Procedure

Title	Video Surveillance Management		
Parent Policy	Video Surveillance	**Responsible Office**	Operations and Resilience
Classification	Administrative	**Effective Date**	2025-Jul-10
Category	Governance & Legal	**Document No.**	1094-PR
Approval	Vice-President, Finance and Operations		

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

The most up-to-date versions of the university's procedures are posted on the policy and procedure website. If you have printed this procedure, 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.

This procedure do not apply to surveillance used for **law enforcement** as an investigative tool where such activity is authorized by law enforcement authorities, legislation, or court order.

1.0 Video surveillance equipment installation and maintenance

1.1 Installation

a) The Responsible Office, in consultation with the Vice-President, Finance and Operations, approves the installation, use, disabling, and disconnection of **video surveillance systems** ("surveillance systems") on Royal Roads University ("University") **campuses**.

b) The Privacy Office conducts a Privacy Impact Assessment ("PIA") and Security/Threat Risk Assessments on surveillance systems. These assessments are completed before the contract for surveillance systems is signed and before the surveillance systems are activated.

c) The Responsible Office, in consultation with Information Technology Services (ITS), supervises the installation of surveillance systems.

d) The University maintains an inventory of surveillance systems and equipment in operation, which indicates the date of installation, reason for installation, and location.

1.2 Placement of surveillance systems

a) Decisions regarding the placement of surveillance systems reside with the Responsible Office.

b) Surveillance systems may monitor exterior and interior areas of University property where individuals have no reasonable expectation of privacy. surveillance systems will not normally be installed in work and teaching spaces, offices, meeting and conference rooms, social spaces, and areas with a reasonable expectation of privacy such as washrooms and changerooms, except in special circumstances as approved by the Director of Emergency Management and Resilience or designate and limited to the prevention/detection of illegal activity and the enhancement of safety.

c) Surveillance systems will not be positioned towards property or buildings that are not owned or operated by the University.

d) Monitors are placed in a secure location with restricted access, away from public view.

1.3 Requesting installation of surveillance systems

a) To request the installation of surveillance systems, provide a letter in writing to the Responsible Office.

b) The Responsible Office will consult with relevant parties to prepare a recommendation regarding the request to install a Security Camera System.

c) The recommendation will be forwarded to the AVP, Operations and Resilience, for approval.

d) Upon approval of the recommendation by the AVP, Operations and Resilience, the recommendation will be forwarded to the University Privacy Office to update the surveillance systems PIA. The updated PIA will be shared with the AVP, Operations and Resilience.

e) If new surveillance systems will be installed, notice will be provided and communicated in writing to anyone directly affected by the installation of surveillance systems.

1.4 Maintenance

Campus Security coordinates operational verification of surveillance systems at least once per month. Malfunctions or concerns are reported to the Director of Emergency Management and Resilience.

2.0 Notice of video surveillance

Signage is posted on the perimeter of areas being monitored by surveillance systems and is visible prior to an individual entering the field of recording. Signage includes the following information:

- Notice that the area is being monitored and recorded by Campus Security;
- Acknowledgement of recorded information being collected in accordance with the *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165 ("FOIPPA"); and
- Contact information for Campus Security.

Sample signage copy:

This area is being MONITORED and RECORDED by Campus Security.

Attention: To enhance security, this area is under 24-hour video surveillance. Information is collected under the Freedom of Information and Protection of Privacy Act*. For more information, contact Campus Security at 250-391-2525.*

3.0 Training and requirements

3.1 The Director of Emergency Management and Resilience or delegate ensures that authorized individuals accessing surveillance systems and equipment, and the records they create, are trained to comply with this procedure and related policies, including the *Privacy and Protection of Information Policy*, and legislation. Misuse of Video Surveillance equipment or records will result in disciplinary action, following the *Standards of Conduct and Service for Employees and Contractors Policy*.

3.2 The Director of Emergency Management and Resilience or delegate maintains a list of authorized individuals per s. 3.1. This list is reviewed on a regular basis to ensure accuracy and relevance.

3.3 Licensed contractors will be authorized by the Director of Emergency Management and Resilience or delegate to access records created by surveillance systems for installation and

maintenance purposes only. Contractors must have a signed non-disclosure agreement in place with the University prior to accessing the surveillance systems. Failure of a video service provider to comply with this procedure, related policies, and legislation will constitute breach of contract and may result in termination of contract and legal action.

4.0 Monitoring

4.1 Only authorized employees and contractors may observe and monitor live footage from surveillance systems and only in the performance of authorized duties.

4.2 Only the following persons are authorized to observe and monitor live footage surveillance systems:

- Members of the University's Campus Security team;
- Director of ITS or delegate; and
- Director of Emergency Management and Resilience or delegate.

5.0 Records storage and access

5.1 Storage

a) The records created by surveillance systems are stored in accordance with the University's Records Management Procedure and *Privacy and Protection of Information Policy*. They are kept in a restricted-access area within Campus Security.

b) Only the following persons are authorized to access the restricted area where the records of surveillance systems are stored:

- Members of the University's Campus Security team;
- Chief Information Officer or delegate;
- Director of Emergency Management and Resilience or delegate; and
- Persons authorized by the Director of Emergency Management and Resilience or delegate, e.g., licensed video service providers.

5.2 Log

Per FOIPPA, all instances of access to, and use of, recorded material produced by surveillance systems are tracked in a log. The log is maintained by Campus Security.

5.3 Removing records

Records produced by surveillance systems may only be removed from the restricted-access area upon the written authorization of the Director of Emergency Management and Resilience or delegate.

5.4 Access to records

a) Requests to access **personal information** recorded by surveillance systems must follow processes outlined in the University's *Privacy and Protection of Information Policy*. Disclosures will be made in accordance with applicable legislation, namely FOIPPA.

b) Where a record created by surveillance systems is requested as part of an investigation of an incident or alleged misconduct (see s.6.1), it will only be disclosed when approved by the Privacy Office and the Director of Emergency Management and Resilience or delegate. If a request to access a record created by surveillance systems creates a real or apparent conflict of interest for the Director of Emergency Management and Resilience, or any person overseeing the Director of Emergency Management and Resilience, the President will appoint a delegate for the purposes of this request.

c) The University may place restrictions on the use of the record created by surveillance systems that is disclosed through the request to access personal information (s.5.4a), as deemed appropriate.

d) If a record created by surveillance systems captures third parties, the faces of third parties will be blurred upon disclosure, in accordance with FOIPPA.

e) If a record created by surveillance systems has been requested as part of a freedom of information request through the Office of the Information and Privacy Commissioner for British Columbia ("OIPCBC"), Campus Security, with direction from the Director of Emergency Management and Resilience, will release the record to the OIPCBC only after receiving written approval from the Vice-President, Finance and Operations.

6.0 Incidents, investigations and reporting

6.1 Incidents and investigations

Records created by surveillance systems may be used to support an investigation, internal or led by law enforcement, and subsequent proceedings of incidents and alleged misconduct.

6.2 Reporting

Records created by surveillance systems that contain evidence of an incident are retained and added to the related Campus Security incident report as an attachment.

Where alleged misconduct is observed in the regular monitoring of live footage recorded by surveillance systems, the Director of Emergency Management and Resilience will notify the appropriate portfolio/department/school of the incident and the existence of the footage.

7.0 Retention and destruction of records

Records created by surveillance systems will be retained and destroyed following relevant University policies and legislation, including records that have been reviewed for law enforcement purposes or are included in a Campus Security incident report.

8.0 Annual Review

This procedure will be reviewed annually.

9.0 Definitions

For the purposes of this procedure**:**

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.

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.

10.0 Related documents and information

- Privacy and Protection of Information Policy
- IT Services Acceptable Use Policy
- Records Management Policy
- Records Management Operation Procedure
- Standards of Conduct and Service for Employees and Contractors Policy
- Video Surveillance Policy

Legislation and Information

- British Columbia Freedom of Information and Protection of Privacy Act (FOIPPA)

Review, Revision and Approval History

Date	Action
2023-Feb-28	Initial approval by Executive
2023-Nov-01	Effective date
2025-Jul-10	Approved by VP, Finance and Operations; key revision was reword of video surveillance assessment committee to consultation with relevant parties; new effective date
2025-Jul-10	Next Review