Information Governance Policy

Establishes the framework for the governance and management of information at RMIT

<table>
<thead>
<tr>
<th>Policy category</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective date</td>
<td>1 October 2019</td>
</tr>
<tr>
<td>Review date</td>
<td>3 September 2022</td>
</tr>
<tr>
<td>Owner</td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>Author</td>
<td>Chief Data &amp; Analytics Officer</td>
</tr>
<tr>
<td>Version no.</td>
<td>1.1</td>
</tr>
<tr>
<td>Contact</td>
<td><a href="mailto:analyticsandinsights@rmit.edu.au">analyticsandinsights@rmit.edu.au</a></td>
</tr>
<tr>
<td>Register reference</td>
<td>POL/2019/00068</td>
</tr>
</tbody>
</table>

1. Purpose

This policy establishes the framework and principles for effective information governance which supports the functions and activities of the RMIT Group.

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 committed to managing information as an organisational asset which is created, used and shared effectively whilst meeting legislative requirements.

Information Governance provides the framework, strategic objectives, policies and standards to manage information as an asset. This policy and supporting procedures and resources support the strategic plan of the organisation to drive outcomes and support continuous improvement and ultimately optimise integrity, security, availability and quality of information.

3. Scope

This policy applies to all RMIT staff including staff of controlled entities, students, temporary employees, contractors, visitors and third parties globally who manage RMIT information with the exception of research data as defined by the Research Policy.

4. Principles

4.1. RMIT is the custodian of all information managed by the RMIT Group. No individual function or group own any part of data or information.

4.2. RMIT will take reasonable and necessary steps to ensure information security protection. Information Security Classifications will enable appropriate management of information.
4.3. RMIT Information will be
   a) collected, created, managed, used, re-used and shared according to ethical practices, any
      applicable laws and with due consideration to individual privacy.
   b) appropriately stored to ensure protection from loss and unauthorised access.
   c) accessible, transparent and available to be used and shared whilst respecting matters of
      identity, privacy and confidentiality. This applies to internal as well as third party data.
   d) managed in accordance with records management and archiving requirements.

4.4. RMIT will implement procedures and practices to ensure all information is captured accurately and
     completely and managed throughout its lifecycle.

4.5. RMIT will provide access to formal or informal learning material to ensure staff have the
     knowledge, competencies and ability to interact with information in their roles.

5. Responsibilities

5.1. Information governance is overseen by the Chief Data & Analytics Officer (CDAO) with sponsorship
     of the Vice Chancellor’s Executive (VCE).

5.2. The Information Governance Board (IGB) provides an information governance forum for the RMIT
     Group.

5.3. The Information Trustees are accountable for their respective domain area as set out in the
     Information Domain Register.

5.4. The Information Stewards Group (ISG) provide operational support and recommendations to the
     Information Governance Board.

5.5. The Information Stewards are responsible for identifying and managing information related risks
     and issues for their assigned information entities and for escalating these to the data trustees
     accordingly.

5.6. All RMIT staff including staff of controlled entities, students, temporary employees, contractors,
     visitors and third parties are responsible for:
     a) ensuring the quality and completeness of information which they collect or create
     b) ensuring that they understand and adhere to procedures and resources under this policy
        which govern the management, control, storage, transfer and destruction of information
        throughout its lifecycle
     c) supporting a culture that promotes good information governance practices and reporting
        any identified compliance breaches or incidents
     d) managing RMIT information in accordance with the Privacy Policy and Information
        Technology Policy.

6. Compliance

6.1. Investigations of breaches of this policy or non-compliance with legislation are undertaken in
      accordance with the Compliance Breach Management Procedure.

6.2. This policy is to be read in conjunction with existing university policy documents which include but
      are not limited to the following:
      a) Research Policy
7. Review

7.1. The Information Governance Board will review this policy annually and undertake a major review every three years in accordance with the Policy Governance Framework.

8. Definitions

<table>
<thead>
<tr>
<th>Data</th>
<th>Data is a fundamental component of information. It forms the building blocks of information. Data includes metadata, reference data and derived data. The definition of data in this policy excludes ‘Research Data’ as defined and governed by the Research Policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Information is data in context which has relevance and is timely.¹ For the purpose of this policy, the term ‘information’ refers to information, records and data, with the exception of ‘Research Data’ as defined and governed by the Research Policy.</td>
</tr>
<tr>
<td>Records</td>
<td>Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.² Records include (but are not limited to) emails, documents, websites, photographs, conversations undertaken via Instant Messaging clients, meeting minutes, research data, posts to RMIT social media sites.</td>
</tr>
<tr>
<td>Chief Data &amp; Analytics Officer (CDAO)</td>
<td>The Chief Data &amp; Analytics Officer is appointed to provide organisation-wide oversight of all data and information related functions. This includes providing strategic guidance for data governance across the whole organisation including information management, records management, data quality management, analytics, business intelligence, data security and data privacy.</td>
</tr>
<tr>
<td>Information Governance Board (IGB)</td>
<td>The IGB recognises information as a valuable asset and advocates for information governance. The IGB endorses strategy, provides strategic advice for information governance activities and issues, monitors progress against strategy, ensure risks are managed and that decisions are made in accordance with all applicable policies and regulations. Further details are set out in the Information Governance Board Terms of Reference.</td>
</tr>
</tbody>
</table>

### Information Trustee
An information trustee is accountable for one or more domains of RMIT’s information. This accountability is outlined in the Information Domain Register. The information trustee may delegate the management and handling of operational responsibilities associated with the information asset to an information steward.

### Information Stewards Group (ISG)
The ISG is comprised of Information Stewards who provide operational oversight of information governance activities, identify information governance issues, identify opportunities for improvement, provide support for resolving issues and harnessing opportunities and escalating these to the IGB where appropriate for comments, decisions, approval or sponsorship. Further details are set out in the Information Stewards Group Terms of Reference.

### Information Steward
An information steward is responsible for ensuring that information assigned to them by the information trustee is meeting RMIT’s requirements. This includes monitoring, managing and escalating any risks and issues associated with the information.

### 9. Procedures and resources
- Data Ethics Framework
- Information Domain Register
- Key Term Definition Standard
- RMIT Retention and Disposal Authority
# Schedule 1: RMIT’s Security Classification Levels

<table>
<thead>
<tr>
<th>Classification</th>
<th>Definition</th>
<th>Operational Impact if compromised</th>
<th>Examples</th>
</tr>
</thead>
</table>
| **Restricted** | Information that is highly sensitive and intended to be used by a small, limited number of authorised individuals on a need-to-know basis. | Unauthorised disclosure may result in extreme or severe impact to RMIT such as:  
- Severe financial harm  
- Significant harmful reputational damage  
- Extreme regulatory penalties or loss of key licenses and/or funding  
- Significant interruption of critical operational system/processes  
- Significant impact to research activity  
- Severe risks to the safety or wellbeing of individuals | Security vulnerabilities, confidential out-of-court settlements, records affecting national security, protected disclosures, unpublished cybersecurity research, Records including the following government issued unique identifiers that identify individuals: driver’s license number, national identification number, Centrelink account number, Tax file number, Medicare account, Passport number. |
| **Protected** | Information that is personal and/or sensitive and intended to be used by authorised individuals for an authorised purpose on a need-to-know basis | Unauthorised disclosure may result in severe or major impact to RMIT such as:  
- Major financial harm  
- Major harmful reputational damage  
- Major regulatory penalties or loss of key licenses and/or funding  
- Major interruption of critical operational system/processes  
- Major impact to research activity  
- Major risks to the safety or wellbeing of individuals | Information relating to ongoing commercial or research projects where disclosure could jeopardise the project, personal identifiable information, unreleased student results, banking details, information related to discipline, grievances, salary information, audit reports, strategic and governance documentation, medical and health information |
| **Trusted (default)** | Information that is intended to be used internally in the day-to-day operations of RMIT | Unauthorised disclosure may result in moderate or minor impact to RMIT such as:  
- Minor financial harm  
- Minor harmful reputational damage  
- Minor regulatory penalties or loss of key licenses and/or funding  
- Minor interruption of critical operational system/processes  
- Minor impact to research activity  
- Minor risks to the safety or wellbeing of individuals | User manuals, training manuals and documentation, employee newsletters, meeting minutes, de-identified clinical research |
| **Public** | Information which has been authorised by the trustee for public access and circulation | Unauthorised disclosure causes minor or negligible impact to RMIT | Information authorised to be available on or through RMIT’s website, publicly available campus brochure, publicly available campus map, published annual report, information in the public domain, job postings |
Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Effective Date</th>
<th>Summary of Changes</th>
<th>Approval Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>3 September 2019</td>
<td>1 October 2019</td>
<td>New policy</td>
<td>ARMC</td>
</tr>
<tr>
<td>1.1</td>
<td>15 November 2019</td>
<td>1 October 2019</td>
<td>Editorial amendment</td>
<td>UPM</td>
</tr>
</tbody>
</table>

See also

- Compliance Breach Management Procedure
- Information Technology Policy
- Intellectual Property Policy
- Research Policy
- Privacy Policy
- Research Data Management Procedure