



Information Breach Policy

1. COMPLIANCE OBLIGATION SUPPORTED

[Curtin University Act 1966 \(WA\)](#)

[Privacy Act 1988 \(Cth\)](#)

[Higher Education Support Act 2003 \(Cth\)](#)

[Student Identifiers Act 2014 \(Cth\)](#)

[Freedom of Information Act 1992 \(WA\)](#)

[Privacy \(Tax File Number\) Rule 2015 \(Cth\)](#)

2. PURPOSE

To set out how the University community will secure and protect personal information and sensitive personal information and to support procedures which ensure that the University community responds to an information breach in a timely and effective manner, minimizing any potential harm to individuals and the University.

3. POLICY STATEMENT

3.1 The University community is responsible for handling personal information and sensitive personal information in accordance with this policy and any related [Policies and Procedures](#).

3.1.1 Third-party vendors and contractors entrusted with personal information and sensitive personal information must adhere to contractual agreements and to University Policies and Procedures to protect the confidentiality and integrity of the information.

3.1.2 Personal information and sensitive personal information will be stored securely in accordance with requirements set out in relevant University Policies and Procedures.

3.2 The University will ensure that staff, students and the University Community are provided with access to training and guidance to ensure they understand their responsibilities and obligations under this Policy and relevant privacy laws.

3.3 The University is committed to adherence to the [Australian Privacy Principles \(APPs\)](#) contained in the [Privacy Act 1988 \(Cth\)](#) and will ensure that the University community is adequately informed of their obligations.

3.4 The University will collect, store, use and protect personal information and sensitive personal information of individuals in a way which is compliant with the Australian Privacy Principles and any other applicable Australian Privacy law, or relevant jurisdictional law for overseas locations (e.g., General Data Protection Regulations (GDPR)).

3.4.1 The University will implement and regularly review reasonable measures to prevent information breaches.

3.4.2 The University will provide a privacy collection notice regarding the use and disclosure of personal information and sensitive personal information.

3.5 Personal information and sensitive personal information will be retained only for as long as necessary to fulfill the purposes for which it was collected or as required by law. When no longer needed, reasonable steps will be taken to destroy the information in accordance with the [Information Management Procedures](#) or to ensure that the information is de-identified prior to the decommissioning of systems.

3.6 Cybersecurity procedures will be established to promptly respond to and investigate any actual or potential unauthorised access or modification to University systems or loss or disclosure of information held within University systems.

- 3.7 In the event of any misuse, interference, loss or accidental disclosure, as well as any actual or potential information breach (including unauthorised access, modification to or disclosure of personal information and sensitive personal information) held by the University (including its affiliates and contractors) the University will respond in accordance with the [Information Breach Procedures](#).

4 SCOPE OF POLICY

This policy 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.

5. DEFINITIONS

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

Disclose

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

Information Breach

Any unauthorised access to personal information or sensitive personal information, or any unauthorised or accidental disclosure of personal information or sensitive personal information, or any loss of personal information or sensitive personal information which is likely to result in serious harm to any individual.

Privacy Collection Notice

A statement that is provided to an individual at the time an organisation collects personal information from them (or as soon as possible after the information is collected). A collection notice explains the purpose for which the information is collected, and how the organisation will use and handle the information.

Potential information breach

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.

6. SUPPORTING PROCEDURES

Information Breach Procedures (forthcoming)

7. RELATED DOCUMENTS/LINKS

- [Curtin Information Statement](#)
- [Privacy Policy](#)
- [Privacy Procedure](#)
- [Information and Communication Technology \(ICT\) Appropriate Use Procedures](#)
- [Information Management Policy](#)
- [Information Security and Information and Communication Technology \(ICT\) Appropriate Use Policy](#)

- [Information Security Classification Policy](#)
- [Information Security Classification Decision Matrix](#)
- [Information Security Classification Flowchart](#)
- [Privacy Advice – Student Confidentiality](#)
- [Research Data and Primary Materials Policy](#)
- [Student’s Privacy Collection Notice](#)
- [Investigate a Privacy Data Breach](#)
- [Australian Privacy Principles](#)
- [Criminal Code Act Compilation Act 1913 \(WA\)](#)
- [Electronic Transactions Act 2011 \(WA\)](#)
- [Evidence Act 1906 \(WA\)](#)
- [Freedom of Information Act 1992 \(WA\)](#)
- [Privacy Act 1988 \(Cth\)](#)
- [State Records Act 2000 \(WA\)](#)
- [WA Government Information Classification Policy](#)
- [Privacy and Responsible Information Sharing Act 2024 \(WA\)](#)

| | |
|----------------------------------|---|
| Policy Compliance Officer | Krista Bell , Director, Data & Information Governance |
| Policy Manager | Chief Operating Officer |
| Approval Authority | Senior Executive Team |
| Review Date | 1 st April 2030 |

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 | 12/12/2024 | Senior Executive Team | SET 109/24 | Attachment B to Item 5.1 |