

NAME OF PROJECT LEAD AND DEPARTMENT

Privacy Impact

Assessment

Date

PROJECT TYPE

|  |
| --- |
| ***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 officer for their public body to determine internal policies for review and to sign off on the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.  Contact the CMTN privacy officer for question-specific guidance on completing a PIA by sending an email to [foi@coastmountaincollege.ca](mailto:foi@coastmountaincollege.ca). |

|  |
| --- |
| ***What if my initiative does not include personal information?***  Public bodies (which include CMTN) still need to complete Part 1 of the PIA and submit it, along with the signature pages, to their privacy officer even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed. |

**Part 1 – General Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name of Department/ Branch** |  | | |
| **PIA Drafter:** |  | | |
| **Email:** |  | **Phone**: |  |

## Description of 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 are doing, how it works, who is involved, and when or how long your initiative runs.

## Scope of this 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 beyond the scope of this PIA?

## Data or Information Elements Involved in Your Initiative

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, list categories or other groupings of personal information in a table or in an appendix.

## Did you list personal information in question 3?

## [Personal information](https://www2.gov.bc.ca/gov/content?id=45F56451625849E49141D4AF85D8EEC2) 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](#_PART_2:_).
* If no, answer [question 4](#_How_will_you_1) and submit questions 1 to 4 to your institution’s privacy officer. You do not need to complete the rest of the PIA template.

## Reducing the Risk of Unintentionally Collecting Personal Information

Sometimes initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident or privacy breach. How will you reduce this risk?

**Part 2 – Collection, Use, and Disclosure**

This section will help you to identify the legal authority for collecting, using, and disclosing personal information and to confirm that all personal information elements are necessary for the purpose of the initiative.

1. **Collection, Use, and Disclosure**

In the first column of this table, describe the way personal information moves through your initiative, step by step, as if you were explaining it to someone who knows nothing about your initiative.

In the shaded columns, your privacy officer will identify whether each step represents collection, use, or disclosure and will ensure you have legal authority for what you want to do.

Add or delete rows as needed.

**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.

| **Movement of Personal Information Through Your Initiative** | | **Information Collection, Use, and Disclosure** | **FOIPPA Authority** | **Other Legal Authority** |
| --- | --- | --- | --- | --- |
| Step 1 |  |  |  |  |
| Step 2 |  |  |  |  |
| Step 3 |  |  |  |  |

1. **Collection Notice**

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

Review the [sample collection notice](https://www2.gov.bc.ca/gov/content?id=650377D1931545499C09A855830530C3#q-6) and write your collection notice below. You can also attach the notice as an appendix.

**Part 3 – Storing Personal Information**

1. **Storing Personal Information Outside Canada**

If you are storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

* 1. **Is any personal information stored outside of Canada?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, go to question 7.2.
* If no, go to Part 5.
  1. **Where will you store the personal information involved in your initiative?**

**7.3 Does your initiative involve sensitive personal information?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, go to question 7.4.
* If no, go to Part 5.
  1. **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 5.
* If no, contact your PO and go to Part 4.

**Part 4 – Assessment of Disclosures Outside of Canada**

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You will likely need help from your privacy officer to complete this section. More help is available in the [Guidance on Disclosures Outside of Canada](https://www2.gov.bc.ca/gov/content?id=154B2A25C6DD493D8FA0F70C8135347C).

1. **Type of Storage Outside of Canada**
   1. **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 8.3.
* If no, go to question 8.2.

| **Name of Service Provider** | **Name of Cloud Infrastructure and/or Platform Provider(s)1** | **Where and How Sensitive Personal Information is Stored2** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
| 1. If applicable. 2. Including backups. | | |

* 1. **Provide details on the disclosure, including to whom it is disclosed and where and how the sensitive personal information is stored.**
  2. **Describe the contractual terms in place (if applicable).**
  3. **Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, go to question 8.5.
* If no, go to question 8.6.
  1. **Which enterprise service are you accessing?**

There may be a corporate PIA or other information to help you.

* 1. **What controls are in place to prevent unauthorized access to sensitive personal information?**
  2. **Provide details about how you will track access to sensitive personal information.**

* 1. **Describe the privacy risks for disclosure outside of Canada.**

Use the table below to indicate the privacy risks, potential impacts, likelihood of occurrence, and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include a reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Privacy Risk** | **Impact to Individuals** | **Likelihood of Unauthorized Use1 (L, M, H)2** | **Level of Privacy Risk (L, M, H)** | **Risk Response3** | **Any Outstanding Risks4** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 1. This includes collection, use, disclosure and storage of sensitive personal information. 2. Low (L), Medium (M), High (H). 3. This may include contractual mitigations, technical controls, and/or procedural and policy barriers. 4. Please describe any outstanding risks. | | | | | |

|  |
| --- |
| **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 or not to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 8.8. **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**

This part captures information about the privacy aspects 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 ensure that the personal information is safely secured in both physical (e.g., your office building or work environment) and technical (e.g., online cloud service) environments.

**9. Does your initiative involve digital tools, databases, or information systems?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, you may need to involve your privacy officer and possibly your director of IT. Together you can assess whether or not your initiative needs a security assessment.
  1. **Do you or will you have a** [**security assessment**](https://www2.gov.bc.ca/gov/content?id=7175C19B66564EA3A343AB8B668BEFC2) **to help you ensure the initiative meets the reasonable security requirements of**[**FOIPPA section 30**](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section30)**?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, append the security assessment to this PIA and go to question 9.4.
* If no, go to question 9.2.
  1. **Does your initiative involve generative artificial intelligence or machine learning?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* 1. **Are all digital records stored on government servers and are all physical records stored in government offices with government security?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, go to question 9.4**.**
* If no, describe where the records are stored and the technical and physical security measures in place to protect those records.
  1. **Controlling and tracking access**

In the table that follows, 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** | **Y or N** |
| We allow employees only in certain roles access to information. |  |
| Employees that need standing or recurring access to personal information must be approved by the appropriate authority. |  |
| We use audit logs to see who accesses a file and when. |  |

**Describe any additional strategies:**

**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.

**10. Accuracy of Personal Information**

[FOIPPA section 28](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section28) states that a public body must make every reasonable effort to ensure that an individual’s personal information is accurate and complete.

**10.1 How will you ensure that the personal information is accurate and complete?**

**11. Requests for Correction**

[FOIPPA](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section29) 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.

* 1. **Do you have a process in place to correct personal information?**

**Type “yes” or “no” to indicate your response.** **\_\_\_\_\_\_\_\_\_**

* 1. Sometimes it is not possible to correct the personal information. [FOIPPA](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section29) requires that you make a note on the record about the request for correction if you are unable to correct the record itself.

**Will you document the request to correct or annotate the record?**

**Type “yes” or “no” to indicate your response.** **\_\_\_\_\_\_\_\_\_**

* 1. If you receive a request for correction from an individual and you know you disclosed their personal information in the last year,[FOIPPA](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section29) requires that you notify the other public body or third-party recipient of the request for correction.

**Will you notify the other public body or third-party recipient?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* 1. **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 11.5.
* If no, go to Part 7.
  1. 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*](https://www2.gov.bc.ca/gov/content?id=EF2251FC065C485A8111A5CAB78DC952) requires that you dispose of government information only in accordance with an approved information schedule or with the approval of the chief records officer.

**Do you have an approved information schedule in place related to personal information used to make decisions?**

**Type “yes” or “no” to indicate your response.** **\_\_\_\_\_\_\_\_**

* If you answered no, describe how you will ensure that the information will be kept for a minimum of one year after it is used to make a decision that directly affects an individual.

**Part 7 – Agreements and Personal Information Banks**

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

**12. Does your initiative involve an** [**information sharing agreement**](https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/agreements-contracts/sharing-personal-information)**?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, complete the Information sharing agreement supplement and attach it to your PIA.

**13. Will your initiative result in a personal information bank?**

**Type “yes” or “no” to indicate your response. \_\_\_\_\_\_\_\_\_**

* If yes, complete points 13.1 to 13.4.
* If no, go to question 14.

**13.1 Describe the type of information in the bank.**

**13.2 Name the main ministry or agency involved.**

**13.3 Name any other ministries, agencies, public bodies, or organizations involved.**

**13.4 List the business contact title and phone number for the person responsible for managing the personal information bank.**

**Part 8 – Additional Risks**

**14.** In the table below describe any additional risks that arise from collecting, using, disclosing, or storing 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: |  |

**Part 9 – Privacy Officer 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 the privacy officer.

**Part 10 – Signatures**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Privacy Officer/Privacy Office Representative |  | Signature |  | Date |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Program/Department Manager |  | Signature |  | Date |
| Contact responsible for systems maintenance and/or security (signature not required unless they have been involved in the PIA) |  | Signature |  | Date |
| President & CEO |  | Signature |  | Date |

|  |
| --- |
| A final copy of this PIA (with all signatures) must be kept on record. |