Policy

Title	**INFORMATION AND DATA MANAGEMENT AND SECURITY**		
Classification	Board	**Oversight Responsibility**	Office of the President
Category	Governance	**Responsible Office**	Office of the Vice President, Finance and Operations
Approval	Board of Governors	**Effective Date**	June 20, 2024
		Document No.	1097

This policy is applied in a manner consistent with applicable statutory and legal obligations, including university collective agreements and terms of employment.

The most up-to-date versions of the University's policies are posted on the policy and procedure website. If you have printed this policy, please check the website to ensure you have the current version.

The first appearance of terms in **Bold** in this document (except titles) are defined terms – refer to the Definitions section.

1.0 POLICY STATEMENT

The Board of Governors (Board) of Royal Roads University (University) is committed to upholding its duties, obligations, and responsibilities for the **management** and **security** of **information** and **data** in its control and/or custody, regardless of its **form** and **storage medium**. In fulfillment of this commitment, the Board requires the adoption and implementation of robust direction that meets or exceeds applicable federal and provincial legislation, and industry standards to support and safeguard information and data throughout the University.

2.0 SCOPE AND COMPLIANCE

This policy extends to **members of the University community**.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, contract, or other relationship with the University. Any disciplinary action is taken in consideration of the applicable laws, legislation, collective agreement, or contract.

3.0 POLICY TERMS

To ensure the Board and the University meet its duties, obligations, and responsibilities, direction provided to the University community includes, but is not limited to, the following elements:

3.1 **Classification**
Information and data are classified and managed in accordance with the sensitivity levels established for the University.

3.2 **Collection, Use and Disclosure**
The collection, use, and disclosure of information and/or data must relate directly to an individual's role and responsibilities, necessary for the overall effective operation of the University, including the provision of academic programs.

3.3 **Supports and Safeguards**
The University is required to establish and implement appropriate staffing, programs, systems, mechanisms, processes, infrastructure, and training to support and safeguard information and data's confidentiality, integrity, and availability throughout the University as part of effective operations and to provide for business continuity in the event of adverse situations.

3.4 **Review Period**

Policies related to information and data management and security, including this policy, are reviewed at least once every three (3) years.

4.0 AUTHORITIES, ROLES AND RESPONSIBILITIES

4.1 **Board of Governors**

The Board is responsible for the governance of information and data in the University's control and/or custody and requires the President to oversee the implementation and monitoring of relevant policy direction for managing and securing that information and data throughout its lifecycle.

4.2 **President**

The President is responsible for ensuring that the Executive adopts and implements relevant policies, procedures, and/or standards in compliance with the direction provided in this policy.

4.3 **Vice-President, Finance and Operations**

The Vice-President, Finance and Operations is responsible for strategic management and regular reporting to the Executive and the Board on the overall activities related to the management and security of information and data.

5.0 DEFINITIONS

For the purposes of this policy**:**

Data means raw facts and statistics that, on their own, do not have any specific meaning, but may be collected and organized to provide information that has a logical meaning.

Form means the manner in which the information and/or data is created, e.g., written, audio, visual.

Information means:

a) **Business information** – information, including confidential information, which is generated or collected for the operations of the University including, but not limited to: financial information, human resource information, technical plans, forecasts, reports, legal opinions, and budgets;

b) **Personal information** - information, including an identifying number or symbol assigned to an individual, collected and/or recorded in any format about an identifiable individual, other than contact information (e.g., name, title, business phone/email), that is within the control or custody of the University, and includes all information that the University collects and uses about identifiable members of its employees, students, and other individuals.

Management means the people, programs, mechanisms, processes, technologies, and systems within the University for the purposes of collection, use, storage, dissemination, retention, and disposal of personal and business information.

Members of the University Community means members of the Board of Governors, employees, students, contractors, volunteers, guests, visitors and others who access and/or participate in University academic, administrative, and research activities and operations undertaken on behalf of the University on or off-campus.

Security means guarding the safety of information and data against misuse, theft, inadvertent release, or other threats and protecting confidentiality and privacy while maintaining the integrity of that information and data.

Storage medium means the manner in which information and data are retained and managed including paper, hard-drive, Cloud, flash drive, electronic system, recording, or other media.

6.0 INTERPRETATION

Questions of interpretation or application of this policy or its procedures are referred to the Vice President, Finance and Operations for resolution.

7.0 RELATED DOCUMENTS

Royal Roads University Documents and Information

- Information Technology System Security (policy #1098)
- IT Resources' Access and Acceptable Use (policy #1063)
- Network Access (standard #1098-S)
- Privacy and Protection of Personal Information (policy #1090)
- Records Management (policy #1029)

Legislation and Other Information

- *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, (CASL), SC 2010, c 23
- BC Core Policy & Procedures Manual, Chapter 12: Information Management and Information Technology Management
- Center for Internet Security Controls (2023), v.8
- *Freedom of Information and Protection of Privacy Act*, RSBC 1966, c.165 (FIPPA) and applicable regulations
- ISO 270001:2022 – Security Control Framework and Annex A

Review, Revision and Approval History

Date	Activity
2024-Jun-20	Approved by the Board; first implementation and effective date
2025-Jun-20	Next Review (post-implementation)