

Title	Video Surveillance		
Classification	Administrative	Oversight Responsibility	Office of Vice-President, Finance and Operations
Category	Governance & Legal	Responsible Office	Operations and Resilience
Approval	Executive	Effective Date	2023-Nov-01
		Document No.	1094

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, 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

This policy and related documents outline the responsible use of **video surveillance systems** ("surveillance systems") on Royal Roads University ("University") campuses. The University recognizes that the use of surveillance systems impacts the privacy of employees, contractors, students, volunteers, clients, and visitors, and this policy explains the ways in which it seeks to balance privacy interests with the important safety and other benefits arising from the reasonable use of surveillance systems.

The use of these surveillance systems is compliant with the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FOIPPA") and other laws applicable to the privacy of personal information.

2.0 SCOPE AND COMPLIANCE

- 2.1 This policy applies to **University campuses** and to **Personnel** with responsibility or access to the surveillance systems.
- 2.2 The terms of this policy are monitored for compliance. Issues related to compliance are managed in accordance with applicable law and the University's policies, collective agreements, and contracts.

3.0 POLICY TERMS

- 3.1 The University uses surveillance systems for the purposes of maintaining and enhancing safety and security of persons, assets, property, and infrastructure, including preventing and deterring crime, identifying suspects, and gathering evidence.
- 3.2 surveillance systems are not used to monitor work performance or productivity of employees or contractors. However, the University may refer to footage, or inspect or rely upon it, if it is relevant to a workplace incident or investigation.
- 3.3 surveillance systems are not used to monitor academic conduct or performance, such as exam invigilation. However, the University may refer to footage, or inspect or rely upon it, if it is relevant to an incident or investigation.

- 3.4 The University collects, uses, stores, and discloses surveillance and recording data in compliance with the University's *Privacy and Protection of Information Policy*, FOIPPA, and other applicable laws.
- 3.5 Only authorized Personnel, licensed security contractors, and licensed video service providers shall be granted access to the surveillance systems' controls, equipment, and records. Such access is to be exercised only when it is necessary in the performance of authorized duties.
- 3.6 Recorded information is stored on encrypted devices and destroyed after 30 days, except for records awaiting review by **law enforcement** agencies, information seized as evidence, or information that has been duplicated for use by law enforcement agencies, which shall be destroyed after one year. The University does not retain video footage when there is no legal, business, or operational purpose for keeping it.
- 3.7 Notice of surveillance systems is posted at the perimeter of surveillance areas and includes notice of the purposes for the surveillance, the legal authority for collecting it, and the contact information of a University representative who can answer questions about the surveillance systems.
- 3.8 All cameras are installed where they are visible to Personnel, clients, and visitors and are positioned in hallways, entrances and exits, and parking lots. Cameras are not installed in or near areas where there is a general expectation of privacy, such as washrooms or change rooms.
- 3.9 surveillance systems do not include the use of hidden cameras or any surreptitious collection of **personal information**.
- 3.10 The University will consider other available, less intrusive methods of monitoring before implementing new surveillance systems.
- 3.11 Requests for access to video footage may be made following the University's *Managing Video Surveillance Procedure*, and access will be provided as authorized or required under FOIPPA.
- 3.12 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

- 4.1 The Vice-President, Finance and Operations:
 - a. delegates the administration of this policy and relevant standards, procedures, and directions to the Responsible Office to manage surveillance systems on University campuses; and
 - b. informs Executive of any significant issue or matter regarding surveillance systems on University campuses.
- 4.2 The Responsible Office:
 - a. administers and manages this policy and relevant standards, procedures, and directions; and
 - b. identifies, applies, and maintains internal controls that support consistent and appropriate use of surveillance systems and effective privacy compliance.

5.0 DEFINITIONS

For the purposes of this policy:

Law enforcement, per the Public Sector Surveillance Guidelines produced by the OIPCBC, means "policing, including criminal intelligence systems; investigations that lead or could lead to a penalty or sanction being imposed; or proceedings that lead, or could lead, to a penalty or sanction being imposed."

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.

Personnel means Board members, employees, and contractors with responsibility or access to the University’s surveillance systems.

Video surveillance systems refers to a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of specific locations on University property and the actions of individuals in those locations.

University campuses means all University facilities, buildings, and grounds.

6.0 INTERPRETATION

Questions of interpretation or application of this policy are referred to the Vice-President, Finance and Operations.

7.0 RELATED DOCUMENTS

Royal Roads University Documents and Information

- Privacy and Protection of Information
- [Records Management](#)
- [Standards of Conduct & Service for Employees & Contractors](#)
- [Student Rights & Responsibilities](#)
- Video Surveillance Management Procedure

Legislation and Information

- *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c.165 and applicable Regulations

Review, Revision and Approval History

<u>Date</u>	<u>Action</u>
2023-Feb-28	Initial approval by Executive
2023-Nov-01	Effective date
2025-Jul-10	Administrative revisions; 2025-Nov-10 effective date remains
<hr/>	
2026-Jul-10	Next Review