Privacy Impact Assessment for Non-Ministry Public Bodies

Respondus Inc.

PIA# *2020 009*

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:	**Health Sciences Division**		
PIA Drafter:	**Deborah Richards**		
Email:	dyrichards@jibc.ca	Phone:	604.812.5002
Responsibility:	**John Trimble**		
Email:	jtrimble@jibc.ca	Phone:	604.528.5600

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

1. Description of the Initiative

This PIA relates to the Justice Institute of British Columbia's ("**JIBC**") use of Respondus Inc. Lockdown Browser ("**Respondus**").

A JIBC Department has identified a need to implement the use of a tool to support the ongoing security and integrity of the administration of program examinations online within its program. An existing tool was identified to support that need. It is a custom browser that locks down the testing environment within the learning management system, and which integrates with JIBC's existing learning management system, Blackboard. The tool is Blackboard Respondus Lockdown Browser (https://web.respondus.com/he/lockdownbrowser/) which is a downloadable application that can be

installed on local computers and provides a customized user interface within the person's internet browser.

Respondus is used at over 1500 higher educational institutions for securing online exams in classrooms or proctored environments.

2. Scope of this PIA

The following items are considered in-scope for this review:

- privacy and security of the Respondus tool and service; and
- data collected, stored, retained, disclosed and disposed in connection with the User of Respondus.

3. Related Privacy Impact Assessments

No other PIAs are currently related to this project.

4. Elements of Information or Data

Respondus collects various information relating to the User's purchase or use and/or interactions with its Services to deliver, improve, update and enhance the Services it provides to the User.

For the proposed use of the tool within the Health Sciences Division, learners (end users) will be required to download and install the lockdown browser via a link that is provided to the following site:

https://download.respondus.com/lockdown/download.php?id=544886982

To take the online test, learners start LockDown Browser, log into the Institute's Blackboard LMS, go to their course, then navigate to the exam.

Learners enter no personal identifying information in order to access the lockdown browser.

The data privacy information on the Respondus website (Respondus_Data_Privacy.pdf) indicates that the use of the plug tool **does not**:

- require students to register at a Respondus website
- have students provide an email, password, or address
- link students with a 3rd-party identification service
- store biometric profiles on our servers
- watch students live while taking exams

- "drop in" on students during an exam
- cross-reference network or location data of student
- sell or share data (it's the institution's data
- store student grades on Respondus servers
- access files or data on the student's computer

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 S.15(1)(l)

[redacted]

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.	

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.	

**** 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

No end user personal information is required or entered for the student to use the lockdown browser during an exam.

9. Risk Mitigation Table

The following table indicates the associated risk levels as applicable and the potential or intended mitigation steps.

Risk Mitigation Table				
	Risk	Likelihood	Impact	Mitigation
1.	Student personal information is compromised when transferred to or from the service provider	Low	Medium	• Transmission is encrypted

10. Collection Notice

The use of the Blackboard Respondus Lockdown Browser does not require learners to input any personal information. The program area will provide learners with notice that the tool is being used for exam invigilation throughout the program. The notice would state clearly

1. the purpose for the use of the tool;
2. that personal data is not collected by use of the system, except for instances when a student exits an exam early with LockDown Browser. In that situation the student ID (which, in the absence of any other identifiable information, we do not consider to be personal information) and the reason provided by the student are stored by Respondus, so the reason can be accessed and assessed by the instructor;
3. information to contact the lead instructor for the course if they have questions.

This notice would be included on literature addressed to learners in program guidelines, as well as during delivery of verbal examination instructions at each exam sitting.

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 Ministry Information Security Officer (MISO) when filling out this section. Your MISO will also be able to tell you whether you will need to complete a separate assessment called a Security Threat and Risk Assessment (STRA) for this initiative.

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

[redacted]

S.15(1)(l)

[redacted]

[redacted]

12. Please describe the technical security measures related to the initiative (if applicable).

See section 11.

13. Does your branch rely on security policies other than the Information Security Policy?

No.

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.

N/A

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

N/A

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 ministry notify them of the update, correction or annotation?

Not applicable - as individual student information, other than potentially Student ID, is not stored by Respondus.

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

If a student had to leave an examination for any reason the student ID the student ID would be sent to Respondus, and then information sent for the instructor to look review. An instructor, upon reviewing the information could make a decision that would affect the student's ability to continue writing the exam, continue from where they exited the examination or start the exam again, or write the exam not using the browser, etc. Any student decisions would be made in relation to program examination guidelines.

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.

The invigilator would be required to confirm that the Student ID and exam details match with the information that they have for the student, is accurate and complete. As all examinations are delivered online in an in person setting this verification would be in person. If the issue is more than an administrative or system failure issue then the process that would be followed would be in line with academic integrity procedures.

19. If you answered "yes" to question 17, do you have approved records retention and 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?

Yes.

Part 5 – Further Information

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

No.

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

No.

22. Will a personal information bank (PIB) result from this initiative?

No.

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

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

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).

Comments

Respondus stores personal information outside of Canada and engaged service providers who may be located outside of Canada but not for its Lockdown Browser.

Although Respondus stores personal information outside of Canada, the only information of a student that may be stored with Respondus is the student's student ID, which, in the absence of any other identifiable information, we do not consider to be personal information.

Privacy Impact Assessment for Non-Ministry Public Bodies

Respondus Inc.

PIA# *2020 009*

Part 7 – Program Area Signatures

Deborah Richards	Deborah Richards Digitally signed by Deborah Richards Date: 2021.05.04 10:37:09 -07'00'	5/4/21
Program/Department Manager	Signature	Date
George Jones	N/A	
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Mike Proud	Mike Proud Digitally signed by Mike Proud DN: cn=Mike Proud, o=JIBC, ou=Finance, email=mproud@jibc.ca, c=CA Date: 2021.05.05 10:25:17 -07'00'	5/5/21
Head of Public Body, or designate	Signature	Date
Derek Deacon	Derek Deacon Digitally signed by Derek Deacon Date: 2021.05.04 11:54:09 -07'00'	
Privacy Officer/Privacy Office Representative	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.