



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn

Camera Use

PIA#2018-002

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our [PIA Guidelines](#) for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?

Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department/Branch:	JIBC Police Academy		
PIA Drafter:	Nora Houlahan		
Email:	nhoulahan@jibc.ca	Phone:	604-528-5769
Police Academy Director:	Steve Schnitzer		
Email:	sschnitzer@jibc.ca	Phone:	604-528-5756

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

Police Recruit training involves frequent scenarios which are recorded on video for the recruits' exclusive use in their learning. They view the videos, compare them with assessor feedback, and self-assess their performance. The ability to watch themselves on video is a powerful part of their development. Currently, videos are recorded using "Kindles" or recruits' personal devices and the videos are downloaded at the end of the day by the recruits. The Kindles are not very robust and do not hold up well in outdoor use. The video upload process is extremely time consuming and



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

frustrating for the recruits. After more than one year of use, the Kindles are nearing the end of their lifespan and will need to be replaced. Relying on recruits to use their own personal devices is not a reasonable solution as devices with sufficient storage can be costly.

The solution is the Axon body-worn cameras that have been supplied by the manufacturer. These cameras are rugged, can be used in the rain, and the company has provided enough of the cameras to assign one per recruit. The cameras dock in a station and automatically upload to evidence.com, the secure site supported by Axon. The site servers are located in Canada and the site meets all security requirements of police departments. It is currently in use by the [REDACTED]

S.15(1)
(1)

among others. The Axon company has no access to any information uploaded to the site. Because there are enough cameras to assign one per recruit (assigned through the recruits' student numbers), the JIBC Police Academy administrator can set up permissions so that the recruits can only view their own videos. As such, although the information contains identifiable information in the form of recruit images, it will not be accessible to anyone other than the recruit who was the lead investigator in the scenario.

As this information is for training purposes, the videos will be retained on evidence.com until the completion of the block of training in which it occurred. At the end of the block of training, the JIBC Police Academy administrator will bulk delete all videos so that there is no remaining record of personal information.

2. Scope of this PIA

This PIA covers the use of the cameras and the uploading, storage, and retrieval of the associated videos.

3. Related Privacy Impact Assessments

N/A

4. Elements of Information or Data

The recruits will be assigned a camera that will use their JIBC student number to link them to that camera. The videos will contain images of the recruits and recruits may say their names during the scenario.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

The data is stored within Canada and only accessible in Canada.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.

1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

7. Common or Integrated Program or Activity*

<p>In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.</p>	
1. This initiative involves a program or activity that provides a service (or services);	no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

**** Please note: If your initiative involves a “data-linking initiative” or a “common or integrated program or activity”, advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body’s privacy office(r) to determine how to proceed with this notification and consultation.***

For future reference, public bodies are required to notify the OIPC of a “data-linking initiative” or a “common or integrated program or activity” in the early stages of developing the initiative, program or activity. Contact your public body’s privacy office(r) to determine how to proceed with this notification.



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Recruits record and upload their training videos	Collection	26(c)
2.	Recruits view and download their training videos	Disclosure	33.2(a)
3.	Recruit videos are deleted by JIBC Police Academy administrator after completion of that block of training	Use	32(a)

9. Risk Mitigation Table

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	JIBC Police Academy administrator will be able to view recruit videos	Limit the number of staff with administrative access to a very small number (2-3) individuals. See question 12 for the positions that will have access.	Low	Low
2.	Administrative error may assign camera to wrong recruit resulting in one recruit having access to a different recruit's videos.	The camera assignment process will be: camera number assigned to each recruit by administrative staff and recorded in a spreadsheet. When the recruit is assigned the camera they will verify it is the same camera number that is indicated on the spreadsheet and initial that this is the camera they have received.	Low	Low



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

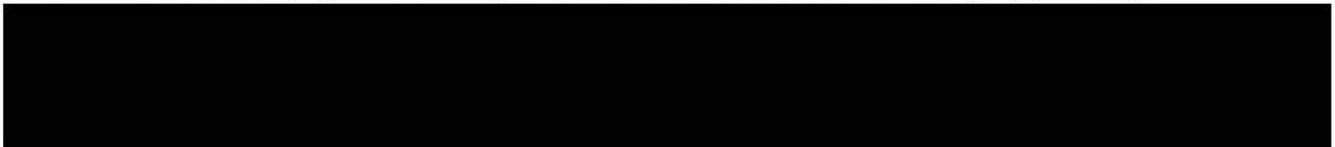
10. Collection Notice

The recruits are verbally told the purpose of recording scenarios for training purpose, the process they will use to upload and retrieve their videos, and the process for deletion of the records at the end of the training block.

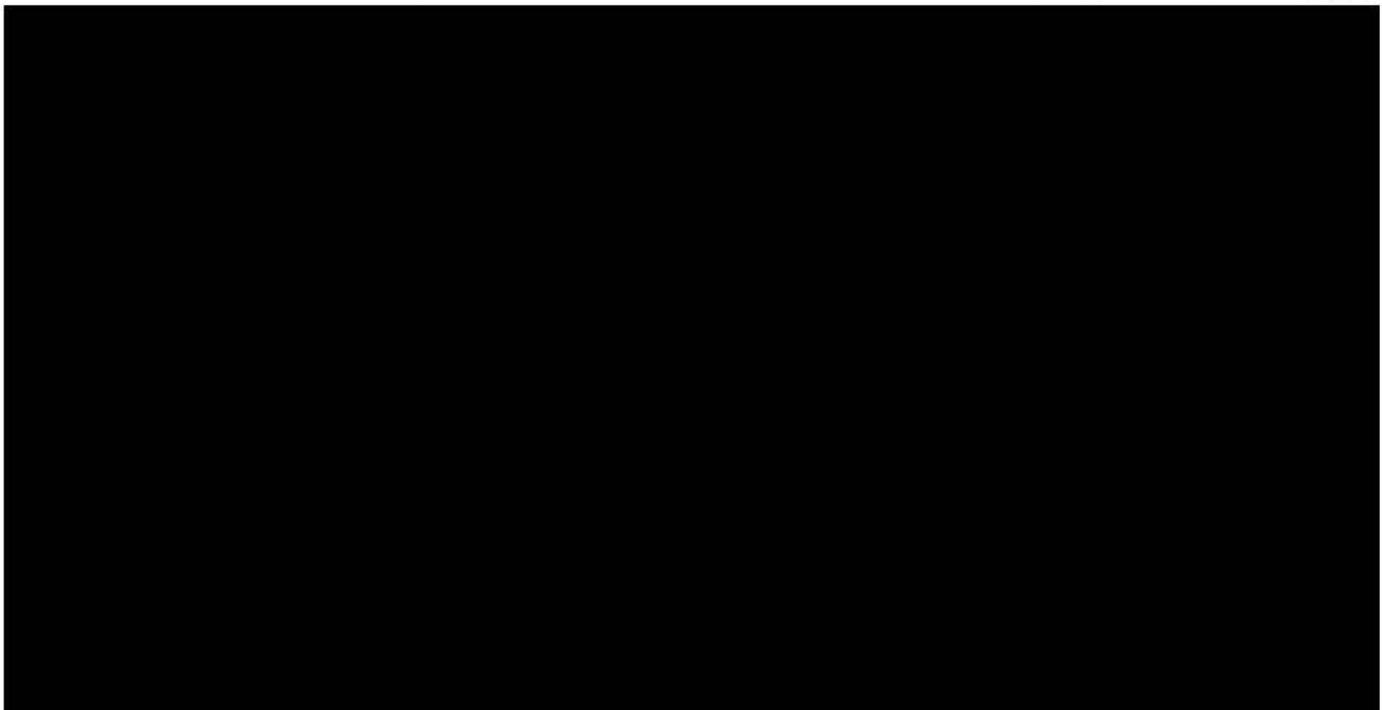
Part 3 - Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

11. Please describe the physical security measures related to the initiative (if applicable).



12. Please describe the technical security measures related to the initiative (if applicable). S.15(1)(l)

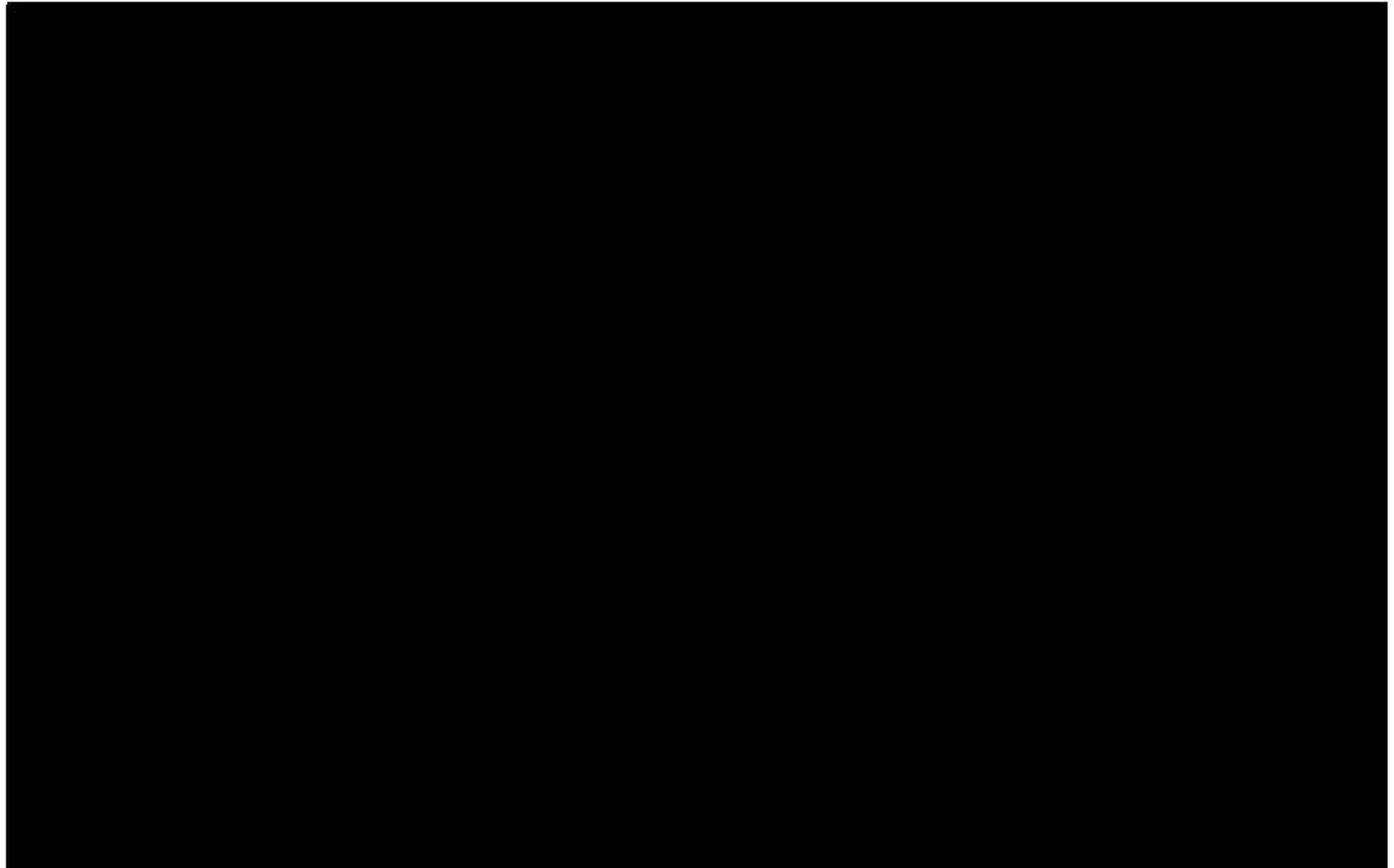




Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002



13. Does your branch/department rely on any security policies?

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Role based access: recruits will only be able to view videos uploaded from the camera assigned to them

15. Please describe how you track who has access to the personal information.

There are robust audit trails of who accesses the videos.

Part 4 – Accuracy/Correction/Retention of Personal Information



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

- 16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?**

There is no need to update information as it is videos for training purposes that will not be disclosed and will be deleted after a short period of time (8-13 weeks upon completion of the block of training in which the videos were filmed).

- 17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.**

No, the videos are used by the recruit for training purposes only and are not the basis of any decisions.

- 18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

N/A

- 19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

N/A.

Part 5 – Further Information

- 20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

No.

<p><i>Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).</i></p>	<input type="checkbox"/>
---	--------------------------



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

No.

Please ensure Parts 6 and 7 are attached to your submitted PIA.



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

Part 6 - Privacy Office(r) Comments

I recommend that this PIA be approved. There are sufficient controls in place, given the potential risks. There are great benefits to this in providing a more effective learning environment for police recruits that justify the use of this new system.

Part 7 - Program Area Signatures

Sue Schitzer

Program/Department Manager

Signature

2018 Feb 28

Date

George Jones

Privacy Officer/Privacy Office Representative

Signature

2018 Feb 28

Date



Privacy Impact Assessment for Non-Ministry Public Bodies

Police Recruit Training Body-worn Camera Use

PIA#2018-002

Contact Responsible for Systems Maintenance and/or Security
(Signature not required unless they have been involved in this PIA.)
N/A

Signature

Date

Kayoko Takemura

Head of Public Body, or designate

[Signature]

Signature

March 1 2018

Date

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

