comments on this draft should be directed to the Policy Developer: [Yue Lin SUN](mailto:yue.sun@ecu.edu.au), Senior Privacy Risk & Compliance Advisor.

**Policy Owner: Director Strategic and Governance Services**

**Keywords:** **information, personal, health, sensitive, access, disclosure, record keeping**

**Policy Code: PL090**

[Intent](#Intent)

[Organisational Scope](#OrgScope)

[Definitions](#Definitions)

[Policy Content](#_POLICY_CONTENT)

[Accountabilities and Responsibilities](#Accountabilities)

[Related Documents](#RelatedDocs)

[Contact Information](#ContactInfo)

[Approval History](#Approval)

## INTENT

The purpose of this policy is to provide guidelines for all collection, use, disclosure, storage and destruction of Personal or Health Information by the University, including parameters to address access, sharing, amendment and loss of personal information.

## ORGANISATIONAL SCOPE

This policy applies to all University Staff (including contractors, honorary and associated appointees, outsourced personnel), Students, Vendors/Suppliers, Contracted Service Providers and broader University community.

## DEFINITIONS

The [University Glossary](https://edithcowanuni.sharepoint.com/:w:/s/SGS-CorpKB/EQ3-eRb52i1OuSCFDZ5vH50BwBks0VstyQkfoMWm4dNjtw?e=pm7K8g) and the following definitions apply to this policy:

| Term: | Definition: |
| --- | --- |
| Contracted Service Provider | A Contracted Service Provider is   1. a party to a State or Commonwealth services contract who provides services to or on behalf of an outsourcing entity under the contract; or 2. a personal who is a subcontractor (whether direct or indirect) of a personal referred to in the above paragraph for the purposes of the services contract. |
| Cyber Security Incident | One or more acts, events or circumstances involving any of the following:   1. unauthorised access to (i) computer data or (ii) a computer program; 2. unauthorised modification of (i) computer data or (ii) a computer program; 3. unauthorised impairment of electronic communication to or from a computer; or 4. unauthorised impairment of the availability, reliability, security or operation of (i) a computer, (ii) computer data or (iii) a computer program. |
| Data Subject | As set out in Article 4 Definitions of the [General Data Protection Regulation (EU) 2016/679](#RelatedDocs) (**GDPR**) – Means an identified or identifiable natural person |
| De-identified Information | Has the meaning given in Section 11(2) of the [*Privacy and Responsible Information Sharing Act 2024* (WA)](#RelatedDocs) (**PRIS Act**).  Means to modify, or apply a process to, the information, with the result that the identity of an individual is not apparent, and cannot reasonably be ascertained, from the information. |
| Health Information | Has the meaning given in [*PRIS Act*](#RelatedDocs)and[*Privacy Act 1988* (Cth)](#RelatedDocs) (**Privacy Act**).  Means (a) personal information that relates to:   1. the health (at any time) of an individual; or 2. the disability (at any time) of an individual; or 3. an individual’s expressed wishes about the future provision of health services to the individual; or 4. a health service provided, or to be provided, to an individual;   or   1. other personal information collected to provide, or in providing, a health service; 2. other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; 3. genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual. |
| Information Breach Incident | A potential, suspected or actual incident where unauthorised access, disclosure of Personal Information held by the University. An Information Breach may also be a privacy breach. |
| Permitted General Situation | As set out in section 16A of the [*Privacy Act 1988* (Cth)](#RelatedDocs) as if the University was an “APP entity” as defined in the Act. |
| Permitted Health Situation | As set out in section 16B of the [*Privacy Act 1988* (Cth)](#RelatedDocs) as if the University was an “APP entity” as defined in the Act. |
| Permitted Purpose | Has the meaning given in section 159(1) of the [*Privacy and Responsible Information Sharing Act 2024* (WA)](#RelatedDocs).  Means information may be handled under information sharing agreement for any of the following purposes, related to:   1. government policy; 2. government programs and services; 3. research and development for the public benefits; 4. emergency management; 5. any other purposes prescribed by regulations. |
| Personal Data | As set out in Article 4 Definitions of the [General Data Protection Regulation (EU) 2016/679](#RelatedDocs).  Means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Personal Information | As set out in Section 4 of the [*Privacy and Responsible Information Sharing Act 2024* (WA)](#RelatedDocs).  Means an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion. Including:   1. a name, date of birth or address; 2. a unique identifier, online identifier or pseudonym; 3. contact information; information that relates to an individual’s location; 4. technical or behavioural information in relation to an individual’s activities, preferences or identity; 5. inferred information that relates to an individual, including predictions in relation to an individual’s behaviour or preferences and profiles generated from aggregated information; 6. information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual. |
| Privacy and Responsible Information Sharing Champion | The PRIS Champion is the Director, Strategic and Governance Services, responsible for promoting a culture of privacy and responsible information sharing and compliance with [*Privacy and Responsible Information Sharing Act 2024* (WA)](#RelatedDocs)within the University. |
| Privacy Impact Assessment | Means a systematic assessment of a function or activity of the University that identifies potential privacy impacts and recommendations to manage, minimise or eliminate the identified impacts. Under the PRIS Act, a PIA is required for any high privacy impact function or activity, where the handling of personal information is likely to have a significant impact on the privacy of individuals. |
| Privacy Officer | The Privacy Officer is the subject matter expert in support of the PRIS Champion. |
| Sensitive Information | Means (a) personal Information where it is:   1. information or an opinion about an individual’s:    1. racial or ethnic origin;    2. political opinions;    3. membership of a political association;    4. religious beliefs or affiliations;    5. philosophical beliefs;    6. membership of a professional or trade association;    7. membership of a trade union;    8. sexual orientation or practices; or    9. criminal record; 2. health Information about an individual; 3. genetic information about an individual that is not otherwise health information; 4. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or biometric templates. |
| Sensitive Aboriginal family history information | Means information, including family history information, that:   1. relates to Aboriginal people and their ancestors; and 2. was collected in the period from 1898 until 1972 for the purposes of implementing laws, and government policies and practices, applying specifically to Aboriginal people. |
| Sensitive Aboriginal traditional information | Means information that, according to Aboriginal tradition, should not be disclosed to individuals who are not the knowledge holders of that information. |

## POLICY CONTENT

#### General Principles

* 1. The University will collect, use and disclose Personal Information in a manner that is consistent with this Policy and the [*Privacy and Responsible Information Sharing Act 2024* (WA)](#RelatedDocs).
  2. The University will also reasonably endeavour to ensure its collection, use and disclosure are broadly consistent with the Australian Privacy Principles as defined in the [*Privacy Act 1988* (Cth)](#RelatedDocs), noting that its requirements under the [*Privacy Act 1988* (Cth)](#RelatedDocs) are limited to the following circumstances:
     1. the collection, use and disclosure of information obtained for the purposes prescribed by the [*Higher Education Support Act 2003* (Cth)](#RelatedDocs);
     2. the collection, use and management of data concerning tax file number information of individuals – which must also be consistent with [*Privacy (Tax File Number) Rule 2015*](#RelatedDocs); and
     3. where it has agreed to be contractually bound.
  3. The University is committed to the responsible management of Personal and Health Information in undertaking its core functions of teaching, research and activities to support these functions.
  4. The University will balance openness, transparency, public interest in access to information and the protection of the privacy of individuals with whom it interacts.

#### Accountable Roles

* 1. The University has appointed the Privacy and Responsible Information Sharing Champion to promote a culture of privacy and responsible information sharing and compliance within the University. The Privacy and Responsible Information Sharing Champion is the Director, Strategic and Governance Services
  2. The Senior Privacy Risk & Compliance Officer will serve as Privacy Officer. The role:
     1. is responsible for the development, maintenance and oversight of University’s privacy management framework.
     2. acts as the University’s Information Sharing Officer role for the purposes of the PRIS Act;
     3. provides support and advice on:

1. the University’s privacy management practices;
2. privacy complaints or concerns in line with [Complaints Policy](#RelatedDocs);
3. identification, assessment and articulation of privacy risks in line with [ECU Risk Management Framework](#RelatedDocs) to enable ECU to make informed risk-based decisions;
4. Privacy Impact Assessment with University stakeholders and wider University community as necessary;
5. investigation and response to information breach incident reports in line with [Critical Incident and Business Continuity Management Policy and Guidelines](#RelatedDocs).
   1. The University has appointed Relevant Data Owners with the authority to approve access or sharing of Personal Information. The Relevant Data Owners will take into account the University’s legal responsibilities, and its role under the [*Edith Cowan University Act 1984* (WA)](#RelatedDocs), and obligations under this Policy.
      1. The Relevant Data Owner depends on the type of Personal Information:

|  |  |
| --- | --- |
| Type of Personal information | Relevant Data Owner |
| Information or data is about a student (context of request) | Director, Student Administration  or  Director, Student Life |
| Information or data is about a staff member. | Director, People & Culture |
| Information or data is about an individual in their capacity as a research subject | Director, Research Services |
| Information or data in any other circumstances | Director, Strategic and Governance Services |

#### Collection[[1]](#footnote-2)

* 1. The University will provide relevant collection notices and only collect Personal Information:
     1. for lawful purposes and when reasonably necessary for, or related to, the University’s functions, services or activities; and
     2. from the individual it relates to, unless:

1. the individual has consented otherwise;
2. it is required or authorised by Australian law or a court or tribunal order; or
3. it is unreasonable or impracticable to do so.
   1. Where the University receives unsolicited Personal Information, it will determine whether possessing such information is reasonably necessary for, or directly related to, the University’s functions or activities, and whether the University could have collected the Personal Information if the University had actively solicited the information. If so, the provisions of this Policy will apply to the use, disclosure and management of that information. Otherwise, where lawful and reasonable to do so, unsolicited information will be destroyed or de-identified.
   2. The University will only collect Sensitive Information:
      1. where a person consents to the collection as per Section 4.8.
      2. in relation to a Permitted General Situation or Permitted Health Situation or for a Permitted Purpose; or
      3. where the information relates to University’s functions, services of activities, and solely relates to University Staff or Students, or to individuals who have contact with and in connection with University’s functions, service or activities.
   3. At or before the collection of Personal Information, or as soon as practicably possible thereafter, the University will take reasonable steps to notify the individual or ensure the individual is aware of the collection, and that the collection is fair and reasonable in the circumstances. The notification may take the form of a collection notice and must contain:
      1. the University’s contact details;
      2. where the University has collected this information from someone other than directly from the individual or where the individual may not be aware the University has collected the information, the fact that the information has been collected and circumstances around its collection;
      3. how the individual may access the information (if applicable);
      4. the purpose for collecting the information, and any laws that require the particular information be collected (if applicable);
      5. the use or handling of information of this kind and the third parties to whom the information is usually disclosed (per **Use and Disclosure**);
      6. the consequences (if any) for the individual if the University does not collect some or all of the information; and
      7. that the individual’s information will be managed in accordance with this Policy, including individual rights to:
   4. access or correct information (per **Access, Quality and Correction**), and
   5. complaints processes (per **Privacy Complaints Handling**)

#### Use and Disclosure[[2]](#footnote-3)

* 1. The University will only use or disclose Personal Information when it is reasonably necessary for, or directly connected to, its functions, services, or activities.
  2. The University will not use or disclose Personal Information unless:
     1. the individual to whom the relation relates to have expressly or by inferenced consented to its use or disclosure;
     2. it is reasonable to expect that the University would use or disclose the information in the ordinary course of its functions, services or activities, including to meet its compliance and reporting obligations, and the improvements of its functions, services or activities;
     3. it is required or authorised by Australian Law or a court or tribunal order applies;
     4. it is reasonable in the circumstances to disclose the information to third parties such as government agencies, statutory board, law enforcement agencies, accreditation or registration bodies, independent oversight bodies, regulators, mediators, or conciliators, or to a court or tribunal.
     5. it is reasonable to disclose the information to lessen or prevent a serious threat to the life, health, or safety of any individual, or to public health or safety or welfare of any individual due to domestic violence;
     6. where the University were bound by Australian Privacy Principles and permitted to disclose the information;
     7. the purpose is to provide Students, prospective Students, alumni, Staff, contractors, volunteers and the community with information which may be useful and relevant to them, or about University functions, services, events and activities provided by or on behalf of the University, its partners and affiliates;
     8. it is authorised under the University’s legal obligations and statutory functions under [*Edith Cowan University Act 1984* (WA)](#RelatedDocs); or
     9. it is for a Permitted Purpose and it is not practicable to obtain the agreement of each individual that is the subject of a Personal Data before use or disclosure.
  3. The University may disclose Personal Information:
     1. to various government agencies, including for purposes concerning Student eligibility for support services and payments such as loans under [*Higher Education Support Act 2003* (Cth)](#RelatedDocs), [*Vocational Education and Training Act 1996* (WA)](#RelatedDocs), scholarships, and Centrelink payments;
     2. to the Student Guild for the purpose of enabling the Student Guild to maintain membership details, determine the facilities and services available to Students, and to make those facilities and services available to relevant Students;
     3. to a third party which is:

1. a related body corporate;
2. a placement host or Work Integrated Learning provider;
3. a university collaborator for research or joint delivery of Courses;
4. engaged by the University to assist with the University’s functions, services or activities; or
5. a student exchange or study abroad partner, transnational education service agreement partner, pathway provider, sponsor, education agent or similar.
   * 1. about a prospective Student for the purposes of assessing the effectiveness of marketing or to assist with future marketing;
     2. about a prospective Staff member for the purposes of assessment employability and suitability, including to undertake or verify relevant background checks, or for compliance and accreditation purposes;
     3. to maintain the University’s graduate verification service;
     4. where it is required by the University’s external advisers (including external lawyers, insurer, and risk advisers);
     5. to a person’s next of kin, guardian, or legal representative;
     6. to a Contracted Service Provider for a State, Commonwealth contract, as necessary to meet obligations under the contract; or
     7. in accordance with the University’s [Access to Personal Information for Research Purposes Procedure](#RelatedDocs).

whilst ensuring that wherever practicable, appropriate contractual or technological safeguards are established to protect the Personal Information disclosed;

* 1. The University recognises that Sensitive Information, which includes Health Information, generally requires a higher level of privacy protection, and:
     1. without limiting the above, will ensure that Sensitive Information is appropriately safeguarded, particularly for storage, record keeping, access, and determining whether disclosure is reasonable;
     2. where disclosure occurs, will take such steps as are reasonable in the circumstances to ensure the information is de-identified; and
     3. will ensure that appropriate assessment, safeguards, use plan and engagement with Aboriginal stakeholders will be undertaken regarding Sensitive Aboriginal family history information or Sensitive Aboriginal traditional information.
  2. The University may use or disclose Sensitive Information where:
     1. the person whom the information is about has expressly consented to its use or disclosure;
     2. it is required or authorised by Australian law, a health direction, or a court or tribunal order;
     3. it is reasonable to expect the University to use or disclose the Sensitive Information for a purpose which is directly related to the primary purpose for which the information was collected;
     4. it is reasonable in the circumstances to disclosure the information to entities or bodies such as government agencies, statutory boards, law enforcement agencies, accreditation or registration bodies, independent oversight bodies, regulators, mediators, or conciliators, or to a court or tribunal;
     5. it is reasonable to disclose the information to lessen or prevent a serious threat to the life, health, or safety of any individual, or to public health or safety;
     6. it is reasonable to disclose the information to a person’s next of kin, guardian, or legal representative; or
     7. in instances where the University is bound by the Australian Privacy Principles, or is an “APP entity”, such use or disclosure would be permitted.

#### Direct Marketing[[3]](#footnote-4)

* 1. The University may use or disclose Personal information, other than Sensitive Information, for the purposes of direct marketing, if:
     1. all of the following apply:
        1. the University collected the Personal Information from the individual;
        2. the individual would reasonably expect the University to use or disclose the Personal Information for the purposes of direct marketing;
        3. the University provides a simple means by which the individual may easily request not to receive direct marketing communications; and
        4. the individual has not made such a request.

Or

* + 1. all of the following apply:
       1. the University collected the Personal Information from someone other than the individual;
       2. the individual has consented to the use or disclosure for the purposes of direct marketing,
       3. it is impracticable to obtain that consent from the individual;
       4. the University provides a simple means by which the individual may easily request not to receive direct marketing communications;
       5. the University includes a prominent statement that the individual may make such a request, or draws the individual’s attention to the fact that the individual may make such a request; and
       6. the individual has not made a request.

#### Overseas Disclosure

* 1. The University will only disclose Personal Information or de-identified information in circumstances where disclosure is necessary for contractual obligations or where disclosure is to the benefit of the individual.[[4]](#footnote-5) Circumstance may include situations when:
     1. a student studies or undertake work integrated learning activities abroad;
     2. a student or staff member undertakes official University travel or business abroad; or
     3. the University have contractual or data transfer arrangements with third parties.
  2. Where overseas disclosure is required, the University will take reasonable steps to ensure compliance with appropriate collection, usage and handling safeguards and security detailed within this Policy.
  3. The University may be bound by extra-territorial privacy legislation and standards in some circumstances either because of the nature of work being undertaken or because of its contractual obligations.
  4. It is the responsibility of the contract sponsor to ensure any contract entered into by the University includes appropriate safeguards to comply with this Policy and the protection of Personal and Health Information. Privacy advice from the Privacy Officer and Legal Services must be sought where Personal and Health Information is to be transferred outside of Australia. Where applicable, a Privacy Impact Assessment may be required.
  5. The University will comply with extraterritorial privacy legislation, including the [European Union / United Kingdom General Data Protection Regulation](#RelatedDocs), to the extent it applies to the handling of specific Personal Data by the University.

#### Security[[5]](#footnote-6) and De-identification[[6]](#footnote-7)

* 1. The University will take a proactive approach to manage Personal Information, Sensitive Information (including Health Information) by ensuring appropriate safeguards and protocols are in place:
     1. against information breach incidents including from misuse, interference, loss and from unauthorised access, modification, and disclosure;
     2. follow ‘privacy by design’ approach for processes and system change initiatives;
     3. where relevant undertake a [Privacy Impact Assessment](#RelatedDocs) to appropriately consider and manage privacy risks and impact;
     4. align accountabilities and responsibilities of Relevant Data Owners in line with [Data Governance Framework](#RelatedDocs); and
     5. ensure storage and retention protocols per [Record Management Policy](#RelatedDocs).
  2. The University will take reasonable steps to de-identify or destroy Personal information about an individual where the:
     1. University no longer needs the information for any purpose for which the information may be used or disclosure by the entity under this Policy;
     2. information is not contained in a Commonwealth record; and
     3. University is not required by or under an Australian law, or a court or tribunal order, to retain the information.

#### Access, Quality and Correction[[7]](#footnote-8)

* 1. The University will take steps to reasonably ensure that the Personal Information it collects, uses, or discloses is accurate, up-to-date and complete.
  2. Individuals may request access to their own Personal Information or correction of this Personal Information by contacting the relevant University area, or by application to the Privacy Officer. Such requests will be actioned, provided it is reasonable to do so, within 45 days.[[8]](#footnote-9) If the University determines that it is not reasonable to allow access or amend an individual’s Personal Information, it will inform the individual of the reasons for denial of access or correction.
  3. Individuals may also apply under the [*Freedom of Information Act 1992* (WA)](#RelatedDocs) (**FOI Act**) for an amendment of Personal Information. Further information is set out in the University’s [Freedom of Information Statement](#RelatedDocs).
  4. The University will consider the following when handling applications for access or correction:
     1. [*PRIS Act*](#RelatedDocs) IPP 6.1;
     2. [*Privacy Act*](#RelatedDocs) APP 12;
     3. *FOI Act Exemptions*;
     4. the need for reasonableness;
     5. University policies and procedures (including human resources processes); and
     6. its contractual obligations;

to assess whether access to information is appropriate and whether third party consultation and notifications are required.

* 1. Access and use of Personal Information within the University will only be by University Staff who would reasonably be expected to have access to such information and who have a need to use it to carry out the University’s functions and activities.

#### Automated Decision-Making[[9]](#footnote-10)

* 1. The University, during its functions and activities, may use or engage in third party services that use computer programs, including rule-based systems and artificial intelligence or machine learning technologies, to assist or support in the review of and decision making which could significantly affect individual rights or interest.
  2. The University is committed to ensuring transparency, fairness and accountability of in all automated decision-making (ADM) processes through:
     1. assessment of the impact of the ADM processes; and
     2. regular review to minimise bias and ensure compliance under applicable privacy laws.
  3. Where these decisions relate to eligibility for services, access to benefits, or other outcomes affecting an individual, the University will disclose the following:
     1. Types of personal information used;
     2. Nature of decisions made; and
     3. Human intervention and review controls in place.

#### Information Breach Management

* 1. The University is committed to preventing information breaches and ensuring the protection of the Personal Information it holds. This is achieved through:
     1. appropriate collection, use, disclosure, security and management of Personal Information in accordance with this Policy; and
     2. the University’s [Information Security and Information Technology Policy](#RelatedDocs).
  2. An eligible Information Breach Incident is a potential, suspected or actual incident where there is unauthorised access, or disclosure of Personal Information held by the University:
     1. that is likely to result in serious harm to one or more individuals; and
     2. the University has been unable to prevent the likely risk of serious harm with remedial action.
  3. Individuals aware of an Incident Breach Incident can report this to
     1. ECU IT Service Desk as a Cyber Security Incident; or
     2. the Privacy Officer via an Information breach notification form.
  4. The University will respond as soon as reasonably practicable upon receiving an incident report to manage an Information Breach Incident in the following manner:
     1. assess and prioritise harm prevention to the affected individuals;
     2. review and respond to the incident in line with:
  5. the requirements under the PRIS Act Information Breach Reporting Scheme within 30 days where reasonable and practicable;
  6. the University’s [Cyber Security Incident Response and Information Breach Response procedures](#RelatedDocs);
  7. [Critical Incident and Business Continuity Management](#RelatedDocs) Policy; and
  8. any other legislative or regulatory reporting obligations.
     1. evaluate, treat the cause of the incident to protect Personal Information held by the University; and
     2. review and remediate to prevent and/or reduce the risk of future Information Breach Incidents.

#### Privacy Complaints Handling

* 1. Individuals may lodge a privacy related complaint in accordance with:
     1. the University’s [Complaints Policy, Complaints, Grievances and Incident process](#RelatedDocs); or
     2. by writing to the Privacy Officer (via [privacy@ecu.edu.au](mailto:privacy@ecu.edu.au))

## ACCOUNTABILITIES AND RESPONSIBILITIES

The Director, Strategic and Governance Services is the Policy Owner and has overall responsibility for the content of this policy and its operation.

The Manager, Legal and Integrity is responsible for currency of information and provision of advice relating to operationalising this policy.

The Privacy Officer is the first point of contact for all privacy related matters.

## RELATED DOCUMENTS

#### Legislation

[*Edith Cowan University Act 1984* (WA)](https://www.legislation.wa.gov.au/legislation/statutes.nsf/main_mrtitle_282_homepage.html)

[*Freedom of Information Act 1992*](https://www.legislation.wa.gov.au/legislation/statutes.nsf/main_mrtitle_353_homepage.html) (WA)

[*General Data Protection Regulation* (EU) 2016/679](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679)

[*Health Services Act 2016* (WA)](https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_28638.pdf/$FILE/Health%20Services%20Act%202016%20-%20%5B00-00-01%5D.pdf)

[*Higher Education Support Act 2003* (Cth)](https://www.legislation.gov.au/Details/C2020C00078)

[*Privacy Act 1988* (Cth)](https://www.legislation.gov.au/Details/C2014C00076)

*Privacy & Responsible Information Sharing Act 2024* (WA)

[*Privacy (Tax File Number) Rule 2015*](https://www.legislation.gov.au/Details/F2015L00249)

[*State Records Act 2000* (WA)](https://www.legislation.wa.gov.au/legislation/statutes.nsf/main_mrtitle_924_homepage.html)

[*Vocational Education and Training Act 1996* (WA)](https://www.legislation.wa.gov.au/legislation/statutes.nsf/RedirectURL?OpenAgent&query=mrdoc_47549.pdf)

#### Policies

[Staff Code of Conduct](https://edithcowanuni.sharepoint.com/:w:/s/SGS-CorpKB/ESCieAKYvjdDuzLlbypBM0AB_k8Go67VyjSain_OH1a2Sg)

[Information Security and Information Technology](https://edithcowanuni.sharepoint.com/:w:/s/SGS-CorpKB/EVmAOzCHh1dNgnswKEjwlOoBI81kAr2f4ZZaNt98247Yfw)

[Critical Incident and Business Continuity Management](https://intranet.ecu.edu.au/__data/assets/pdf_file/0010/926254/CI-BCM-Policy-2024-FINAL.pdf)

[Complaints](https://edithcowanuni.sharepoint.com/:w:/s/SGS-CorpKB/EZMuTBxQ0NBGsZbnL1UD22kBmbbVB1pY39B7frcRfd2zJA)

[Grievance Resolution](https://edithcowanuni.sharepoint.com/:w:/s/SGS-CorpKB/EZs7ciU-g1pMprGB20ljyUwB1c6bSUzTRykVnODHWfmGdQ)

[Records Management](https://edithcowanuni.sharepoint.com/:w:/s/SGS-CorpKB/EU2WsFbuz9VJvyfTJGvUWMcBxhUOom4OKzxpzTnMxKQriA)

#### Operational documents and resources

[Access to Personal Information for Research Purposes Procedure](https://www.ecu.edu.au/supplemental/privacy)

[Artificial Intelligence Framework and Ethical Principles](https://www.ecu.edu.au/centres/centre-for-learning-and-teaching/artificial-intelligence-framework)

[Complaints, Grievances and Incidents processes](https://www.ecu.edu.au/complaints/lodge-a-complaint-grievance-misconduct-or-safety-incident)

[Critical Incident and Business Continuity Management Guidelines](https://intranet.ecu.edu.au/__data/assets/pdf_file/0005/926258/CI-BCM-Guidelines-2024-FINAL.pdf)

Critical Incident Plan

[Cyber Security Incident Response Procedure](https://edithcowanuni.sharepoint.com/:w:/r/sites/DCS/_layouts/15/Doc.aspx?sourcedoc=%7B4924C492-2C36-4538-8937-A6734CEF420F%7D&file=ECU%20Cyber%20Security%20Incident%20Response%20Procedure.docx&action=default&mobileredirect=true)

[Freedom of Information Statement](https://www.ecu.edu.au/__data/assets/pdf_file/0006/378438/FOI-Statement.pdf)

[Information Breach Response Procedure](https://www.ecu.edu.au/supplemental/privacy)

Privacy Impact Assessment Procedure

## CONTACT INFORMATION

For queries relating to this document please contact:

|  |  |
| --- | --- |
| Policy Owner: | Director Strategic and Governance Services |
| All Enquiries Contact: | Manager, Legal and Integrity  Privacy Officer – Senior Privacy Risk & Compliance Advisor |
| Telephone: | 08 6304 2158 |
| Email address: | [privacy@ecu.edu.au](mailto:privacy@ecu.edu.au) |

## APPROVAL HISTORY

|  |  |
| --- | --- |
| Policy approved by: | Vice-Chancellor |
| Date policy first approved: | 20 October 2008 |
| Date last modified: | October 2025 |
| Revision history: | **October 2025**  A comprehensive review of the policy was undertaken to ensure it was reflective of the legislative requirements of the *Privacy & Responsible Information Sharing 2024 (WA)*.  **July 2022**  A comprehensive review of the policy was undertaken to ensure it was contemporary and reflective of the University’s legislative requirements with respect to Privacy. Changes were made to address cyber security incidents and data breach management; categories of use and disclosure of personal and sensitive information; overseas disclosure and privacy obligations; and direct marketing.  **20 February 2015**  Revision of the Policy to generally reflect the Australian Privacy Principles which came into effect from 12 March 2014.  Approved by the Vice-Chancellor. Reviewed in consultation with MCSC, OLS, HRSC, ITSC and OGS.  **December 2012**  Minor Amendment as a result of amendments to the Higher Education Support Act.  **September 2012**  Minor amendment to re-word Records staff responsibilities.  **July 2011**  Minor amendments only, addition of new section 4.3 on Records Management and removal of references to the *Information Privacy Bill 2007 (WA)*, update of position titles.  **July 2009**  Added the Statement on Confidentiality of Personal Student Information as a Schedule. |
| Next revision due: | October 2028 |

1. IPP 1 – Collection [↑](#footnote-ref-2)
2. IPP 2 – Use and Disclosure [↑](#footnote-ref-3)
3. APP 7 – Direct Marketing [↑](#footnote-ref-4)
4. IPP 9 – Disclosure outside Australia [↑](#footnote-ref-5)
5. IPP 4 – Information security [↑](#footnote-ref-6)
6. IPP 12 – De-identification [↑](#footnote-ref-7)
7. IPP 3 – Information quality [↑](#footnote-ref-8)
8. IPP 6 – Access and correction [↑](#footnote-ref-9)
9. IPP 10 – Automated decision making [↑](#footnote-ref-10)