

# Privacy Policy

## Section 1 - Purpose

(1) This policy affirms RMIT's commitment to privacy and its approach to the responsible handling of personal, sensitive and health information in all its forms, consistent with relevant legislation.

## Section 2 - Overview

(2) RMIT values the privacy of every individual and is committed to the responsible handling of personal, sensitive, and health information in accordance with relevant privacy laws.

(3) As a public university established under Victorian law, RMIT's privacy obligations are primarily governed by the [Privacy and Data Protection Act 2014](#) (Vic) and the [Health Records Act 2001](#) (Vic). RMIT or its controlled entities may be required to comply with other privacy regulations in other jurisdictions to the extent they apply to its activities, including the [Privacy Act 1988](#) (Cth), the Vietnam Decree on Personal Data Protection (PDPD), and the European Union General Data Protection (GDPR).

(4) This policy outlines:

- a. the principles that direct privacy management at RMIT, and
- b. the responsibilities of RMIT, its staff, students, researchers, and affiliates when handling personal, sensitive and health information (collectively referred to as personal information) on behalf of RMIT across all its locations.

## Section 3 - Scope

(5) Throughout this policy and its associated procedures, RMIT means the RMIT Group. The RMIT Group is defined as RMIT University and its controlled entities (e.g. RMIT Vietnam, RMIT Europe, RMIT Online and RMIT UP).

(6) This policy applies to all staff, students, researchers, and any individuals who collect, manage or handle personal information on behalf of the RMIT Group, including service providers.

(7) This policy applies to the handling of personal information, regardless of how it is collected, processed, or stored (or whether it is hardcopy, electronic, or by verbal means).

## Section 4 - Policy

### Principles

(8) RMIT values the privacy of individuals and will foster a positive and respectful privacy culture that builds trust with staff, students, and individuals with whom it interacts.

(9) RMIT will apply and adhere to the Information Privacy Principles under the [Privacy and Data Protection Act 2014](#) (Vic), the Health Privacy Principles under the [Health Records Act 2001](#) (Vic), and any other relevant laws as they apply

to the entities, functions and activities of the RMIT Group.

(10) RMIT adopts a privacy by design approach and aims to proactively embed privacy requirements into its systems, processes and practices.

(11) RMIT prescribes its approach to responsible and transparent handling of personal information across the RMIT Group in an accessible [RMIT Privacy Statement](#).

(12) RMIT ensures those covered by the scope of this policy are made aware of their responsibilities and will provide appropriate information and compliance training opportunities.

## **Responsibilities**

(13) Privacy is everyone's responsibility. All individuals who handle personal information for or on behalf of RMIT have a responsibility to:

- a. comply with the requirements of this policy, the procedures and resources under this policy, the [Information Governance Policy](#) and the [Information Technology and Security Policy](#)
- b. ensure that personal information in their control is protected against loss, unauthorised access, use, modification or disclosure, or any other misuse
- c. notify the Privacy Office of actual or suspected privacy breaches in accordance with the Privacy Breach Management Procedure.

(14) Managers and supervisors are responsible for ensuring all staff within their team handle personal information in accordance with this policy and the procedures and resources under this policy.

(15) In addition to the responsibilities set out in section 14, Heads of Department/Heads of School are responsible for:

- a. overseeing and being accountable for the management of personal information within their respective portfolio/area
- b. appointing Privacy Champions to perform the responsibilities outlined in section 16 of this policy
- c. implementing and monitoring corrective and/or preventative actions recommended by the Chief Privacy Officer in relation to a privacy breach or complaint.

(16) Privacy Champions appointed under section 15b are responsible for:

- a. ensuring that privacy procedures implemented to support this policy are applied in the management of personal information within their respective portfolio/area
- b. implementing effective local procedures to ensure that personal information held is managed in accordance with this policy
- c. ensuring that any person who has access to personal information held within their area understand their responsibilities in regard to such information
- d. assisting and supporting the investigation of privacy complaints and/or breaches
- e. promoting a culture of privacy that values and protects personal information
- f. providing a point of contact for the Privacy Office and assisting with the cascading of privacy communications to staff within their respective portfolio/area.

(17) The Privacy Office is responsible for:

- a. developing and maintaining the privacy management framework to enable communication and implementation of applicable privacy requirements

- b. developing procedures, guidelines, training, and other supporting materials to support this policy and awareness of obligations imposed by applicable privacy laws
- c. providing advice and leadership to Privacy Champions and other internal stakeholders on the obligations imposed by applicable privacy laws across the RMIT Group
- d. reviewing and advising on privacy impact assessments
- e. investigating and responding to privacy breaches, incidents and complaints
- f. issuing and maintaining the [RMIT Privacy Statement](#) and core collection statements
- g. providing a central contact point for and on behalf of the RMIT Group for privacy related matters.

(18) The Executive Director, Governance, Legal and Strategic Operations is responsible for making determinations on external reporting on the recommendation of the Head of Compliance, Privacy and Contract Services in the event of a privacy breach.

(19) The Chief Data and Analytics Officer is responsible for overseeing information governance at RMIT to ensure effectiveness and fit for purpose.

(20) The Chief Information Security Officer oversees information security controls and responses to enable RMIT to deliver effective protection of personal information held by RMIT consistent with privacy management obligations.

## Compliance

(21) The Head of Compliance, Privacy and Contract Services monitors compliance with this policy and reports on complaints and breaches of this policy to internal governance bodies and external agencies, as required.

(22) This policy, as well as procedures under this policy, include consideration of compliance requirements from the following legislation:

- a. [Privacy and Data Protection Act 2014](#) (Vic)
- b. [Health Records Act 2001](#) (Vic)
- c. [Privacy Act 1988](#) (Cth)
- d. General Data Protection Regulation (EU)
- e. Decree No. 13/2023/ND-CP on Persona Data Protection (VN)
- f. [Freedom of Information Act 1973](#) (Vic)
- g. [Public Records Act 1973](#) (Vic).

## Section 5 - Procedures and Resources

(23) Refer to the following documents, which are established in accordance with this policy:

- a. [Privacy Procedure](#)
- b. [Privacy Breach Management Procedure](#)
- c. [RMIT Privacy Statement](#)
- d. [Staff Privacy Statement](#)
- e. [Student Privacy Statement](#)
- f. [Recruitment Privacy Statement](#)

(24) Local resources are available via the [Privacy website](#).

## Section 6 - Definitions

(Note: Commonly defined terms are in the RMIT Policy Glossary. Any defined terms below are specific to this policy).

Core collection statements	Includes the RMIT <a href="#">Staff Privacy Statement</a> , RMIT <a href="#">Student Privacy Statement</a> , and RMIT <a href="#">Recruitment Privacy Statement</a> published on RMIT's website and in RMIT applications and systems.
Health information	Information or an opinion about an individual's physical, mental or psychological health; a disability; health services provided or future provision of health services; and a variety of other health matters (including information about organ or body substance donation and genetic information).
Personal information	Information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Typically, this includes information like name, date of birth, address, phone number etc. For the purposes of this policy and related procedures, reference to personal information includes sensitive and health information.
Privacy by design	The means for ensuring privacy protections are integrated in process and technology design.
Sensitive information	A special category of personal information that requires more protection. It includes the following information about an individual: racial or ethnic origin; political opinion; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preference or practices; criminal record.

## Status and Details

Status	Not Yet Approved
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	
Approval Date	To Be Advised
Expiry Date	Not Applicable
Policy Owner	Fiona Notley Chief Operating Officer
Policy Author	Briony Lewis Executive Director, Governance, Legal and Strategic Operations
Enquiries Contact	Privacy Office

## Glossary Terms and Definitions

**"RMIT Group"** - RMIT University and its controlled entities (RMIT Europe, RMIT Online, RMIT Vietnam, RMIT University Pathways)