Vancouver Island University

CCTV for Invigilated Exams - Not Recorded

Privacy Impact Assessment

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	CCTV for Invigilated Exams – Not Recorded
Organization:	Vancouver Island University
Branch or unit:	
Your name and title:	Jo-Ann Bellamy, Privacy Consultant
Your work phone:	250-208-3431
Your email:	jbellamy@hooperconsulting.ca
Initiative Lead name and title:	Bryan Tinlin, Director, Student Affairs

Initiative Lead phone:	
Initiative Lead email:	
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:
None

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

Vancouver Island University (VIU) invigilates exams for students, prospective students and external third parties. VIU's exam centre is located on VIU premises in [redacted] (group exam room with 14 computers and 4 tables) and [redacted] (private exam rooms). Students may write VIU exams (including with approved accommodations), pre-program assessments, or exams for other institutions. Exams are paper or computer based.

s. 15(1)(l)

VIU is assessing the addition of closed-circuit television (CCTV) with audio to 1 group exam and 2 private exam rooms to ensure students writing exams in the exam centre are more thoroughly monitored, both for exam misconduct and for safety. Currently, invigilators in the group exam rooms cannot always sufficiently monitor students as they often are engaged with a student one-to-one at check-in or check-out or if they need to troubleshoot an issue that arises during the exam.

CCTV and audio monitoring is expected to serve as a deterrent to students who may otherwise cheat on exams. It may also increase student safety as some students writing exams in private exam rooms have serious conditions that could require medical attention (e.g., seizure disorders, diabetes, etc.).

Currently 10 invigilators work on temporary contracts and are hired as needed to invigilate exams. Exams run between the hours of 8:00 am and 9:00 pm. It is expected that monitoring by CCTV and audio will allow for fewer invigilators to be required to monitor exams.

The group exam feed would be primarily monitored by the invigilator in the group exam room. This would allow them to view the examinees more closely than their current position at the desk at the front of the room and less obtrusively than frequently walking around the room which can be distracting to students. Depending on the number of exams running in the group exam room, the private exam room feed would also be primarily monitored by the invigilator in the group exam room. An Invigilator, office team member or an AES Assistant may monitor the live feed in the exam room to ensure safety of all in that room.

Students will be notified when their exam is scheduled that CCTVs and audio may be used for invigilation purposes. Students will have the option to make alternative arrangements for writing the exam should they not consent to the CCTV. Notification regarding CCTVs will also be posted outside the exam rooms.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This PIA addresses the collection, use and security of personal information in the live CCTV with audio feed for the invigilation of exams at VIU. The live feed will not be recorded.

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

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

The personal information consists of live CCTV and audio of students writing exams in VIU facilities. The feed will not be recorded.

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.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template**.**

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

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

Only personal information from students writing exams who have been notified and agree to complete the exam with the CCTV live feed being used will be collected. CCTV will be turned off

at any other times. Signage will also be in place outside of the exam room to notify any other individuals who may enter the room while the live feed is operational.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or 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: Viewing and listening to live CCTV feeds of students completing exams for invigilation purposes and to ensure the safety of students. The live feed is not recorded.	Collection Use	S. 26 S. 32(a) and 32(b)	

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).

Notification prior to exam date:

> *Vancouver Island University (VIU) collects personal information under the Freedom of Information and Protection of Privacy Act (FIPPA). VIU may collect your personal information via Closed-Caption Television (CCTV) and audio when you write exams on*

VIU premises. The CCTV and audio feed will not be recorded. The personal information will be used for the purpose of invigilating exams. If you do not consent to the collection of your personal information as stated above, please contact your instructor to make alternate arrangements for writing your exams. For more information regarding the collection and use of your personal information, please contact the Vancouver Island University Privacy Office at: privacy.officer@viu.ca.

Notification outside room:

You are about to enter an area that is monitored by Closed Circuit Television (CCTV) and audio. The CCTV system is in use for invigilation purposes and is not being recorded. By entering the room, you consent to the collection and use of your personal information as stated above. For more information regarding the collection and use of your personal information, please contact the Vancouver Island University Privacy Office at privacy.officer@viu.ca.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

No

8. Does your initiative involve sensitive personal information?

Yes

- If yes, go to question 9
- If no, go to question 10

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

No

- If yes, go to question 10
- If no, go to Part 4

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

After you answer this question go to Part 5.

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

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
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

- If yes, describe the contractual measures related to your initiative.

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.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

Not applicable.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**
Not applicable					

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

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

Yes

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30.

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

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

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

Invigilators will use laptops that are docked at VIU workstations. VIU has privacy protocols in place for using laptops for monitoring exams including strong passwords, closing room windows, and positioning screens away from traffic.

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	Yes
Employees that need standing or recurring access to personal information must be approved by executive lead	Not applicable
We use audit logs to see who accesses a file and when	Not applicable
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

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.

The CCTV and audio are live feed and therefore cannot be altered.

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.

Corrections cannot be made as the CCTV and audio is a live feed and will not be recorded.

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

Not applicable, the CCTV and audio is a live feed and will not be recorded.

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, there may be consequences if a student is found to be cheating on an exam.

- If yes, go to question 25
- If no, skip ahead to Part 7

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.

Not applicable. The camera feed will not be recorded and will not be retained.

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

No

- If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA

26. 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

- If yes, please complete the table below.

Describe the type of information in the bank:
Name of main organization involved:
Any other ministries, agencies, public bodies, or organizations involved:
Business contact title and phone number for person responsible for managing the PIB:

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. 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.

Add new rows if necessary.

Possible risk	Response
Risk 1: Unauthorized individuals view or hear the live CCTV feed.	Access is limited to invigilators and authorized employees at VIU only. Employees sign confidentiality agreements. VIU has privacy policies and protocols in place to ensure the security of personal information.

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	Bev Hooper Hooper Access and Privacy Consulting Ltd.		

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			
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate Only required if personal information is involved			