

# Privacy Policy

Category	Governance
Effective date	1 July 2019
Review date	6 May 2022
Owner	Chief Financial Officer
Author	Chief Audit and Risk Officer
Version no.	1.1
Contact	<a href="mailto:privacy@rmit.edu.au">privacy@rmit.edu.au</a>
Register reference	POL/2019/00061

## 1. Purpose

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.

## 2. Overview

RMIT University is a public-sector organisation under Victorian law and stands on Aboriginal Country of the Kulin Nation. RMIT recognises and acknowledges the Bundjil Statement that helps all RMIT staff to respectfully work, live and study on Aboriginal Country.

RMIT is required to comply with the *Privacy and Data Protection Act 2014 (Vic)* and *Health Records Act 2001 (Vic)* in respect to the handling of personal, sensitive and health information. RMIT controlled entities in Australia are also required to comply with the *Privacy Act 1988 (Cth)* and will comply with the Victorian laws when handling personal, sensitive and health information. This policy is modelled on Australian and international privacy requirements, recognising that extra-territorial privacy obligations extend to RMIT's global activities and operations, including RMIT Europe and RMIT Vietnam.

This policy outlines:

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

## 3. Scope

This policy applies to all staff, students, researchers and affiliates of the RMIT Group including contractors and partners providing services on behalf of RMIT.

## 4. Principles

- 4.1. RMIT values the privacy of individuals and will foster a positive and respectful privacy culture which supports a relationship of trust between RMIT and staff, students, researchers and third parties.

- 4.2. RMIT will apply and adhere to the Victorian Information Privacy Principles (IPP), the Victorian Health Privacy Principles (HPP), the Australian Privacy Principles (APP), and any other relevant laws as they apply to the entities, functions and activities of the RMIT Group. To the extent that inconsistencies or differences might exist in the global context, best practice privacy management will guide RMIT's actions to achieve compliance.
- 4.3. RMIT adopts a privacy by design approach, proactively incorporating privacy requirements, ensuring compliance with law, and enabling continuous improvement of privacy practices.
- 4.4. RMIT will prescribe its approach to responsible and transparent handling of personal information across the RMIT Group in an accessible RMIT Privacy Statement.
- 4.5. RMIT will ensure those covered by the scope of this policy are made aware of their responsibilities and will provide appropriate information and compliance training opportunities.

## 5. Responsibilities

- 5.1. Privacy is everyone's responsibility and all staff, students, researchers and affiliates have an obligation to manage personal information collected, accessed, used, re-used or disclosed during their engagement with RMIT in accordance with this policy, the RMIT Privacy Statement, and associated information security, information management and data governance policies.
- 5.2. Managers are required to ensure that privacy principles and practices are implemented locally, and suspected or actual breaches of this policy are reported in accordance with the Compliance Breach Management Procedure.
- 5.3. The RMIT Privacy Office is responsible for:
  - a) establishing the privacy management framework to enable communication and implementation of applicable privacy requirements
  - b) reviewing privacy impact assessments
  - c) providing privacy training, other education programs and advice
  - d) monitoring compliance with this policy and reporting on complaints and breaches of this policy to internal governance bodies and external agencies, as required
  - e) investigating privacy breaches, incidents or complaints
  - f) appointing a Chief Privacy Officer who issues and maintains the RMIT Privacy Statement and core collection statements
  - g) providing a central contact point for and on behalf of the RMIT Group.
- 5.4. The Chief Information Security Officer oversees information security controls and responses to enable RMIT to deliver effective protection of personal data held by RMIT consistent with privacy management obligations across all its operations.
- 5.5. The Chief Financial Officer is responsible for making determinations on external reporting on the recommendation of the Chief Privacy Officer or Chief Audit and Risk Officer, in the event of a privacy breach.
- 5.6. The Privacy Office monitors compliance with this policy and reports on complaints and breaches of this policy to internal governance bodies and external agencies, as required.

## 6. Review

- 6.1. The Chief Privacy Officer will review this policy at least every three years in accordance with the Policy Governance Framework, and review and update the RMIT Privacy Statement annually.

## 7. Definitions

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

<b>Core collection statements</b>	Includes the RMIT Staff Privacy Statement and Student Privacy Statement published on RMIT's Policy Register and in RMIT applications and systems.
<b>Health information</b>	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).
<b>Personal data</b>	Refers to any information relating to an identified or identifiable natural person, directly or indirectly, 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. (Article 4, GDPR Regulations).
<b>Personal information</b>	Information or an opinion, that is recorded in any form 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. Personal information includes personal data.
<b>Privacy by design</b>	The means for ensuring privacy protections are integrated in process and technology design.
<b>Sensitive information</b>	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.

## 8. Procedures and resources

- RMIT Privacy Statement
- Compliance Breach Management Procedure
- Privacy Impact Assessment Process and template
- EU General Data Protection Regulation FAQs

## Document history

Version	Approval date	Effective date	Summary of changes	Approval authority
1.0	6 May 2019	1 July 2019	New policy	ARMC
1.1	15 November 2019	1 July 2019	Editorial amendment	UPM

## See also

- Compliance Policy [in development]
- Information Management and Data Governance Policy [in development]
- Information Technology Policy