Privacy Impact Assessment for Non-Ministry Public Bodies

ApplyProof

PIA#*2021-012*

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:	Office of International Affairs		
PIA Drafter:	Derek Deacon - General Counsel		
Email:	ddeacon@jibc.ca	Phone:	**604-528-5897**
Program Manager:	Rod Torrezan – Manager, International Programs and Partnerships		
Email:	rtorrezan@jibc.ca	Phone:	**604-528-5753**

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

1. Description of the Initiative

ApplyProof makes it possible for students and immigration officials to verify their JIBC Proof of Acceptance securely and efficiently.

2. Scope of this PIA

This section should explain, where applicable, exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover. For example, if a public body is overhauling its citizen engagement process to better align with emerging self-service trends and is launching new website features, this particular PIA may only be about the public body's new blog.

This blog would then be the "scope" of the PIA. This section may also describe what phase of the initiative this PIA covers.

3. Related Privacy Impact Assessments

This section should identify, where applicable, PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative. To follow on from the above example, this section may cite a PIA that has already been completed on the public body's website or on the video site that the new blog will sometimes link to.

4. Elements of Information or Data

Student name, student number, email address, birthdate.

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;	N/A
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.	N/A
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.	N/A ??
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

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

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*JIBC staff uploads proof of acceptance documents to ApplyProof and insert relevant information*	*Use and Disclosure*	*32(a) and 33.2(a)*
2.	*Documents are made accessible via code and passcode on ApplyProof's website*	*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.	*Employees could access personal information and use or disclose it for personal purposes*	*Oath of Employment; contractual terms, etc.* *Minimal Staff with access. Roll access minimized to Operations team.*	*Low*	*High*
2.	*Request may not actually be from client (i.e. their email address may be compromised)*	*The system implements two keys for use. One is created by the supplier of the document and the other is known to the data subject. A compromised email would not allow access to the data within the system.*	*Low*	*High*
3.	*Client's personal information is compromised when transferred to the service provider*	*Transmission is encrypted using strong ciphers using public certificates*	*Low*	*High*
4.	*Inherent risks in sending personal information to a client via email*	*Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail* *Institution routinely (monthly) tested for defaulted encrypted email transport. Any institution which does not default to an strong encrypted email transport is notified to correct. Escalation occurs if they fail to correct. Testing automated via TLSChecker.*	*Low*	*Medium*

10. Collection Notice

Not applicable, as the use of ApplyProof itself does not require collection of personal information not already collected.

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).**

S.15(1)(l)

[redacted]

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

[redacted]

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

There are over 50 polices in our compliance program. Our compliance is designed to meet GDPR and Canadian new CPPA legislation. As legislation changes ApplyProof will adapt.

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.

[redacted]

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

[redacted]

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?

Should a data subject request an information clarification, this would be routed through to the education institution or other entity which posted the incorrect content. For example, a Bank issues a GIC certificate into the system which allows the Student, (Data Subject) to file a Canadian Visa application. The document is part of the "Proof of financial support" to be given to Canadian Immigration. The Data subject realized there is an error in the GIC certificate when they view the posted file. They would then contact their financial institution requesting a correction. The financial institution would make the corrections and repost the file with a new set of access keys.

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

No, the system simply provided a way to certify the content provided by the posting organization is accurate and digitally signed confirming it has been unaltered from it's time of posting.

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 Posting entities have access controls in place to prevent unauthorized content from being fraudulently posted to the ApplyProof system.

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?

The schedule is set by the posting organization and can be overridden by the data subject.

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.

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).

ApplyProof may be used for its intended purpose without restriction.

Privacy Officer/Privacy Office Representative	Derek Deacon Digitally signed by Derek Deacon Date: 2021.04.15 16:34:10 -07'00' Signature	Date

Part 7 – Program Area Signatures

Rodolfo Torrezan	Rodolfo Torrezan Digitally signed by Rodolfo Torrezan Date: 2021.04.15 11:39:00 -07'00'	April 15, 2021
Program/Department Manager	Signature	Date
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: 2021.04.19 09:01:31 -07'00'	April 19, 2021
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.