Privacy Procedures

1. COMPLIANCE OBLIGATION SUPPORTED

Privacy Policy (forthcoming)

2. PROCEDURAL DETAILS

This document outlines procedures for appropriate collection, use and handling of personal information and sensitive personal information.

2.1 Responsibilities

Refer below.

2.2 Collection of personal information and sensitive personal information

Personal information and sensitive personal information about individuals' interactions with us will be collected, managed and protected in order to allow the University to perform its functions.

2.2.1 Personal information and sensitive personal information will be managed in accordance with relevant Policies and Procedures.

2.2.2 We will only collect personal information and sensitive personal information, which is necessary to perform a function, carry out an activity or offer a service.

2.2.3 Personal information and sensitive personal information will only be collected by fair and reasonable means including collection from:

a) individuals when they interact with us; or

b) through third parties with whom we interact; or

c) remote access to our online materials and online learning; or

d) involvement in any University hosted event, extra-curricular educational, sporting, volunteer or secondment activity;

e) using CCTV; or

f) use of web tracking technologies such as cookies; or

g) use of any service or facility hosted and/or managed by us (for example; student run clinics, childcare services, sporting facility, health or counselling services).

2.3 Use and Storage of personal information and sensitive personal information

2.3.1 Personal and sensitive information will only be used for the purpose for which it was originally collected (primary purpose) or for a secondary use which directly relates to the original reason for which the information was collected. Any other use must be subject to the consent of the individual and may be subject to a *Privacy Impact Assessment*.

2.3.2 Personal information and sensitive personal information about individuals must be given an appropriate information security classification and stored and protected accordingly.

2.3.3 The University and individual areas may use third party storage providers both in Australia and overseas which may include cloud services and will take reasonable steps (including contractual, organisational and technological measures) to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure via those services.

2.3.4 Where the University or individual areas use any third-party storage provider to store, use or disclose personal or sensitive information, an area representative will be required to complete a Privacy Impact Assessment and may also be required to complete a *Security Assessment*

2.3.4 If we no longer need to hold personal information or we are no longer required by law to keep it, we will take reasonable steps to either destroy the information or to ensure that the information is de-identified prior to the decommissioning of systems (See the Information Management Procedures with regards to disposal of information).

2.4 Disclosure of personal information and sensitive personal information

2.4.1 The University will not disclose personal information or sensitive personal information about individuals to another individual or to an organisation or entity unless:

a) the individual would reasonably expect that information to be disclosed in order to perform a function, carry out an activity or offer a service, or

b) the individual has given consent for the disclosure, or

c) the disclosure is necessary in order to inform any audit, analysis, reporting or statistics which furthers research or the functions of the University, or

c) the disclosure is required by law or to prevent or lessen a serious threat to life, health, safety or welfare as defined by the *Australian Privacy Principles (Chapter C and D)*

2.4.2 Where personal information and sensitive personal information is to be shared or disclosed to any individual, entity or service outside of the University (including outside of Australia) then a Portfolio Area Representative should ensure that a Privacy Impact Assessment, and Security Assessment are completed prior to sharing or disclosure.

2.4.3 Any sharing or disclosure outside of Australia is to include a contract or terms of service which are at least the equivalent to Australian privacy laws and principles (including any State, Commonwealth or overseas jurisdictional law which applies to the University).

2.4.4 Any misuse, interference, loss or accidental disclosure, as well as any actual or potential unauthorised access, modification to or disclosure of personal information and sensitive personal information held by the University (including third parties, such as contractors) will be managed as an information breach and will be reported and registered as required under the *Information Breach Policy*.

2.5 Handling personal information and sensitive personal information

2.5.1 Personal information and sensitive personal information which is collected and used for the purposes of research must include a *data management plan* which may require a Privacy Impact Assessment.

2.5.2 Research, statistics or any analytical data which is published or reported must be de-identified or anonymised in such a way that individuals cannot be identified (or reasonably identified) from the published work.

2.5.3 De-identified information received by the University from a third-party may not be re-identified without written authority from that third-party and only for purposes specified in that authorisation, unless it is required by law.

2.5.4 If an individual requests anonymity or pseudonymity, the University will advise that individual of the potential impact of such non-disclosure, including any services, facilities or activities which may not be undertaken or for which identification is considered a requirement of participation.

2.5.5 If any personal information and sensitive personal information collected, stored, used or held by the University is to be used for an automated decision-making process or system (including artificial intelligence, machine learning or process automation), then that process will be subject to a Privacy Impact Assessment and will be subject to appropriate Artificial Intelligence (AI) guidance (once developed) and any other relevant government Policy.

3. SCOPE OF PROCEDURES

This procedure applies to the University Community, including Council members, students, staff, University Associates, Curtin controlled entities, and all persons participating in University business or activities, including whether as a visitor, adjunct appointee, service provider, contractor or volunteer. Global campuses must abide by freedom of information, privacy and any requirements for the management and reporting of data breaches which apply to their jurisdiction.

4. DEFINITIONS

(Note: Commonly defined terms are located in the Curtin Common Definitions. Any defined terms below are specific to this document)

Approved Secondary Use

Using personal information or sensitive personal information for a purpose other than the primary purpose for which the information was obtained.

Consent

Authority provided by an individual for the University to handle their personal information for a particular purpose (for example, granting permission to disclose, use, share or store personal information). The individual must be adequately informed about the specific use or disclosure and must voluntarily give current and specific permission for the proposed use or disclosure. Such consent must be given with capacity to understand and communicate that consent.

Disclose

The University discloses your personal information when they give access to it or show it to another individual, organisation or agency.

Area Representative

The staff member, officer or project manager within an area of the University who is responsible for a project, activity, task or action.

Potential unauthorised access

Any circumstance where it is possible that someone may have gained access to a computer system, network, or data in error or without permission, including loss of a device or suspected access.

Sensitive personal information

A classification of personal information that includes a person's racial or ethnic origin; political opinions or memberships of a political association; religious or philosophical beliefs or affiliations; membership of a professional or trade association or union; sexual orientation or practices; criminal records; genetic, health or biometric information.

5. RELATED DOCUMENTS/LINKS/FORMS

- Curtin University Cookies Statement
- *Disclosure of Personal Information Procedures*
- *Freedom of Information Act 1992 (WA)*
- *Information Breach Policy*
- *Information Breach Procedures*
- *Information Management Policy*
- *Information Management Procedures*
- *Information Security and ICT Appropriate Use Policy*
- *Information Security Classification Policy*
- *Information and Communication Technology ICT Appropriate Use Procedures*
- *Privacy Act 1988* (Cth)
- *Privacy and Responsible Information Sharing Act* (WA)
- *Research Data and Primary Materials Policy*

- *Research Management Policy*
- *State Records Act 2000* (WA)

Policy Compliance Officer	Krista Bell, Director, Data & Information Governance
Policy Manager	Chief Operating Officer
Approval Authority	Chief Operating Officer
Review Date	1st April 2028

REVISION HISTORY (*filled out by Risk, Compliance and Audit*)

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
	Approved	19/12/2024	Chief Operating Officer	EM2433	