



Privacy Impact Assessment

Employee Experience Survey

Human Resources

Christina Kiriakakis, Director of Human
Resources

March 23, 2026



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.

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	Human Resources		
PIA Drafter:	Christina Kiriakakis, Director of Human Resources Aman Kang, Director of President's Office		
Email:	CKiriakakis@coastmountaincollege.ca	Phone:	250.615.8634

1. Description of the Initiative

The initiative involves the administration of an anonymous employee experience survey designed to collect feedback from employees regarding their workplace experiences. The survey will gather information related to overall employee satisfaction, workplace improvement, and organizational practices.

Participation in the survey is voluntary, and responses are intended to be collected anonymously. No directly identifying personal information will be requested, and responses will not be intentionally linked to individual employees. Measures are in place to support anonymity and ensure that individuals cannot be reasonably identified through structured survey responses.

However, it is recognized that open-ended response fields may introduce a risk that individuals could voluntarily disclose identifying information about themselves or others. To mitigate this risk, participants will be advised not to include personal identifiers or sensitive information in open-text responses.

The information collected will be used solely to assess overall employee satisfaction, identify areas for improvement, and inform organizational decision-making aimed at fostering a positive and supportive workplace environment. Survey results will be analyzed and reported in aggregate form only to support continuous improvement initiatives and enhance employee engagement across the institution.

2. Scope of this PIA

This Privacy Impact Assessment (PIA) applies to the collection, use, disclosure, and storage of information obtained through the employee experience survey.

The collection of information through this initiative is authorized under section 26(c) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA), as it is necessary for the purposes of program planning, evaluation, and improvement of workplace practices and employee experience at Coast Mountain College (CMTN).

The scope of this PIA includes all processes and systems involved in administering the survey, including survey design, distribution, data collection, submission, analysis, reporting, and retention of survey responses. Survey responses will be submitted to the Human Resources department via [REDACTED] and accessed only by authorized staff for the purposes outlined above. Survey data will be retained for five years to analyze trends.

15 (1)(I)

Although the survey is designed to be anonymous and does not intentionally collect directly identifying personal information, this PIA assesses potential privacy risks associated with indirect identification, including the possibility of self-identification through open-ended responses.

This PIA is limited to the employee experience survey initiative and does not extend to other human resources data collection activities or employee information systems. Any future changes to the scope, purpose, or method of information collection, including the introduction of identifiable data elements or new technologies, will require a review and potential update of this PIA.

3. Data or Information Elements Involved in Your Initiative:

The personal information collected through this form includes the following elements (see included form):

Category	Information Collected	Purpose
Survey Response Data	Responses to structured questions, including employee satisfaction levels, and feedback on workplace experience. Questions are based on the following categories: 1. Job Satisfaction 2. Leadership	To assess overall employee satisfaction, evaluate workplace conditions, and inform organizational decision-making and continuous improvement initiatives

	3. Communication and Collaboration 4. Equity, Diversity, Inclusion, and Belonging 5. Health and Wellness 6. Professional Development 7. Other – Open-ended question	
Open-Ended Responses	Voluntary written comments and qualitative feedback provided by participants	To gather detailed insights, suggestions, and contextual feedback to support improvements in the workplace environment
Technical/Administrative Data	Limited system-generated data such as submission timestamps or response identifiers	To support survey administration, ensure data integrity, and manage response collection

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.

Not applicable.

8. 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?

The survey is designed to be anonymous and does not intentionally collect directly identifying personal information. However, there is a risk that individuals may voluntarily include identifying information in open-ended responses. Participants will be advised not to include personal identifiers, and any such information will be mitigated prior to analysis and reporting.

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.

9. 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	Anonymous survey responses are collected directly from employees through ExploranceBlue, a College approved survey platform. No directly identifying personal information is requested. Participants may voluntarily provide information in open-ended responses, but are warned not to provide identifiable information.	Collection	Section 26(c) – Information is collected for the purposes of program planning, evaluation, and improvement of workplace practices	Not applicable
Step 2	Survey responses are submitted to the Human Resources department via [REDACTED] and accessed only by authorized staff	Collection	Section 26(c)	Not applicable
Step 3	Survey data is used in aggregate to assess employee satisfaction, identify trends, and inform organizational decision-making to improve the workplace environment	Use	Section 32(a) – Use consistent with the purpose for which the information was collected	Not applicable
Step 4	Aggregated and de-identified results may be shared internally with leadership or relevant	Use and disclosure	Section 33 (2)(d) – Disclosure for the same	Not applicable

15 (1)(l)

Movement of Personal Information Through Your Initiative		Information Collection, Use, and Disclosure	FOIPPA Authority	Other Legal Authority
	departments to support planning and improvement initiatives		purpose for which the information was collected or a consistent purpose	

10. 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).

The following collection notice will be provided:

"Personal information collected through this survey is authorized under section 26(c) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA-BC). The information you provide will be used solely for the purpose of assessing overall employee satisfaction, identifying areas for improvement, and informing organizational decision-making to support a positive workplace environment.

Your responses will be treated confidentially and will be accessed only by authorized staff within Coast Mountain College's (CMTN) Human Resources Department. Personal information will not be disclosed except as necessary to fulfill the purposes identified above or as required by law.

To maintain data integrity, survey responses are limited to one submission per employee.

If you have questions about the collection, use or disclosure of this information, please contact the Director of Human Resources by emailing [REDACTED]

For questions or concerns related to privacy, please contact the Privacy Officer by emailing foi@coastmountaincollege.ca."

15 (1)(l)

Part 3 – Storing Personal Information

11. 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.

7.1 Is any personal information stored outside of Canada?

No, personal information is not being stored outside of Canada.

7.2 Where will you store the personal information involved in your initiative?

Not applicable.

7.3 Does your initiative involve sensitive personal information?

Not applicable.

7.4 Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

Not applicable.

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](#).

8 Type of Storage Outside of Canada

Sensitive personal information is not being disclosed outside of Canada.

8.1 Is the sensitive personal information stored by a service provider?

Not applicable.

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

Not applicable.

8.3 Describe the contractual terms in place (if applicable).

Not applicable.

8.4 Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Not applicable.

8.5 Which enterprise service are you accessing?

Not applicable.

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

Not applicable.

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

Not applicable.

8.8 Describe the privacy risks for disclosure outside of Canada.

Not applicable.

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?

Yes, the Explorance Blue SaaS platform is used, which is a web-based survey and feedback system hosted in Canada.



15 (1)(l)

Based on the controls in place, the residual privacy risk related to security is assessed as low.

9.1 Do you or will you have a [security assessment](#) to help you ensure the initiative meets the reasonable security requirements of [FOIPPA section 30](#)?

No, a security assessment will not be conducted. Explorance Blue has completed its own Privacy Impact Assessment (v2.0, March 2025), which includes a detailed security review.

CMTN's IT department has reviewed this assessment and confirms it aligns with security best practices and FOIPPA requirements. CMTN's IT department will continue to monitor vendor security posture as part of contract renewal and ongoing oversight.

9.2 Does your initiative involve generative artificial intelligence or machine learning?

No, this initiative does not involve generative artificial intelligence or machine learning.

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

Yes, digital records are stored on government servers (College Servers) and all physical records are stored in College owned offices with role-based access.

9.4 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
Access to survey information is restricted to employees whose roles require it.	Yes
Employees who require standing or recurring access to survey information must receive approval from the appropriate Manager or Director.	Yes
Audit logs are used to monitor access to files, including identifying who accessed the file and when.	Yes

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](#) 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?

As the survey is designed to collect anonymous feedback, the initiative does not rely on the accuracy of personal identifiers or individual-level data. Instead, accuracy and completeness are supported through the design and administration of the survey instrument.

Survey questions are structured to be clear, concise, and relevant to the purpose of the initiative, reducing the likelihood of misunderstanding or incomplete responses. Participation is voluntary, and respondents may choose to answer only those questions they are comfortable with.

Where open-ended responses are provided, the information reflects the views and perspectives of the participant and is used for qualitative analysis rather than factual verification. As such, the initiative does not require validation of personal information in the traditional sense.

11. 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.

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

No. As the survey is anonymous and does not collect directly identifying personal information, individual responses cannot be linked to a specific person for correction. Participants are encouraged to review their responses prior to submission to ensure accuracy.

11.2 Sometimes it is not possible to correct the personal information. [FOIPPA](#) 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?

Not applicable. As the survey is anonymous and responses cannot be linked to an identifiable individual, requests to correct or annotate records cannot be actioned or documented.

11.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, [FOIPPA](#) requires 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?

Not applicable. The survey is anonymous and does not involve the disclosure of identifiable personal information to other public bodies or third parties. As such, there are no correction notifications required.

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

No. The survey is anonymous and responses are used in aggregate form only to inform organizational improvements. The information collected is not used to make decisions that directly affect any identifiable individual.

11.5 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 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?

Not applicable.

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](#)?

No, this initiative does not involve an information sharing agreement.

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

No, this initiative does not result in a personal information bank.

13.1 Describe the type of information in the bank.

Not applicable.

13.2 Name the main ministry or agency involved.

Not applicable.

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

Not applicable.

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

Not applicable.

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
Self-identification in open-ended responses	Participants will be advised not to include identifying or sensitive information in open-text fields. Responses will be

13 (1)

Possible Risk	Response
Data breach or unauthorized disclosure	The College will follow established breach response procedures in accordance with FOIPPA, including containment, assessment, notification, and reporting where required.
Perception of lack of anonymity leading to reduced participation or biased responses	Clear communication will be provided to employees regarding the anonymous nature of the survey, how data will be used, and the safeguards in place to protect confidentiality.
Transmission of responses via email [REDACTED]	Access to the email inbox is restricted to authorized staff. Emails will be handled securely and stored in accordance with institutional records management and IT security practices.
Retention of survey data longer than necessary	Survey data will be retained only as long as necessary to fulfill the purpose of collection and will be securely disposed of in accordance with the College's records retention policies.

15 (1)(l)

Part 9 – Privacy Officer Comments

This Privacy Impact Assessment has been reviewed based on the information provided as of March 23, 2026. The initiative is designed to collect anonymous employee feedback and is authorized under section 26(c) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

The survey appropriately limits the collection of personal information by not requesting directly identifying data and by committing to aggregate reporting. However, there remains a residual risk of indirect identification, particularly through open-ended responses where employees may voluntarily disclose identifying information. This risk will be reasonably [REDACTED] of responses prior to analysis and reporting.

13 (1)

13 (1)

Subject to the mitigation measures identified in this assessment, the privacy risks associated with this initiative are considered low and manageable. This PIA is on track for approval.

If any substantive changes are made to the scope of this initiative, including changes to the type of information collected, the introduction of identifiable data elements, or the use of new technologies or service providers, this PIA must be reviewed and updated accordingly.

Part 10 – Signatures

Aman Kang		10/04/2026	22 (1)
Privacy Officer		Date	
Christina Kiriakakis		10/04/2026	
Program/Department Manager		Date	
Michael Doyle		10/04/2026	
Vice-President, Corporate Services & CFO		Date	
Dr. Laurie Waye		15/04/2026	
President & CEO		Date	

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