Compliance Breach Management Procedure

Section 1 - Context

(1) This procedure details the requirements for identifying, assessing, remediating, reporting and recording breaches of compliance obligations in accordance with the Compliance Policy.

Section 2 - Authority

(2) Authority for this document is established by the Compliance Policy.

Section 3 - Scope

(3) This procedure applies to all staff, including researchers, affiliates, contractors and volunteers of the RMIT Group.

(4) It does not apply to allegations of breaches of the Code of Conduct, which are handled under separate policies.

(5) Breaches relating to the Code of Conduct, such as staff misconduct, are reported in accordance with the Complaints Governance Policy. Student-related complaints are made in accordance with the Student and Student-Related Complaints Policy.

Section 4 - Procedure

Policy Governance

(6) RMIT policies and procedures governing a specific type of breach or critical incident response may take precedence over this procedure. However, the requirements for reporting and recording (clauses 14-19) apply to all types of breaches.

Identifying and Responding to Compliance Breaches

(7) All RMIT staff who identify or suspect a breach must report it to their manager or supervisor as soon as practicable. All evidence relating to the breach must be retained and secured for the Legislative Owner to consider in the assessment of the breach.

(8) Managers must report the identified or suspected breach to the relevant Legislative Owner or Legislative Specialist, as listed in the Legislative Obligations Register, and the Head of Compliance, Privacy and Contract Services.

(9) If staff are unable to discuss a breach with their manager or supervisor, they must report the breach directly to the relevant Legislative Owner or Legislative Specialist, and/or the Head of Compliance, Privacy and Contract Services.

(10) Staff who wish to make a confidential or anonymous disclosure about an identified or suspected compliance breach should make the disclosure directly to Central Compliance (compliance@rmit.edu.au), unless there is a

corruption or fraud concern (see clause 27).

(11) Staff who are aware of a breach and fail to report it may be subject to disciplinary action in accordance with the Code of Conduct and relevant RMIT policies.

(12) Where reasonable and practicable, immediate action must be taken to contain the breach. This may include stopping unauthorised practices, recovering any records, implementing safety measures, etc. In certain cases, action may be required before the matter can be reported.

(13) Where incidents or breaches relate to high risk regulatory activities, the Compliance Escalation Guide must be followed.

Assessing and Remediating Compliance Breaches

(14) Legislative Owners are responsible for assessment of compliance breaches. The Legislative Owner assesses the nature, scale and impact of breaches with reference to risk management protocols and determines the appropriate course of action. Where there is a concern about a conflict of interest, the Legislative Owner may seek advice from the Head of Compliance, Privacy and Contract Services.

(15) The assessment identifies root causes and determines whether the breach is an isolated or systemic issue. It identifies corrective or preventative actions to mitigate or eliminate the impact of the breach and likelihood of recurrence.

(16) Breaches that may give rise to a risk of harm to individuals must be evaluated to determine likelihood and severity. This informs corrective action and determines if an external agency needs to be notified.

(17) Corrective or preventative action plans for breaches of privacy and personal data security must be endorsed by the Privacy Office and Office of the Chief Information Security Officer.

(18) The implementation of corrective or preventative actions is approved and monitored by the Legislative Owner. Regular updates on implementation of the action plan must also be provided to the Central Compliance Team.

(19) Staff who may have access to confidential or personal information during breach management must comply with the Privacy Policy and the Information Governance Policy.

Recording and Reporting Compliance Breaches

(20) Suspected or actual breaches must be reported to the Central Compliance Team by Legislative Owners as soon as practicable, with timelines for assessment of the breach to ensure that any independent investigation, as necessary or required, commences in a timely manner.

(21) Breaches relating to high risk regulatory activities must also be reported to the compliance management contact identified in the Compliance Escalation Guide.

(22) Material breaches relating to high-risk regulatory activities must be reported to the relevant governance body – Academic Board, Audit and Risk Management Committee or Council.

(23) The Legislative Owner must report compliance obligation breaches to the relevant government department or external regulatory agency within the legislated timeframe, when mandatory. Before any disclosure is made, approval must be obtained from the Executive Director, Governance, Legal and Strategic Operations and advice sought from them on the reporting process.

(24) The Executive Director, Governance, Legal and Strategic Operations reports on identified compliance breaches to the Audit and Risk Management Committee no less than twice per year in accordance with the approved schedule.

(25) The Central Compliance Team retains a record of breaches and outcomes in the RMIT Compliance Breach Register.

Public Interest Disclosure

(26) Breaches caused by suspected or confirmed corruption must follow the Anti-Corruption and Fraud Prevention Policy and Whistleblower Procedure.

Section 5 - Resources

(27) Refer to the following documents which are established in accordance with this procedure:

a. Compliance Procedure
b. Compliance Escalation Guide.

Section 6 - Definitions

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

Breach	A failure to meet the clauses, principles, or requirements of regulatory, contractual and legislative obligations or RMIT policies and procedures. Significant or material breaches may be reportable to an external agency or regulator. See also: Material breach
Compliance Breach Register	A record of breaches of RMIT's compliance obligations, managed by the Central Compliance team.
Compliance	Meeting all requirements of laws, regulations, statutes, standards and policies.
Compliance management	The coordinated institutional approach to identifying, assessing, managing, monitoring, and reporting compliance obligations, risks and performance across the RMIT Group.
Compliance obligation	Refers to any legal, regulatory, contractual or internal requirement that RMIT must adhere to. This includes obligations arising from legislation, regulations, standards, contracts, codes of practice, and internal policies and procedures that govern RMIT's operations and activities and ensures that RMIT meets its responsibilities to staff, students, government bodies and the broader community.
Legislative Owner	Legislative Owners are senior officers responsible for compliance with specific obligations and provide leadership to ensure requirements are met. They are accountable for guiding the implementation of compliance processes, systems and controls within their area, as well as implementing compliance action plans. Additionally, they are responsible for nominating Legislative Specialists for the Central Compliance Team to liaise with.
Legislative Specialist	Subject-matter experts with operational knowledge of how specific legislation or Acts apply to RMIT. They support the Legislative Owner in implementing the Compliance Policy, provide advice about specific legislation, and are responsible for facilitating or undertaking assessments against obligations.
Material breach	A severe and significant breach, in terms of scale and/or regulatory requirements, or with implications for safety and security, and/or legal requirements. See also: Breach.

Status and Details

Status	Current
Effective Date	3rd February 2025
Review Date	3rd February 2030
Approval Authority	Manager, Central Policy
Approval Date	12th December 2024
Expiry Date	Not Applicable
Policy Owner	Fiona Notley Chief Operating Officer
Policy Author	Briony Lewis Executive Director, Governance, Legal and Strategic Operations
Enquiries Contact	Central Compliance

Glossary Terms and Definitions

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