



COLLEGE OF
THE ROCKIES

Privacy Impact Assessment

Name of Initiative:

PIA Number:

INSTRUCTIONS (READ BEFORE STARTING)

Submit a completed privacy impact assessment (PIA) before starting a new College Initiative or significantly changing an existing College Initiative that directly collects Personal Information, or results in the collection of Personal Information by COTR or a COTR service provider.

BC's Freedom of Information and Protection of Privacy Act (FIPPA) defines an "Initiative" as any enactment ("policy/procedure"), system (conceptual or technical), project, program, or activity.

Contact the COTR Privacy Officer (Keltie Rass – PrivacyOfficer@cotr.bc.ca) to receive support determining whether any change in how COTR employees are completing their duties to the College may require a Privacy Impact Assessment.

Read through this form entirely before starting to populate it. Each question is designed to capture specific information for review.

Some information recorded in the PIA may be confidential or proprietary and not intended for distribution. Before you share the draft or completed PIA (internally or externally), please contact COTR'S Privacy Officer, Keltie Ross at PrivacyOfficer@cotr.bc.ca for guidance.



PART 1: GENERAL INFORMATION

Initiative Title:	Github [REDACTED] S. 17(1)(c)
Department:	[REDACTED] S. 17(1)(c)
Initiative Lead (PIA Drafter) Name and COTR Email Address:	Miguel Peinado – mpeinado@cotr.bc.ca
Dean or Director Name, Title, and Email:	Nathan Skretting - CIO – nskretting@cotr.bc.ca
Privacy Officer Assigned:	
If initiative involves a third-party (i.e. vendor, consultant, partner), provide	
Third Party Name:	Github, Inc
Product Name (if applicable):	Github
Third Party Contact Name and Email:	
Third Party URL:	https://github.com/

1. In three to five sentences, describe the Initiative including:

- a) what you are doing,
- b) an overview of the process,
- c) who is involved,
- d) and when and/or how long your Initiative runs.

S. 17(1)(c)



2. In a few sentences, explain the scope of this PIA. For example, is this initiative limited to specific individuals or departments at COTR? Is this PIA covering the full initiative or just one phase of a larger project? Are there exceptions to how the Initiative will be implemented?

S. 17(1)(c)



3. Is this an administrative/operational, teaching and learning, or research Initiative? Select all that apply.

Administrative/Operational

Research (**Contact COTR
Privacy Officer before
continuing this PIA**)

Teaching and Learning

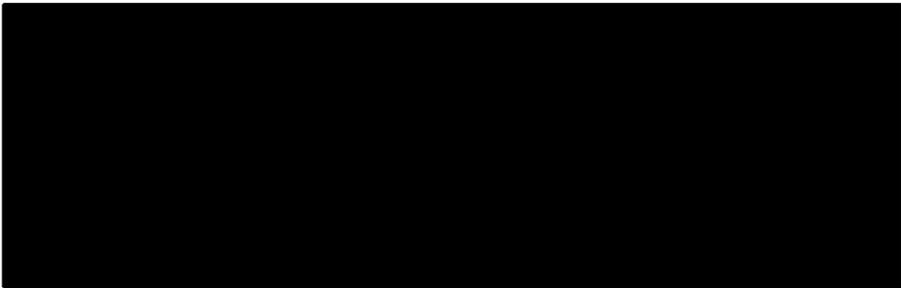
4. Has a PIA previously been completed for this Initiative?

Yes

No

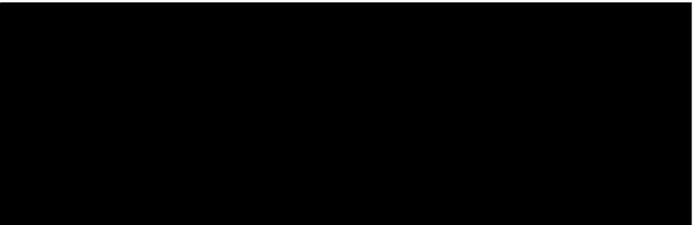
Not sure

5. What activities will occur within the Initiative? Use the bullet points below to make action statements. Replace the example action statement. Add or delete bullets as necessary.



S. 17(1)(c)

6. In a bulleted list, please list all the types of data or information you might collect, use, store, disclose, or access in your Initiative - even if they are not Personal Information. Replace the bullet points below with the actual elements of information or data.



S. 17(1)(c)

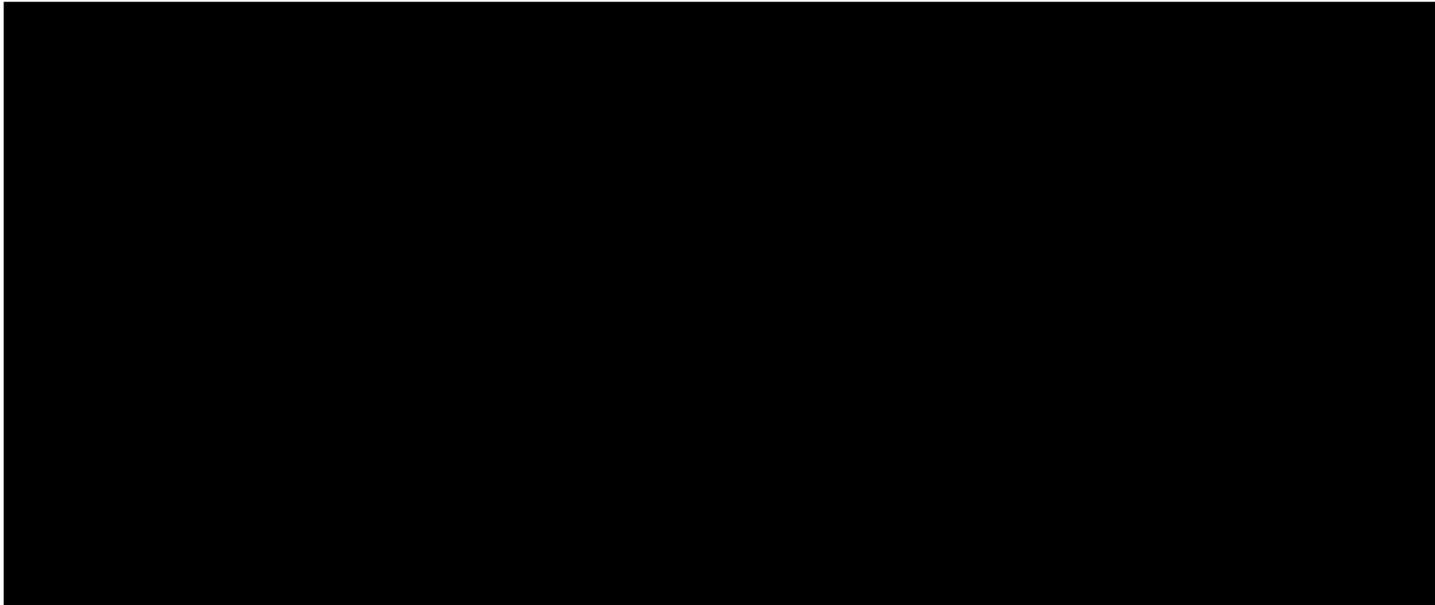
7. Did you list Personal Information in question 6? [Personal Information](#) is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.



Yes

No

8. If you answered "No" to question 7, in three to five sentences explain how will you ensure that you do not unintentionally collect Personal Information? S. 17(1)(c)



9. Does the Initiative involve integration between COTR IT systems and Third-Party systems?

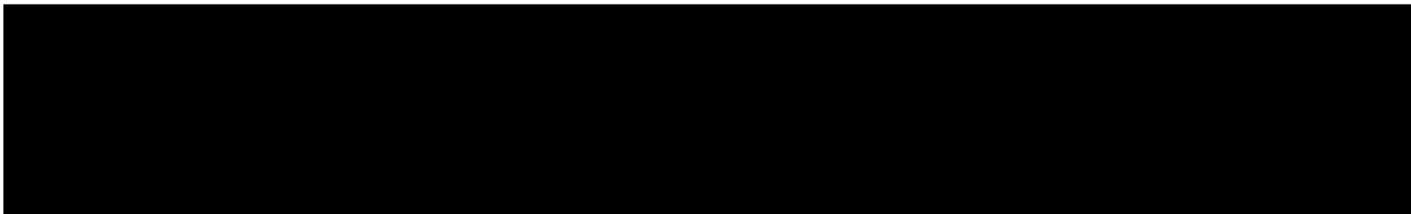
Yes

No

N/A

S. 17(1)(c)

If yes, list below: (put N/A on the first row if you answered No or N/A above. Add or delete rows)



If there is Personal Information involved in this Initiative, continue to complete the remaining sections of the PIA. If there is not any Personal Information involved in this Initiative, please submit questions 1-9 to the Privacy Officer along with the completed signatures page.

PART 2: COLLECTION

FIPPA sets out rules for public bodies and their employees to collect Personal Information. Unauthorized collection is prohibited. This section will help you identify the legal authority for **collecting** Personal Information and confirm that all Personal Information elements collected are necessary for the purpose of the initiative.

10. Whose Personal Information is collected in this initiative? Check all that apply.

- | | |
|---|---|
| <input type="checkbox"/> Students | <input type="checkbox"/> Former employees |
| <input type="checkbox"/> Prospective students | <input type="checkbox"/> Service provider employees |
| <input type="checkbox"/> Former students | <input type="checkbox"/> Donors or other constituents |
| <input type="checkbox"/> Alumni | <input type="checkbox"/> Volunteers |
| <input type="checkbox"/> Employees | <input type="checkbox"/> Other community members |

11. How frequently will the Initiative collect Personal Information?

- Single instance of collection within one semester or quarter
- Ongoing collection up to a single year
- Ongoing collection over more than one year

12. How many individuals' Personal Information will be collected?

- 1 - 50
- 51 - 500
- Over 500

13. If the Initiative involves a Third Party, are you able to test the product to see what personal information it collects?

- Yes
- No
- N/A (No Third-Party product involved)

14. Why is the Personal Information being collected? (check all that apply)
- The Personal Information is necessary and directly related to college operations. The collection of this Personal Information is directly related to the college's documented strategic directives, goals, or mandate letter directions.
 - The Personal Information is necessary and directly related to requirements explicitly stated in college bylaws, policy, and procedure.
 - The Personal Information is collected because collection is required or authorized under local, provincial, or federal law. Be prepared to directly cite the section of a particular law that applies if asked.
 - The Personal Information is collected for determining suitability for an honour or award including a scholarship, prize, or bursary.
 - The Personal Information is being collected for a quality assurance or improvement initiative that has been approved by the college Executive.
15. How will you reduce the risk of collecting unnecessary Personal Information? (Check all that apply.)
- The Initiative will only collect specific information deemed necessary for and directly related to the initiative
 - The Initiative will use forms with primarily closed-ended questions and minimal open-ended questions
 - The Initiative will use forms with drop-down menus
 - The Initiative will have documented data gathering and aggregation processes for open ended submissions or fields
 - The Department needs Privacy Officer review and support because none of the above apply
16. FIPPA Collection Notice: When collecting Personal Information, FIPPA requires that you provide a collection notice (except in limited circumstances). Please fill in the template collection notice below and remove bold and square brackets.

*The College of the Rockies ("COTR") collects your Personal Information in accordance with section 26 of the Freedom of Information and Protection of Privacy Act ("FIPPA"), R.S.B.C. 1996, c.165 for the purposes of **[explain purposes]**. If you have any questions about the processing of your Personal Information, please contact **[COTR employee or department/faculty]** at **[COTR email address]**.*

Please ask the Privacy Officer for assistance drafting your collection notice if your Initiative requires indirect collection of Personal Information (i.e. if a service provider collects Personal Information from students or employees on behalf of COTR). The Privacy Officer may recommend changes to the FIPPA Collection Notice that you draft above.



Privacy Impact Assessment

The Privacy Officer may also provide additional options for the FIPPA Collection Notice that would be required when collecting personal information. Please speak with them directly for this portion of the form before final submission.

PART 3: USE

FIPPA sets out requirements and restrictions related to use of Personal Information. This section will help you identify the legal authority for **using** Personal Information and ensure that the use of Personal Information is limited to the original purpose for collection.

17. What is the intended use of the Personal Information collected? (check all that apply)
- The Personal Information will be used for the purposes checked off in Question 14
 - The Personal Information will be used for secondary purposes, and I have a consent notice attached as an appendix to this PIA that meets the requirements found in FIPPA regulations. I will work with the COTR Privacy Officer to determine if secondary use is appropriate and compliant with FIPPA.
 - The Personal Information will be used for a purpose for which the information may be disclosed to the public body under [section 33](#). The COTR Privacy Officer will attach the relevant section number to this selection if it applies.
18. How will you ensure that parties using the Personal Information will use it only for the purposes stated in 17 above? Check all that apply.
- Documented department information management practices and training
 - Documented use restrictions communicated from your department to another COTR department
 - Written contract between COTR and a Third Party including explicit conditions
 - The Department needs Privacy Officer review and support because none of the above apply
19. Does your Initiative use Personal Information to make decisions that directly affect an individual?
- Yes No



20. What is the intended impact of the decisions that are being made that directly affect an individual? (check all that apply).

- Directly affects academic status or grades
- Directly affects how an individual accesses their courses, campus activities, or student supports
- Directly affects employment status, employee remuneration, or contract opportunities, and pay
- Directly affects how employees and service providers will complete their work
- Directly affects how employees access campus activities and support services
- Directly affects the College's capacity to protect individuals from harm
- Directly affects the College's capacity to interact with and support external parties
- N/A – The decisions are not intended to have a direct impact on individuals

21. Who will be using the Personal Information collected by this Initiative? (Check all that apply and provide details.)

Your department:	[put N/A if a service provider manages all Personal Information]
Other departments at COTR	External Partners and Service Providers
[put N/A if no other departments at COTR manage the Personal Information in this Initiative]	[Put N/A if there are not any External Third Parties including Service Providers managing the Personal Information in this Initiative]
[add more rows as necessary]	[add more rows as necessary]

PART 4: STORAGE

22. Is all Personal Information involved in your Initiative stored within standard COTR storage locations, technologies, or services?

- Yes No

If you answered yes, please list the approved standard COTR storage locations, technologies and/or services.

S. 15(1)(l), s. 17(1) and s. 19(1)



23. Is any Personal Information involved in your Initiative stored outside of Canada?

- Yes No

24. Where is the Personal Information stored? Please identify applicable geographic locations for primary storage and backups. If Personal Information is stored in more than one primary location, the COTR Privacy Officer can expand the response field in this question.

Primary Storage

City (if applicable):
Province, Region, or State:
Country:

Back-up Storage (if applicable)

City (if applicable):
Province, Region, or State:
Country:



25. Does your Initiative involve Sensitive Personal Information? (Any Personal Information can be Sensitive Personal Information in different contexts. Please contact the COTR Privacy Officer to discuss.)

- Yes
- No

26. Is any of the Sensitive Personal Information stored outside of Canada?

- Yes
- No

27. Where is the Sensitive Personal Information stored? Please identify applicable geographic locations for primary storage and backups. Type N/A in the cells on the first row if Sensitive Personal Information is not stored outside of Canada as indicated in Question 26.

Name of Third Party	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Name of cloud infrastructure and/or platform provider(s) (if applicable)

PART 5: DISCLOSURE

FIPPA sets out requirements and restrictions related to disclosure of Personal Information. This section will help identify the legal authority for **disclosing** Personal Information, and consider risks related to that disclosure. **Fill out this section if Question 26 was answered “Yes”**

Complete this section if you are disclosing Sensitive Personal Information to be stored outside of Canada. You may need help from the COTR Privacy Officer.

28. Is any Personal Information being disclosed outside of Canada under FIPPA section 33(2)(f)? This section allows for information to be made available to the public under an enactment that authorizes or requires the information to be made public.

Yes No

29. Is any of the Personal Information being disclosed outside of Canada under FIPPA section 33(2)(p)? This section allows disclosure for the purposes of (i) a payment to be made to or by COTR, (ii) authorizing, administering, processing, verifying, or cancelling a payment, or (iii) resolving an issue regarding a payment.

Yes No
 The payment processor is out of scope of this PIA



30. Describe the privacy risks for disclosure of Personal Information (PI) outside of Canada.

Use the table to indicate the privacy risks. For each privacy risk you identify, describe the potential impact to individuals or COTR, and 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, physical, technical, administrative measures) you outline elsewhere in this PIA. Privacy risks below are examples only; add new rows if necessary.

Privacy risk	Impact to individuals or COTR	Risk response
Unauthorized collection of PI by COTR employees		
Unauthorized use of PI by COTR employees		
Unauthorized disclosure of PI by COTR employees		
Unauthorized collection of PI by Third Party/ies		
Unauthorized use of PI by Third Party/ies		
Unauthorized disclosure of PI by Third Party/ies		

PART 6: PROTECTION

Please share how the initiative will secure Personal Information to protect personal privacy. 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.

31. Does your Initiative involve digital tools, databases, or information systems?

- Yes No

32. What physical security safeguards are in place to protect Personal Information in this Initiative? Identify the elements of physical security that protect where the records for your Initiative are stored (Check all that apply. Specify, "Other" if applicable)

S. 15(1)(l), s. 17(1) and s. 19(1)

Safeguard	At COTR	At Third Party
[Redacted content]		



33. What technical security safeguards are in place to protect Personal Information in this Initiative?

Describe the elements of technical security that protect where the records for your Initiative are stored (e.g. secure passwords, encryption, firewalls, etc.) (More options on the following page)

S. 15(1)(l), s. 17(1) and s. 19(1)

Safeguard	At COTR	At Third Party
[Redacted content]		



34. What administrative safeguards are in place to protect Personal Information?

Describe the elements of administrative security that protect where the records for your Initiative are stored (e.g., aliasing, aggregation, policies/procedures, standards of practice, etc.)

S. 15(1)(l), s. 17(1) and s. 19(1)

Safeguard	At COTR	At Third Party

35. If the Initiative involves a Third Party, please indicate what type of Agreement governs the relationship between COTR and the Third Party. Please select one.

- COTR'S GSA (negotiated Agreement between COTR and the Third Party)
- Vendor's Agreement (negotiated Agreement between COTR and the Third Party)
- Online "Terms of Service" or "Terms of Use" (often non-negotiable)
- Memorandum of Understanding/Memorandum of Agreement ("MOU"/"MOA")
- Other (specify):
- No Agreement

36. If the Initiative involves a Third Party, does an End User License Agreement ("EULA") apply to the individuals whose Personal Information is involved?

- Yes No

37. The Privacy Officer will need to review all draft/proposed Contracts/Agreements (and related materials, i.e. contract appendices/schedules; Third Party privacy policies or online terms and conditions, if any) involved in the Initiative. Have you ensured these have been provided? Check only one.

- Yes No N/A (No Third Party involved)

38. Where are the privacy related terms referenced in the contract or agreement if applicable? (Check all that apply)

- In the body of the contract or agreement
- Third Party will sign COTR's Privacy Protection Schedule
- Third Party will sign COTR's Data Security Schedule
- In the Third Party's privacy or data protection policy or appended schedules
- In a separate Information Sharing Agreement
- There are no privacy related terms in the contract or agreement (or related documentation)
- There is no contract or agreement for this Initiative

39. Controlling and tracking access

Review each strategy below that describes how to limit or restrict who can access Personal Information and how to keep track of who has accessed Personal Information in the past. Check all that apply. Specify "Other" if applicable.

- Managed role-based access to Personal Information for COTR employees
- Managed role-based access to Personal Information for Third Party
- Third Party access is time limited for installing, implementing, maintaining, repairing, troubleshooting, or upgrading an electronic system
- Third Party access escorted by authorized COTR employee
- Audit logs at COTR
- Audit logs from Third Party
- Other: *(fill in details)*

PART 7: ACCURACY AND CORRECTION

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. FIPPA also gives an individual the right to request correction of errors or omissions to their Personal Information.

In this section, please demonstrate how you will make a reasonable effort to ensure the Personal Information you have on file is accurate and complete.

40. How will COTR ensure that the Personal Information is accurate and complete? (Check all that apply)

- Individuals input their own Personal Information
- Individuals update their own Personal Information
- Employee verifies that information is accurate and complete before processing
- Documented processes to ensure accurate and complete data entry and maintenance
- The Third Party manages the accuracy and completeness of Personal Information under the direction of COTR
- Software or service uses automated processes to enter and manage Personal Information
- Other: *(fill in details)*
- Other: *(fill in details)*

41. Is there a documented process in place to correct Personal Information?

- Yes No

42. Sometimes it is not possible to correct the Personal Information. FIPPA requires a process to make a note on the record about the request for correction if it isn't possible to correct the record itself. Is there a documented process in place to annotate the record?

- Yes No N/A (Corrections possible)

43. If there is a request for correction from an individual and COTR or the Third Party disclosed that individual's Personal Information in the last year, FIPPA requires that COTR or the Third Party provide the applicable other public body or Third Party about the request for correction. Will COTR or the Third Party ensure that these notifications are done when necessary?
- COTR will forward correction notifications
 - Third Party will forward correction notifications
 - COTR and Third Party will split responsibility based on who was authorized to disclose Personal Information to third parties before a correction request was made.

PART 8: RETENTION AND DISPOSITION

FIPPA requires that public bodies keep Personal Information for a minimum of one year after it is used to make a decision. Personal Information needs to be disposed of to limit privacy risk after legal retention timelines.

44. How long will COTR need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.

Record Type: Retention Period (in years/months):

45. How long will the Third Party need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.

Record Type: Retention Period (in years/months):

46. How will you ensure that the records containing Personal Information are disposed of in accordance with the retention schedule noted in questions above? (Check all that apply)

- Schedule records review and disposition dates in Outlook calendars
- Build conditions for disposal into department Standard Operating Procedures
- Send direct written communication to staff or service providers.
- Other (explain):

47. What methods will be used to dispose of Personal Information following retention period? (Check all that apply.)

- COTR business unit shredding on campus
- COTR contracted shredding service provider
- COTR deletion of electronic record(s)
- Service Provider shredding/deletion of record(s) under COTR contract
- Service Provider shredding/deletion of record(s) under COTR written instruction
- Other (explain):
- Other (explain):

PART 9: INFORMATION FLOW

48. Complete the Information Flow Table

Use column 1 to describe the way Personal Information moves through your Initiative step by step. Describe the steps as if you were explaining it to someone who does not know about your Initiative.

Use column 2 to identify whether the action in column 1 is a collection, use, or disclosure of Personal Information.

The Privacy Officer will complete column 3 to identify the legal authority you have for the collection, use, or disclosure.

Information Management Steps	Collection, use, or disclosure	FIPPA and other legal authorities
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.

PART 10: TRAINING

49. Identify which of the following activities all employees and Third Party (as applicable), will be trained on when collecting and managing the Personal Information for the College Initiative.

- Collection: Limit the collection to only what is explicitly necessary
- Use: Use the Personal Information only for the purpose for which it was originally collected
- Access: Only authorized employees (and, where applicable, service providers) may access the Personal Information
- Disclosure: Not to disclose the Personal Information inside or outside COTR unless authorized under FIPPA
- Storage: To store the Personal Information only in COTR-provided or approved storage locations and not to store unnecessarily in multiple locations
- Retention: to keep the Personal Information for a minimum of one year – with longer retention periods only when necessary
- Disposal: To dispose, when applicable, in a secure method that renders the Personal Information permanently irretrievable



PART II: PERSONAL INFORMATION BANKS

50. Will your Initiative result in a Personal Information Bank ("PIB")? A PIB is a collection of Personal Information searchable by name or unique identifier. If yes, please complete the table below. If more than one PIB will result, copy and paste an additional copy of the table below and fill out a separate table for each PIB.

Yes

No

Title	
Location	
Personal Information Types	
Categories of Individuals Included	
Collection Authority	
Purpose of Personal Information	
Categories of Persons Managing Information	

PART 12: PRIVACY OFFICE(R) COMMENTS

If, in the future, any substantive changes are made to the scope of this PIA, the College will have to complete a PIA Update and submit it to Privacy Office(r).

This PIA is based on a review of the material provided to the COTR Privacy Office(r) as of **(date/year)**.

The details provided in this PIA, indicates that the application to be developed and uploaded onto the COTR website can be delivered in compliance with FIPPA legislation.

Should there be a change in scope to this part of the initiative, further assessment and/or a PIA update may be required as new related or expanded service is considered, or the privacy policies for the College change in the future.

Any substantive changes made to the scope of this PIA would need to be included in a PIA update and submitted to the Privacy Office(r).

- https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00
- https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section26

Privacy Office Signature

This PIA is based on a review of the material provided to the Privacy Officer as at the date in Part 13 Privacy Officer Comments above.

Name and Title	Signature	Date signed
Keltie Ross		

PART 13: APPROVAL SIGNATURES

Institution Signatures

This PIA is compliant with FIPPA when it accurately documents information management practices 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 Department will inform the COTR Privacy Officer, and if necessary complete a PIA update.

By signing where required below, the signatories acknowledge and confirm their declarations as noted.

Declaration of Initiative Lead: I confirm that I understand the privacy impacts of this College Initiative and I am committed to my FIPPA obligations related to the collection and management of Personal Information involved in the Initiative. If there are any changes to the Initiative, including to the way Personal Information is collected, used, stored, or disclosed, I understand that the department will need to inform the COTR Privacy Officer and if necessary, complete a PIA update. I will establish and document information management guidelines for the Personal Information and ensure these are followed. I will ensure employees are trained on and able to comply with their obligations under FIPPA; related College policies and procedures; and COTR Privacy Officer recommendations relative to this Initiative.

Signature of Initiative Lead or PIA Drafter

Name and Title	Signature	Date signed

Declaration of Dean / Director / One-Over-One Signatory: I confirm that I have reviewed this PIA and I acknowledge the residual privacy risks identified. I support the department by providing required time and operational resources to comply with FIPPA, related College policies and procedures, and COTR Privacy Officer recommendations relative to this Initiative.

Signature of Dean / Director

Name and Title	Signature	Date signed



Privacy Impact Assessment

Name of Initiative:

PIA Number:

Declaration of Information Security: I confirm that I am satisfied that the Information Security safeguards employed in this college Initiative meet reasonable requirements relative to the amount or sensitivity of the Personal Information or COTR business information described in this PIA.

Signature of Information Security (Required only when college Initiative involves Information Security considerations)

Name and Title	Signature	Date signed

Declaration of Information Technology: I confirm that I understand and approve of the proposed use-case of COTR IT systems described in this PIA, where applicable. I understand and approve of the Third Party's integration with COTR's IT systems for the College Initiative described in this PIA, where applicable.

Signature of Information Technology (Required when College Initiative involves use of COTR IT systems or integration of Third-Party technology with COTR IT systems.)

Name and Title	Signature	Date signed

Declaration of Head of Public Body or Designate: I have reviewed this PIA carefully and accept and will be accountable for the residual privacy risks identified for this College Initiative. I am satisfied with the completion of this PIA under FIPPA.

Signature of Head of Public Body or Designate Under FIPPA (Required only if Personal Information is involved in the Initiative as indicated in Question 7).

Name and Title	Signature	Date signed