AP I2 Privacy Impact Assessments

Legislative References: *Freedom of Information and Protection of Privacy Act (FOIPPA)* section 69
Policy Reference: None
Collective Agreement References: None
Date: May 10, 2024

Purpose

Section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires districts to conduct Privacy impact Assessments (PIA) to determine whether a project involves personal information and if so, how personal information will be protected as it is collected or used in a project.

The purpose of this Administrative Practice is to set out the District's process for conducting a Privacy Impact Assessment in accordance with the FOIPPA. If a new initiative has an application or software associated with its use or implementation, then a New Application/Software Request must first be undertaken and approved in accordance with Administrative Practice I7 New Application/Software Request.

Definitions

"common or integrated program or activity" has the same meaning as in the Act;

"**data-linking program"** has the same meaning as in the Act;

"head" has the same meaning as the head of a public body that is a not a ministry in Schedule 1 of the Act;

"initiative" means an enactment, system, project, program, or activity;

"ministry" means a ministry of the government of British Columbia;

"personal information" has the same meaning as in the Act;

"privacy impact assessment (PIA)" has the same meaning as in the Act;

"privacy risk" includes:

- an inherent risk of unauthorized collection, use, disclosure, or storage of personal information; and
- something that may inappropriately override or otherwise limit personal privacy.

The level of risk may vary based on:

- the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information; and,
- the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information.

"public body" means a public body as defined in the Act that is not a ministry; and,

"service provider" has the same meaning as in the Act.

1. When to Conduct a PIA

1.1. A PIA must be conducted on a new initiative for which no PIA has previously been conducted.

1.2. A PIA must be conducted before implementing a significant change to an existing initiative, including but not limited to a change to the location in which sensitive personal information is stored, when it is stored outside of Canada.

1.3. Where a PIA is not required by items 1.1and 1.2 above, a PIA may be conducted at the discretion of the head, and in accordance with these directions.

2. Elements within a PIA

2.1. Identify the purpose or objective of the initiative.

2.2. Identify the information elements, including personal information, to be collected, used, disclosed, or stored, and confirm that the personal information elements are necessary for the purpose of the initiative.

2.3. Where applicable, identify:

2.3.1. how and from whom the personal information will be collected;
2.3.2. how the personal information will be used;
2.3.3. how and to whom personal information will be disclosed; and
2.3.4. if an assessment or disclosure for storage of personal information outside of Canada is required, as per section 3 below..

2.4. Identify relevant legal authority (or authorities) authorizing the collection, use, or disclosure of personal information, as applicable.

2.5. If the initiative involves personal information, identify privacy risks and privacy risk responses that are proportionate to the identified risk.

2.6. Identify reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made.

2.7. Designation of the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative.

2.8. Identify if a supplementary assessment in section 5 of disclosure for storage of personal information outside of Canada is required for an initiative by determining:
  2.8.1. whether the initiative involves personal information that is sensitive; and,
  2.8.2. if the personal information that is sensitive is disclosed to be stored outside of Canada.

3. Where applicable, the head of the public body must confirm their adherence in the PIA to the following requirements under Part 3 of the Act:

3.1. Confirm that notice of collection will be given to individuals per section 27 (2) of the Act, or confirm that notice of collection is not required, per section 27 (3) of the Act;

3.2. Where personal information is used to make a decision that directly affects an individual, confirm that reasonable efforts will be made to ensure the accuracy and completeness of personal information per section 28 of the Act;

3.3. Confirm that a process is in place, per section 29 of the Act, to correct individuals' personal information upon request, or to annotate their personal information if it is not corrected per the individual's request;

3.4. Where personal information is used to make a decision that directly affects an individual, confirm that the personal information will be retained for at least one year after use, per section 31 of the Act;

4. Privacy Assessment Forms

4.1. The district Privacy Assessment Form, in accordance with the template provided by the Minister responsible for the Act, as appended, must be used for a PIA.

5. Directions on a supplementary assessment of disclosure for storage of personal information outside Canada

5.1. If the conditions in 2.8 are not met, or the disclosure outside of Canada is made in accordance with section 33 (2) (f), an assessment of disclosure for storage of personal information outside of Canada is not required.

5.2. If both conditions in 2.8 are met, then an assessment of disclosure for storage of personal information outside of Canada is required.

5.3. If an assessment of disclosure for storage of personal information outside of Canada is required, the head of a public body must identify the privacy risk(s) as well as the level of the privacy risk(s) associated with the disclosure by examining factors which include but are not limited to the following:

5.3.1. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;

5.3.2. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;

5.3.3. whether the personal information is stored by a service provider; and,

5.3.4. where the personal information is stored.

5.4. For each privacy risk, identify a privacy risk response that is proportionate to the level of risk posed. These may include technical, security, administrative or contractual measures (e.g. ways to manage and review access to personal information).

5.5. The outcome of the assessment of disclosure for storage of personal information outside Canada will be a risk-based decision made by the head of the public body on whether to proceed with the initiative, considering 5.3 and 5.4.

PRIVACY IMPACT ASSESSMENT

GULF ISLANDS SCHOOL DISTRICT 64

TEMPLATE

Updated May 2024

TABLE OF CONTENTS

PART 1: GENERAL INFORMATION

OFFICE USE ONLY: PIA file number:

Initiative title:	
Organization:	
Branch or unit:	
Initiative Lead name and title:	
Initiative Lead phone:	
Initiative Lead email:	
Privacy Officer:	Lori Deacon, Director of Corporate Services
Privacy Officer phone:	250-537-5548
Privacy Officer email:	Ldeacon@sd64.org

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
(yes or no)
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
(yes or no)
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.
(general description of the software; how accounts are created; vendor address)

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?
(be sure to reference data collection and use policy and data portability/data retention policy)

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.
(be sure to reference data collection and use policy and data portability/data retention policy)

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 Officer. 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**	**FOIPPA 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, FOIPPA 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're 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 FOIPPA SECTION 33(2)(F)?

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

- If yes, go to Part 4
- If no, go to question 10

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 Officer.

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.

16. 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.

17. DOES YOUR INITIATIVE INVOLVE DIGITAL TOOLS, DATABASES OR INFORMATION SYSTEMS?

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

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

17.1 DO YOU OR WILL YOU HAVE A SECURITY ASSESSMENT TO HELP YOU ENSURE THE INITIATIVE MEETS THE SECURITY REQUIREMENTS OF FOIPPA 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 19
- If no, go to question 18

18. 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.

19. 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.

20. HOW WILL YOU MAKE SURE THAT THE PERSONAL INFORMATION IS ACCURATE AND COMPLETE?

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

21. REQUESTS FOR CORRECTION

FOIPPA 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.

21.1 DO YOU HAVE A PROCESS IN PLACE TO CORRECT PERSONAL INFORMATION?

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

21.2 SOMETIMES IT'S NOT POSSIBLE TO CORRECT THE PERSONAL INFORMATION. FOIPPA 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.

21.3 IF YOU RECEIVE A REQUEST FOR CORRECTION FROM AN INDIVIDUAL AND YOU KNOW YOU DISCLOSED THEIR PERSONAL INFORMATION IN THE LAST YEAR, FOIPPA 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.

22. 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 23
- If no, skip ahead to Part 7

23. DO YOU HAVE AN INFORMATION SCHEDULE IN PLACE RELATED TO PERSONAL INFORMATION USED TO MAKE A DECISION?

FOIPPA 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 yes, 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.

24. 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

25. 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.

Department:	*The organizational unit or units with responsibility for custody of the records: (District, Education, Finance, Governance, HR/Payroll, Operations*
Title	*Self-explanatory.*
Location:	*Physical site or sites at which the records are kept. Note that not all similar locations, example Departments, schools may necessarily maintain any specific bank.*
Individuals in Bank:	*The individual whom the information is about.*
Information Maintained:	*Description of the type of information.*
Purpose:	*The reason that the information is collected and required.*
Users:	*Self-explanatory.*
Authority for Collection:	*Any collection of personal information must be authorized by the Freedom of Information and Protection of Privacy Act. As well as permitting collection for certain purposes, the Act allows collection if authorized under another statute. Accordingly, most of the personal information collected by the District is pursuant to the School Act.*

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.

26. 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 Privacy Officer 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 Officer / 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:

(add comments here)

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)*			