AP116-1 Privacy Impact Assessment for Non-Ministry Public Bodies TEMPLATE

Table of Contents

Before you start 1
PART 1: GENERAL INFORMATION 2
PART 2: COLLECTION, USE AND DISCLOSURE 4
PART 3: STORING PERSONAL INFORMATION 5
PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 5
PART 5: SECURITY OF PERSONAL INFORMATION 8
PART 6: ACCURACY, CORRECTION AND RETENTION 9
PART 7: AGREEMENTS AND INFORMATION BANKS 11
PART 8: ADDITIONAL RISKS 12
PART 9: SIGNATURES 12

Use this privacy impact assessment (PIA) template if you work for or a service provider to a non-ministry public body in BC and are starting a new initiative or significantly changing an existing initiative.

Before you start

- If you are in a non-ministry public body, you may use this template to document a PIA. This template leads you through a complete PIA but you are welcome to use another template or method for documenting your PIA
- An initiative is an enactment, system, project, program or activity
- Find information on the PIA review process and question-by-question guidance.
- If you have any questions, email Privacy.Helpline@gov.bc.ca or phone 250 356-1851

Privacy Impact Assessment [Initiative]

Why should I complete a PIA?

A PIA is a tool to help Schools/Districts ensure compliance with applicable privacy legislation. This document helps mitigate and evaluate many of the unintended risks and consequences that can develop as a result of not anticipating multiple perspectives and circumstances with a new system or project. As part of the process, schools/districts are taking the appropriate steps to ensure that parents, students and educators understand what measures are taken with regards to the safety and security of personal information and the importance of informed consent.

Section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act* (FIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FIPPA.

School/District staff need to contact the privacy office(r) or PIA Drafter, at their School/District, to determine internal policies for review and signing-off of a Privacy Impact Assessment. Staff may submit PIAs to their Superintendent of Schools for consideration. If you have any questions about this PIA template or FIPPA in general, you may contact the designated PIA Drafter as noted in this document or call the provincial **Privacy and Access Helpline at Enquiry BC** as noted below. Completed PIA's must be retained in a secure location at the School/District for the purposes of a Privacy Commissioner's Audit.

Note: This process can help identify and reduce many of the unintended risks and consequences that may potentially jeapordize student and educator privacy and security issues.

What if my initiative does not include personal information?

Best practices indicate that School/Districts' should still complete Part 1 of the PIA and submit it along with the signature pages to their privacy office(r) even if it is thought that no personal information is involved. This process ensures that the initiative has been accurately assessed to meet the requirements of FIPPA.

Note: The definition of personal information is "*Recorded information about an identifiable individual other than business contact information.*"

The following examples are a non-exhaustive list of personal information:

- Name, address, email address or telephone number;
- Age, sex, religious beliefs, sexual orientation, marital or family status, blood type;
- Information about an individual's health care history, including a physical or mental disability;
- Information about an individual's education, financial, criminal or employment history;
- Social Insurance Number(SIN) and Personal Education Number (PEN); and
- Personal views, opinions, religious or political beliefs or associations.

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	
Organization:	
Branch or unit:	
Your name and title:	
Your work phone:	
Your email:	
Initiative Lead name and title:	
Initiative Lead phone:	
Initiative Lead email:	
Privacy Coordinator:	
Privacy Coordinator ph:	
Privacy Coordinator email:	

General information about the PIA:

Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
Is this initiative a common or integrated program or activity? Under section FIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
Related PIAs, if any:

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.

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?

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.

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.

Type "yes" or "no" to indicate your response.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Coordinator. 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.

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**	**FIPPA authority**	**Other legal authority**
Step 1:			
Step 2:			
Step 3:			
Step 4:			

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice (except in limited circumstances).

Review the sample collection notice and write your collection notice below. You can also attach the notice as an appendix.

PART 3: STORING PERSONAL INFORMATION

If you are 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?

Type "yes" or "no" to indicate your response.

8. Does your initiative involve sensitive personal information?

Type "yes" or "no" to indicate your response.

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

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

Type "yes" or "no" to indicate your response.

- 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.

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 Cooridnator.

11. Is the sensitive personal information stored by a service provider?

Type “yes” or “no” to indicate your response.

- 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)?

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

13. Does the contract you rely on include privacy-related terms?

Type “yes” or “no” to indicate your response.

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

14. What controls are in place to prevent unauthorized access to sensitive personal information?

15. Provide details about how you will track access to sensitive personal information.

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.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

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.**

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? Type "yes" or "no" to indicate your response.

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

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FIPPA section 30?

Type "yes" or "no" to indicate your response.

- 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?

Describe where the digital records for your initiative are stored (e.g. on your organization's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.

If you have completed a security assessment, you may want to append it to the PIA.

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	
Employees that need standing or recurring access to personal information must be approved by executive lead	
We use audit logs to see who accesses a file and when	
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?

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

22. Requests for correction

FIPPA 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.

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

Type "yes" or "no" to indicate your response.

22.2 Sometimes it's not possible to correct the personal information. FIPPA 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?

Type "yes" or "no" to indicate your response.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA 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?

Type "yes" or "no" to indicate your response.

23. Does your initiative use personal information to make decisions that directly affect an individual?

Type "yes" or "no" to indicate your response.

- 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?

FIPPA 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.

Type “yes” or “no” to indicate your response.

- 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?

Type “yes” or “no” to indicate your response.

- 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.

Type “yes” or “no” to indicate your response.

- 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:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Secretary-Treasurer's Privacy Office 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 Office Representative			

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			