

Title	Privacy and Protection of Information		
Classification	Administrative	Oversight Responsibility	Office of Vice-President, Finance and Operations
Category	Governance and Legal	Responsible Office	Operations and Resilience
Approval	Board of Governors	Effective Date	31-March-2023
		Document No.	1090

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've printed this policy, check the website to ensure you have the current version.

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

1.0 POLICY STATEMENT

Royal Roads University (“University”) protects the privacy and confidentiality of **Personal Information** of the **University Community**, clients, and visitors to University campuses through robust practices with respect to the collection, use, disclosure, retention, safeguard of, and access to, Personal Information.

This policy and related documents set out principles and practices that ensure the privacy and confidentiality of the Personal Information in the custody and/or control of the University in compliance with the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 (“FOIPPA”) and other applicable Personal Information protection laws.

2.0 SCOPE AND COMPLIANCE

This policy applies to the University's operations and activities and recognizes the privacy interests of the University Community, clients, and visitors to University campuses. Members of the University Community are expected to be familiar and comply with this Policy. Personnel found to have engaged in improper activity related to the privacy and confidentiality of Personal Information may be subject to discipline, up to and including termination of employment, appointment, contract, or other relationship with the University.

3.0 POLICY TERMS

- 3.1 For the purposes of administering FOIPPA, the President is designated as the head of the public body.
- 3.2 Privacy Management Program (“Program”)

The University will develop and implement a Program that meets the requirements described in the Privacy Management Program Directions issued by the minister responsible for FOIPPA (“the Directions”), including:

 - a. a privacy contact, or contacts, designated by the University President, who shall be responsible for performing the privacy contact duties as described in the Directions;

- b. a process for completing and documenting Privacy Impact Assessments and information sharing agreements;
- c. a process for responding to privacy breaches and complaints, in compliance with the requirements detailed in FOIPPA;
- d. development, implementation, and monitoring of the privacy education and awareness programs of the University;
- e. making this Policy and the University's privacy practices available to the University Community and, where practical, the general public;
- f. ensuring that service providers who are handling Personal Information related to the provision of their services to the University are aware of their privacy obligations; and
- g. a regular review of the Program to ensure its effectiveness and currency and to address any gaps in the delivery of the Program.

3.3 Collection

- a. The University collects Personal Information for purposes that relate directly to, and are necessary for, the provision of the University's programs and operations, and for other purposes authorized or required by FOIPPA and other applicable laws.
- b. The University endeavours to collect Personal Information directly from the relevant individual unless another method of collection is authorized under FOIPPA or required by law.
- c. Royal Roads University Websites
University websites will include a privacy notice that explains how the site collects personal data, the type of data collected, the purpose for collecting the data, if and how the data is disclosed, and contact details for the Privacy Office. A website that uses **Cookies** will alert users and inform them why cookies are used and how to opt out.

3.4 Use

- a. The University and Personnel will maintain the confidentiality of all Personal Information and shall exercise the level of care and diligence in the protection of such information that is appropriate to the nature and sensitivity of the information.
- b. Personal Information may be accessed and used only by authorized Personnel, and access and use will be limited by the following principles:
 - i. exercising access and use to what is necessary to allow members of Personnel to fulfill their duties and responsibilities;
 - ii. limiting the internal sharing of information among Personnel on a need-to-know basis; and
 - iii. where applicable, ensuring that access to and use of Personal Information is consistent with the terms of any notices or consents given to or by affected individuals.
- c. Canada's Anti-Spam Legislation (CASL)
University programs that collect Personal Information as part of marketing, recruiting, advancement, or similar activities shall adhere to the requirements of CASL, including, but not limited to, the collection of Personal Information, consent, and the retention of Personal Information.

3.5 Disclosure

- a. Personal Information may be disclosed for the purposes for which it was originally collected, with consent from the affected individual, and in other circumstances authorized or required under FOIPPA or other applicable laws.

- b. The University does not disclose Personal Information to third parties, such as service providers, located outside of Canada, except to the extent permitted by FOIPPA and in compliance with all required risk assessments.

3.6 Safeguards and Training

- a. The University applies appropriate physical, administrative, and technical **Safeguards** to ensure that the Personal Information in its custody and/or control is secure.
- b. Through its Program, the University provides training to employees and contractors to maintain the privacy and security of Personal Information and prevent its unauthorized collection, access, use, and disclosure.
- c. Personnel are expected to exercise reasonable diligence and take appropriate care in protecting Personal Information against such risks as unauthorized collection, use, destruction, retention or alteration, or the loss or theft of such information.

3.7 Access

- a. The University recognizes that individuals have a right to access their own Personal Information in the control of the University, and the University complies with the processes for receiving and responding to such requests in compliance with FOIPPA.

3.8 Retention

- a. The University utilizes a records retention strategy, with related retention schedules, that seeks to ensure records and Personal Information that are no longer required for any business, administrative, operational, or legal reason are securely destroyed when they are no longer needed.
- b. The University endeavours to comply with all legally required retention periods, including by ensuring that Personal Information that is used to make a decision that affects an individual is retained for at least one year to ensure that the affected individual has an opportunity to seek access to that information.

3.9 Reporting Requirements

- a. Personnel are required to immediately report actual or suspected breaches of Personal Information privacy to the Privacy Office.
- b. The Privacy Office reports contraventions, actual or possible, of this Policy or FOIPPA and real or suspected privacy breaches to the Vice-President, Finance and Operations (VPFO), and other persons as determined necessary.
- c. On direction of the VPFO, the Privacy Office notifies the Office of the Information and Privacy Commissioner (“OIPC”) of privacy breaches in accordance with the requirements of FOIPPA.
- d. The University complies with all requirements under FOIPPA to provide notices to affected individuals of privacy breach incidents giving rise to a risk of significant harm.

3.10 Access to Information/Complaint Process

- a. Questions, concerns, or complaints about the University’s privacy management practices and Program should be directed to the Privacy Office. The University will receive and respond to all complaints made under this Policy.
- b. Privacy Contact
Privacy and/or access to information requests, inquiries or questions, will be made in writing or by email and directed to:

Privacy Office
Royal Roads University
2005 Sooke Rd

- 3.11 Review period
The University will monitor government legislation and revise this Policy as required. In any event, this Policy will be reviewed once every three years.

4.0 AUTHORITIES, ROLES, AND RESPONSIBILITIES

Board members, employees, contractors and volunteers are required to agree to confidentiality provisions as part of their employment, contractual agreement, or service to the University.

- 4.1 Board of Governors
The Board is responsible for the oversight and governance of privacy compliance for the University. The Board delegates relevant management responsibility to the President.
- 4.2 Executive
The President is the designated head of the University for the purposes of FOIPPA and may delegate to any person any duty, power, or function of the head, except the power to delegate.
- 4.3 Academic and administrative managers are responsible for ensuring Personnel accessing Personal Information conform to the requirements of the University's Program.

5.0 DEFINITIONS

For the purposes of this Policy:

Cookies means a small text file created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk that provides a way for the website to recognize the user and keep track of her or his searching preferences.

Personal Information means "recorded information about an identifiable individual other than contact information 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 staff, students, and other individuals.

Safeguards means measures to limit access to and protect information and includes but is not limited to: storing information in secure facilities, locked filing cabinets, limited user access, use of passphrases and passwords, firewalls, and encryption software.

University Community includes Board members, employees, students, contractors, volunteers, alumni, and applicants.

6.0 INTERPRETATION

Questions of interpretation or application of this Policy or its procedures will be referred to the Vice-President, Finance and Operations, whose decision is final.

7.0 RELATED DOCUMENTS

Royal Roads University Documents and Information

- [Confidentiality](#)
- [Network Access and Email Use](#)
- [Personal Information of Applicants and Students](#)
- [Records Management](#)

- [Standards of Conduct and Service for Employees and Contractors](#)
- [Student Rights Responsibilities](#)
- Video Surveillance and Managing Video Surveillance Procedure

Legislation and Information

- *Canada's Anti-Spam Legislation (CASL)*
- *Freedom of Information and Protection of Privacy Act (FOIPPA)*, RSBC 1996, c.165 and applicable Regulations

Review and Revision History

Reviewed by Finance and Audit Committee	16 March 2023
Approved by Board of Governors	31 March 2023
Next review (one-year post implementation)	31 March 2024

This Privacy and Protection of Information Policy replaces the following policies:

- Freedom of Information and Privacy (2005)
- Privacy (2015)