Royal Roads University

Privacy Impact Assessment

Video Surveillance System

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number: 2025-04

Initiative title:	Video Surveillance System
Organization:	Royal Roads University
Branch or unit:	John Horgan Campus
Your name and title:	Don Devenney Senior IT Security & Risk Specialist, Royal Roads University
Your work phone:	250-391-4975
Your email:	don.devenney@royalroads.ca
Initiative Lead name and title:	Jason Humphries

	Director, Emergency Management & Resilience Operations & Resilience
Initiative Lead phone:	250-514-1386
Initiative Lead email:	Jason.2Humphries@royalroads.ca
Privacy Officer:	
Privacy Officer phone:	
Privacy Officer email:	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Related PIAs, if any:
Royal Roads University Video Surveillance System PIA #2022-01

1. What is the initiative?

The John Horgan Campus of Royal Roads University (the University) intends to use Video Surveillance Systems on University campuses. The University recognizes that the use of Surveillance Systems impacts the privacy of employees, contractors, students, volunteers, clients, and visitors, and will balance the privacy interests of individuals with the important safety and other benefits arising from the reasonable use of Surveillance Systems.

The University will use 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. Though not an intended purpose, the recordings may also be used in the event of a personal injury claim. The Surveillance Systems will not be 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. Surveillance Systems will not be 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.

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. 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.

Recorded information stored on encrypted devices will be 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 will not retain video footage when there is no legal, business, or operational purpose for keeping it.

Notice of Surveillance Systems will be posted at the perimeter of surveillance areas and will include 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.

All cameras will be installed where they are visible to employees, contractors, students, volunteers, clients, and visitors and will be positioned in hallways, entrances and exits, open areas, and parking lots. Cameras will not be installed in or near areas where there is a general expectation of privacy, such as washrooms or change rooms.

Surveillance Systems will not include the use of hidden cameras or any surreptitious collection of personal information.

The University considered and tried other available, less intrusive methods of monitoring before implementing new Surveillance Systems, such as increased patrols, installing security keys in sensitive areas, and signage indicating authorized personnel only. These methods were not successful in preventing numerous incidents.

The University will use the AXIS P3737-PLE and equivalent Camera. Specifications can be found in Appendix A of this PIA.

14 single lens (4MP, 3-6 mm) and 4 Multi-sensor cameras will be installed throughout the Campus. Further information regarding the locations of the cameras can be found in Appendix B of this PIA.

Requests for access to video footage must be made following the University's *Managing Video Surveillance Procedure*, and access will only be provided as authorized or required under FOIPPA.

The University has a *Video Surveillance Policy* and *Managing Video Surveillance Procedure* in place.

2. What is the scope of the PIA?

This PIA addresses the collection, use, disclosure, storage, and security of personal information collected and recorded by a Video Surveillance system at Royal Roads University.

3. What are the data or information elements involved in your initiative?

The personal information is the live and recorded Surveillance System camera feed of individuals on the University campus.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

4. How will you reduce the risk of unintentionally collecting personal information?

Not applicable.

PART 2: COLLECTION, USE AND DISCLOSURE

5. Collection, use and disclosure

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1: Image of incident is captured	Collection	S. 26 (c)	
Step 2: Image is reviewed to investigate and address specific safety or security incidents. If a security, personal health or safety, or another event has been recorded, the image is saved on the University's secure network. 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.	Use	S. 32(a) and 32(b)	
Step 3: Viewing and preparing recordings in the event of an access/FOI request, e.g., removing third-party personal information.	Use Disclosure	S. 32(a) S. 33(1)	
Step 4: Image is disclosed to third party (e.g., law enforcement) and retained for a minimum of one year.	Use Disclosure	S. 32(c) S. 33(2)(d) S. 33(3)(d) S. 33[2][l]	

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Signage will be posted on the perimeter of areas being monitored by Video Surveillance and will be visible prior to an individual entering the field of recording. The signage will include the following content:

> *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.*

PART 3: STORING PERSONAL INFORMATION

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

Yes, recordings could potentially involve sensitive personal information.

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

10. Where are you storing the personal information involved in your initiative?

Not applicable.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider?

Not applicable.

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

Not applicable.

13. Does the contract you rely on include privacy-related terms?

Not applicable.

15. What controls are in place to prevent unauthorized access to sensitive personal information?

Not applicable.

16. Provide details about how you will track access to sensitive personal information.

Not applicable.

17. Describe the privacy risks for disclosure outside of Canada.

Not applicable.

PART 5: SECURITY OF PERSONAL INFORMATION

18. Does your initiative involve digital tools, databases, or information systems?

Yes.

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

No.

19. What technical and physical security do you have in place to protect personal information?

The records created by Surveillance Systems are stored in accordance with the University's *Records Management Procedure* and *Privacy and Protection of Information Policy*.

Security recordings will be stored on the University server only. The server is located Section 15(1)( ) . The data centre

Section 15(1)(l)

20. Controlling and tracking access

Strategy	
RRU only allows employees in certain roles access to information.	Yes. Only the following persons are authorized to access the restricted area where the recordings of Video Surveillance system are stored: • Members of the University's Campus Security team; • Director of ITS or designate; • Director of Emergency Management or designate; and • Persons authorized by the Director of Emergency Management or designate, e.g., licensed video service providers.
Employees who need standing or recurring access to personal information must be approved by executive lead.	Yes
RRU uses audit logs to see who accesses a file and when.	Yes. All instances of access to, and use of, recorded material produced by Surveillance System will be tracked in a log, to be developed. The log will be maintained by Campus Security.
Describe any additional controls:	Records produced by the Surveillance System may only be removed from the restricted-access area upon the written authorization of the Director of Operations or designate. Requests to access personal information recorded by the Surveillance System must follow the processes outlined in the University's *Privacy and Protection of Information Policy*. Disclosures will be made in accordance with FOIPPA. Where a record created by the Surveillance System is requested as part of an

Strategy	
	investigation of an incident or alleged misconduct, it will only be disclosed when approved by the Privacy Officer and the Director of Operations or designate. If a request to access a record created by the Surveillance System creates a real or apparent conflict of interest for the Director of Operations, or any person overseeing the Director of Operations, the President will appoint a designate for the purposes of the request. The University may place restrictions on the use of a record created by the Surveillance System that is disclosed through the request to access personal information as deemed appropriate. If a record created by the Surveillance System captures third parties, the faces of third parties will be blurred upon disclosure, in accordance with FOIPPA. If a record created by the Surveillance system has been requested as part of a freedom of information request through the Office of the Information and Privacy Commissioner of BC (OIPC), Campus Security, with direction from the Director of Operations, will release the record to the OIPC only after receiving written approval from the Vice-President, Finance and Operations.

PART 6: ACCURACY, CORRECTION AND RETENTION

21. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

Personal information will be recorded live by cameras and is therefore accurate and complete at time of recording.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

No. It is not possible to correct the personal information as it is recorded live by CCTV.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Not applicable.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

Not applicable.

23. Does your initiative use personal information to make decisions that directly affect an individual?

Yes.

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

Yes. Royal Roads has a detailed records and retention schedule that may be viewed HERE. A review of the appropriate section in this schedule confirms that personal information used to make a decision directly affecting an individual is retained for a minimum of one year.

PART 7: AGREEMENTS AND INFORMATION BANKS

1. Does your initiative involve an information sharing agreement?

No.

25. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

No.

PART 8: ADDITIONAL RISKS

26. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Possible risk	Response
Risk 1: Unauthorized individuals at the University view the live feed or access the recordings.	Only authorized personnel, licensed security contractors, and licensed video service providers will be granted access to the Surveillance Systems' controls, equipment, and records. Such access will be exercised only when it is necessary in the performance of authorized duties. The University has policies, procedures, and protocols in place to ensure the security of personal information, e.g., Managing Video Surveillance, Video Surveillance Policy.

Possible risk	Response
Risk 2: Service providers/contractors view the live feed or access the recordings without authorization.	Licensed contractors will be authorized by the Director of Emergency Management or designate to access records created by the Surveillance System for installation and maintenance purposes only. Contractors must have a signed non-disclosure agreement in place prior to accessing the Surveillance Systems. Failure of a video service provider to comply with the procedure, related policies, and legislation will constitute a breach of contact and may result in termination of the contract and legal action.
Risk 2: Personal information is released without consent to a third party.	Campus Security must receive written approval from the Vice-President, Finance and Operations or designate, before releasing recordings. Recordings will be viewed and faces of third parties in the video will be blurred before the recordings are released.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

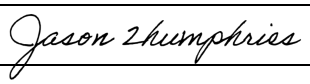
This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative			

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored, or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead	Jason Humphries		Jan, 21, 2026
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA	n/a	n/a	n/a
Head of public body, or designate Only required if personal information is involved	Alex Kortum Vice President, Finance and Operations		

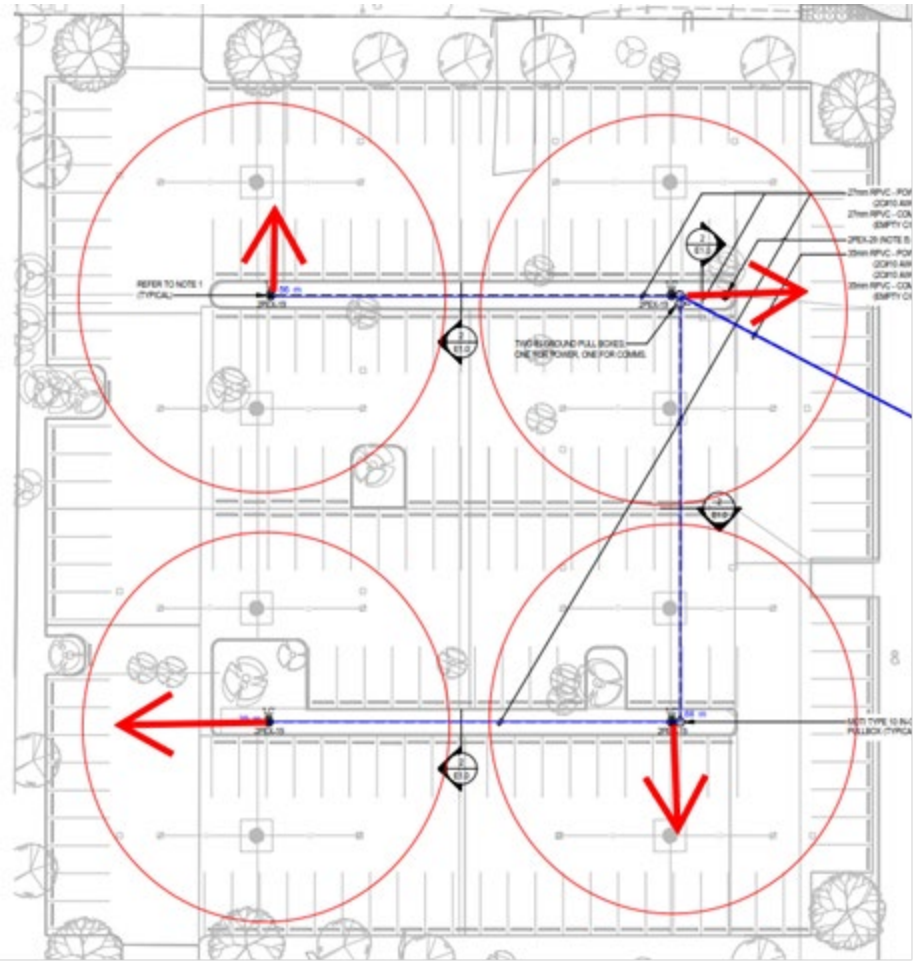
Appendix A

Security camera schedule for the building and “ambulance/Service Park”.

RRU WSC SECURITY CAMERA SCHEDULE							
#	AREA	TAG	PIXELS	LENS	MTD HEIGHT	MOUNT	CABLING
1	BASEMENT	C-B-01	ROUGH-IN ONLY				-
2	BASEMENT	C-B-02	ROUGH-IN ONLY				-
3	BASEMENT	C-B-03	ROUGH-IN ONLY				-
4	EXTERIOR	C-1-01	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
5	EXTERIOR	C-1-02	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
6	EXTERIOR	C-1-03	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
7	EXTERIOR	C-1-04	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
8	EXTERIOR	C-1-05	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
9	EXTERIOR	C-1-06	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
10	EXTERIOR	C-1-07	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
11	EXTERIOR	C-1-08	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
12	EXTERIOR	C-1-09	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
13	EXTERIOR	C-1-10	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
14	EXTERIOR	C-1-11	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
15	VESTIBULE 100	C-1-12	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
16	LOBBY 101	C-1-13	ROUGH-IN ONLY				-
17	CAFE 105	C-1-14	ROUGH-IN ONLY				-
18	CORRIDOR 102	C-1-15	ROUGH-IN ONLY				-
19	IT/SERVER 112	C-1-16	ROUGH-IN ONLY				-
20	VESTIBULE 123	C-1-17	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A
21	AMBULANCE PARK	C-1-18	4MP	3-6mm	2.4-3.0m	CEILING/WALL	CAT6A/FIBER
22	CORRIDOR 202	C-2-01	ROUGH-IN ONLY				-
23	IT/SERVER 208	C-2-02	ROUGH-IN ONLY				-
24	LOBBY 200	C-2-03	ROUGH-IN ONLY				-
25	CORRIDOR 201	C-2-04	ROUGH-IN ONLY				-
26	CORRIDOR 301	C-3-01	ROUGH-IN ONLY				-
27	IT/SERVER 311	C-3-02	ROUGH-IN ONLY				-
28	LEARNING COMMONS 302	C-3-03	ROUGH-IN ONLY				-
29	LOBBY 300	C-3-04	ROUGH-IN ONLY				-
30	LEARNING COMMONS EAST	C-3-05	ROUGH-IN ONLY				-
31	CORRIDOR EAST	C-3-06	ROUGH-IN ONLY				-
32	CORRIDOR 402	C-4-01	ROUGH-IN ONLY				-
33	IT/SERVER 411	C-4-02	ROUGH-IN ONLY				-
34	LOBBY 400	C-4-03	ROUGH-IN ONLY				-
35	CORRIDOR 401	C-4-04	ROUGH-IN ONLY				-
36	NORTH CORRIDOR	C-5-01	ROUGH-IN ONLY				-
37	IT/SERVER 505	C-5-02	ROUGH-IN ONLY				-
38	LOBBY 500	C-5-03	ROUGH-IN ONLY				-
39	OFFICE 502	C-5-04	ROUGH-IN ONLY				-

Appendix B

North Parking Camera Position.



Building Camera locations