Privacy Impact Assessment for Non-Ministry Public Bodies

Blackboard Collaborate Online Screen Sharing

PIA#2020 004

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:	Center for Teaching And Learning		
PIA Drafter:	Mike Fabri		
Email:	mfabri@jibc.ca	Phone:	**778.865.6535**
Program Manager:	**Ron Bowles**		
Email:	rbowles@jibc.ca	Phone:	**604.528.5691**

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

1. Description of the Initiative

This PIA is related to Justice Institute of British Columbia's (JIBC) use of BlackBoard Collaborate that supports the delivery of education through a video conferencing software.

The purpose of the initiative is to offer a new tool for connecting faculty and students outside the physical classroom through the use of video conferencing, shared audio and shared computer screens. The goal is to ensure students and faculty can connect with each other synchronously, when in separate geographic locations.

2. Scope of this PIA

This PIA covers the utilization of BlackBoard Collaborate software as a web based software application where instructors could create office hours so they can use video and audio conferring to communicate.

Additionally, this PIA covers the utilization of BlackBoard Collaborate as an integrated component to Blackboard Learn that JIBC currently uses as its primary Learning Management System. The new software, Blackboard Collaborate, is a plug in that is accessing by students and faculty that is intended to be an alternative to traditional face to face instructional delivery methods.

3. Related Privacy Impact Assessments

None

4. Elements of Information or Data

The software creates URLs for faculty and students to access. When a student accesses the video conferencing tool though either, the existing self-hosted Blackboard LMS or the Collaborate interface, the following information is stored in the cloud environment:

- *Name*
- *Email address*
- *Student and instructor chat information*
- *Video recordings*

An acknowledgment advising students that specific and relevant JIBC staff will have access to the video recordings that contain student chat information will be placed on the application.

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.

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

[redacted]

6. Data-linking Initiative* S.15(1)(l)

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.	no

7. Common or Integrated Program or Activity*

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.	
1. This initiative involves a program or activity that provides a service (or services);	yes
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.	no

**** 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.

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

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA**

			Authority
1.	*User video conferencing made available*	*Use*	*32 (a)*
2.	*Personal data collection statement provided to user*	*Collection*	*27 (2) (a)*
3.	*User accesses video conferencing application*	*Use*	*26 (a), (b), (d) (i) (ii),*
4.	*Users accesses conferencing chat tools within application*	*Use*	*33.2(c) and 32(a)*
5.	*Archived video accessed by institution*	*Use*	*31 (b)*

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Access to information limited by organizational system security. Code of conduct; policies; training server to protect the privacy of the data.*	*Low*	*Low*
2.	*Insecure data transfer*	*Data access is limited and internal and vendor policies and contracts state that data must be transferred in a secure method that is agreeable to both parties.*	*Low*	*Medium*
3.	*System security breach*	*Policies; security assessments; and end user training are used to mitigate the possibility of security breaches.*	*Low*	*Medium*

10. Collection Notice

Individuals using the application are informed of the following:

Privacy considerations in Blackboard Collaborate

Be aware that Blackboard Collaborate session text messages (even 'private' messages) are always visible to moderators, and that all your sessions will be recorded and accessible to program administrative staff, Blackboard Collaborate administrators and Service Desk staff, as well as the other students in your course. You should not enter any text messages, make any verbal statements (into the microphone), or share any materials that you are not comfortable sharing with others or having archived as a permanent record.

Confidentiality Statement

Learning in the Blackboard Collaborate environment requires that you know the extent to which your confidentiality is respected. It also requires that you respect the confidentiality of others. Only the instructor, program administrative staff, Blackboard Collaborate administrators, Service Desk staff, and the students registered in your course should have access to your Blackboard Collaborate sessions. No one else should be given access to the sessions without the approval of the participants; you should not share your login information with anyone! Communication and materials from your Blackboard Collaborate session should not be forwarded to people not registered in your course.

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).**

[redacted]

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

[redacted]

[redacted]

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

The institute has extensive security policies and practices in effect.

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 security. Users only granted access to parts of the system that are required. Changes in access are recorded.

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

Role based security. Users only granted access to parts of the system that are required. Changes in access are recorded.

Part 4 – Accuracy/Correction/Retention of Personal Information

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?

No personal information disclosure.

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

No

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.

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).	

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

Blackboard Collaborate Online Screen Sharing

PIA#2020 004

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

The initiative contains contact information and information that the users of the systems have been warned will be widely viewable. I do not see high risks with this system and it has appropriate controls in effect.

Privacy Officer/Privacy Office Representative	Signature	Date
George Jones		2020 March 25

X

George Jones
Director

Part 7 – Program Area Signatures

Ronald Bowles		2020 March 25
Program/Department Manager	Signature	Date
Mike Proud		2020 March 25
Head of Public Body, or designate	Signature	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.