



Privacy Impact Assessment

Mentimeter

Centre of Learning Transformation

Tracey Woodburn, Dean Learning and
Teaching

April 29, 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	Centre of Learning Transformation		
PIA Drafter:	Tracey Woodburn, Dean Learning and Teaching Aman Kang, Director of President's Office		
Email:	twoodburn@coastmountaincollege.ca	Phone:	250.635.6511 ext. 5340

1. Description of the Initiative

Mentimeter is an online student engagement and presentation tool that allows instructors to create interactive activities for both online and in-person classes. The tool may be used for polls, short-answer questions, live presentations, real-time responses, and class discussions.

CMTN is piloting Mentimeter for one year, from November 5, 2025 to November 5, 2026. The College has not previously held institutional licences for this type of ancillary instructional application. Some instructors may have previously purchased individual licences without a completed PIA.

The pilot includes 10 instructor licences that can be assigned at one time. The Centre of Learning Transformation (COLT) department will act as the administrator and will manage licence assignment and reassign unused licences as needed. The first group of instructors will use the tool from November 5, 2025 to April 30, 2026. After that period, other College employees may apply to participate, with priority given to instructional use.

2. Scope of this PIA

This Privacy Impact Assessment (PIA) applies to the use of Mentimeter at CMTN during the one-year pilot period, for purposes related to College business.

While the primary use of Mentimeter is to support instructional activities (e.g., classroom engagement, polls, and discussions), this PIA also includes other College-related uses, such as employee engagement sessions, town halls, workshops, committee meetings, and institutional feedback activities, where the tool may be used to collect input or facilitate discussion.

Mentimeter enables two modes of participation:

- Anonymous participation (default and most common use): Participants submit responses without providing identifying information.
- Identified participation (optional): Participants may include their name or other identifiers. This feature can be enabled or required by the facilitator or instructor, depending on the purpose of the activity.

The scope of this PIA includes:

- The collection, use, and disclosure of participant responses during College-related activities
- The potential collection of personal information where identified participation is enabled
- The display of responses in real time, including the potential visibility of names or identifiable information to other participants
- The storage of engagement data (e.g., poll results, written responses, participation metrics) within the platform
- The ability for authorized users (e.g., instructors or facilitators) to download and retain reports outside of the platform
- Use across instructional and administrative contexts, where the tool supports legitimate College operations

The tool is primarily used to facilitate discussion, gather feedback, and promote engagement. In some cases, responses may be displayed on-screen during live sessions. Where identified participation is enabled, participant names or identifiers may be visible to others.

To reduce privacy risks within this scope, the following expectations are recommended:

- Anonymous participation should be the default for all uses, unless the collection of personal information is necessary and directly related to a College purpose 13 (1)
- The identified participation feature should be limited or disabled unless required
- Participants should be informed in advance if their name or identifiable responses will be visible or collected
- Facilitators should avoid encouraging the submission of sensitive personal information in open-text responses
- Retention and deletion practices should be established to ensure that session data and downloaded reports are only kept as long as necessary for the identified purpose

This PIA does not cover personal or unauthorized use of Mentimeter outside of College business activities.

3. Data or Information Elements Involved in Your Initiative:

The personal information involved in this initiative through Mentimeter is limited.

By default, participation is anonymous and no personal information is collected. Where enabled by the instructor or facilitator, participants may choose or be required to provide their name when submitting responses.

Where names are collected:

- The information is visible only to the creator of the activity (e.g., the instructor or authorized facilitator) within the platform
- Names are not visible to other participants, unless the facilitator chooses to display responses that include identifying information during a live session
- Access to this information is restricted to the account holder and is not broadly accessible across the institution

In addition to names (if enabled), the tool collects:

- Participant responses (e.g., poll selections, short answers, word clouds)
- Session interaction data (non-identifiable engagement data, unless linked to a name)

As a general practice, the collection of names should be limited to situations where it is necessary to support a defined College purpose. Anonymous participation should remain the default to minimize the collection of personal information.

3.1 Did you list personal information in question 3?

Personal information may be collected where the identified participation feature in Mentimeter is enabled. In this case, participants are required to enter their name to join a session.

As indicated in the platform notice (see image provided), participants are informed that:

- Their name will be shared with other participants, and
- Their name will be recorded alongside their responses and questions

10:30
Camera

Mentimeter

What is your name?

- This session requires participants to enter a name to join.
- Your name will be shared with other participants and recorded with your responses and questions.

Your name

Create your own Menti at [menti.com](https://www.menti.com)

By using Mentimeter you accept our [terms of use](#) and [privacy](#)

menti.com

This means that, where this feature is used, personal information is:

- Visible to the instructor/facilitator, and
- May also be visible to other participants during the session, depending on how responses are displayed

Participation in identified sessions is based on informed consent, as users are presented with a clear notice prior to entering their name. However, where name collection is required to join a session, consent should be considered conditional, and instructors/employees must ensure that the collection is reasonable and necessary for the intended purpose.

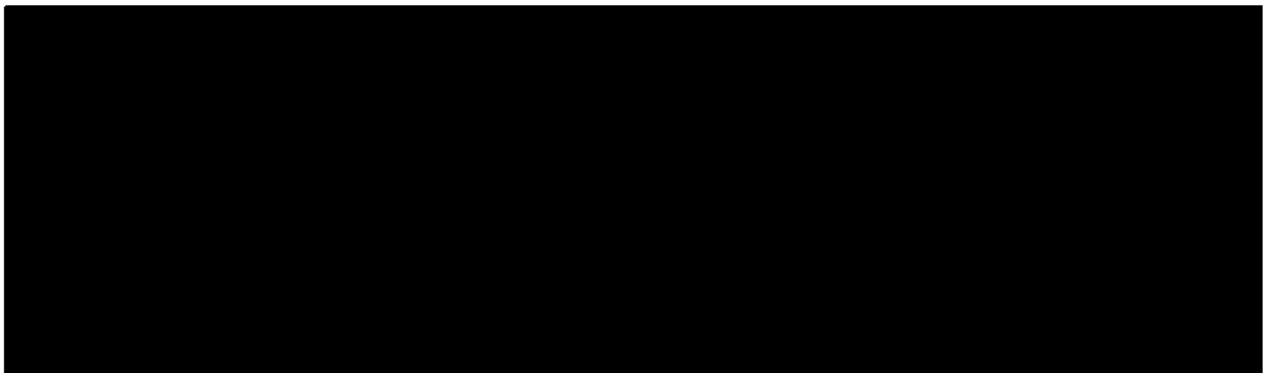
2. Reducing the Risk of Unintentionally Collecting Personal Information

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 use of Mentimeter is designed to support anonymous participation; however, there remains a risk of unintentionally collecting personal information, particularly in open-ended response formats.

The only personal information intentionally collected through this initiative is a participant's name, where the identified participation feature is enabled. There is an additional risk that participants may self-disclose personal information (e.g., names, contact details, or sensitive information) in open-text responses. As there is no character limit or content restriction within these fields, this risk cannot be fully controlled through the platform.

To reduce the risk of inadvertent collection of personal information, the following measures will be implemented:



13 (1)

These measures support minimizing the collection of personal information and align with the principle of limiting collection to what is necessary for the intended College purpose.

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.

3. 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.

Only name, used for engagement. If results are downloaded by the instructor in the form of an excel sheet. Should be save on a college approved platform. Use is very limited for now.

Movement of Personal Information Through Your Initiative		Information Collection, Use, and Disclosure	FOIPPA Authority	Other Legal Authority
Step 1	Instructor or facilitator enables the “name required” feature for a session (if applicable).	Use (configuration of tool)	Section 26 (c)	Not applicable
Step 2	Participant enters their name to join the session, after being presented with a notice.	Collection	Section 26 (c) and Section 27	Not applicable
Step 3	Name is associated with participant responses within the Mentimeter session.	Use	Section 32(a)	Not applicable
Step 4	Responses (with names, if enabled) may be displayed in real time during the session.	Use and potential Disclosure (to other participants)	Section 32(a) and Section 33 (2)(d)	Not applicable
Step 5	Session data (responses and names, if collected) is stored within Mentimeter’s system.	Use and Storage	Section 32(a) and Section 30	Service provider terms
Step 8	Personal information is retained only as long as necessary for the intended purpose and then securely deleted.	Retention and Disposal	Section 31	Not applicable

15 (1)(I)

4. 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).

While the platform provides a notice, a College collection notice should also be given (verbally or on a slide):

Collection Notice:

Personal information (such as your name, if enabled) is collected by Coast Mountain College under section 26(c) of the *Freedom of Information and Protection of Privacy Act* for the purpose of facilitating participation in College

activities. Your information may be visible to the facilitator and, in some cases, other participants. Questions can be directed to the Privacy Officer at foi@coastmountaincollege.ca.

Part 3 – Storing Personal Information

5. 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?

Yes, personal information (e.g., names, if collected) and associated responses are stored on Mentimeter's cloud infrastructure, which may be located outside of Canada (e.g., United States or European Union).

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

Personal information is stored within Mentimeter's hosted environment (cloud-based servers outside Canada). If session results are downloaded, they must be stored on a College-approved Canadian system (e.g., secure network or SharePoint).

7.3 Does your initiative involve sensitive personal information?

No, the initiative is limited to low-sensitivity personal information (e.g., names). However, there is a risk of incidental disclosure of personal or sensitive information through open-text responses.

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

No, the initiative is not intended to collect or disclose sensitive personal information. Any personal information stored outside Canada is limited and should be minimized through the use of anonymous participation.

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 intended to be disclosed or stored outside of Canada. Any personal information involved (e.g., names, if collected) is considered low sensitivity.

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

No sensitive personal information is stored. Limited personal information (e.g., names) may be stored by a third-party service provider (Mentimeter) on cloud infrastructure outside Canada.

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

Personal information (if collected) is stored within Mentimeter's cloud-based platform, which may use servers located in the United States or European Union. The information is accessible only to authorized users (e.g., instructors, facilitators) through their accounts.

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

The College is using a one-year licence agreement with Mentimeter. No enterprise or customized data residency agreement is currently in place.

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?

- Access is restricted to licensed users with College email accounts
- Role-based access (administrator assigns licences)
- Anonymous participation is the default, limiting personal information collection

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

Access to licences is managed by a designated administrator. A College-controlled tracking document (e.g., OneDrive spreadsheet) is used to record which instructors have been assigned licences. Access to Mentimeter session data is limited to the individual account holder.

8.8 Describe the privacy risks for disclosure outside of Canada.

Personal information may be subject to foreign laws and access (e.g., U.S. legislation), and there is a risk of unauthorized access or disclosure through third-party systems. There is also a risk that participants may inadvertently include personal or sensitive information in open-text responses.

These risks are mitigated by limiting the collection of personal information to names only (where necessary), using anonymous participation by default, avoiding the use of the tool for sensitive information, and ensuring that any downloaded data is stored on College-approved Canadian systems.

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, this initiative uses Mentimeter, a cloud-based digital tool. Limited administrative tracking (e.g., licence assignment) may also be maintained on College-approved systems.

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 formal security assessment is being conducted. The initiative involves low-sensitivity personal information only (e.g., names, where enabled) and relies on vendor security controls and College administrative safeguards.

Reasonable security measures include:

- Limiting access to authorized users only (licensed instructors and facilitators)
- Using anonymous participation by default
- Restricting collection to the minimum necessary information
- Ensuring any downloaded data is stored on College-approved systems

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?

No. Data collected through Mentimeter is stored on third-party cloud infrastructure outside College servers.

Where session data is downloaded, it must be stored on College-approved systems (e.g., secure network or SharePoint) with access limited to authorized staff.

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 limited to authorized users (instructors and facilitators)	Yes
Use of College email accounts for authentication	Yes
Role-based access (administrator assigns licences)	Yes
Tracking of licence assignment (e.g., OneDrive spreadsheet)	Yes
Anonymous participation to limit personal information collection	Yes
Regular review/reassignment of licences	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?

Personal information collected through Mentimeter is limited and, where enabled, consists of participant-provided names. Accuracy is ensured by collecting information directly from the individual at the time of participation. No independent verification is required, as the information is used only for real-time engagement and not for administrative decision-making.

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?

Yes. The Registrar's Office (RO) is responsible for processing requests to correct personal information.

If a request to update or correct personal information is received through this initiative or by staff involved, it will be directed to the Registrar's Office for appropriate handling in accordance with established College procedures. Staff will act in accordance with a duty of care to ensure that individuals are guided to the correct process and that no unauthorized changes are made outside of official systems.

- 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?

Yes. Requests to correct personal information will be documented and processed by the Registrar's Office (RO) in accordance with established College procedures.

- 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?

Yes, where applicable. This initiative does not involve routine disclosure of personal information. If it is determined that personal information has been disclosed (e.g., through downloaded reports shared externally), the Registrar's Office may notify the relevant party in accordance with FOIPPA requirements.

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

No. Personal information is not used to make decisions that directly affect individuals. It is used solely to support engagement and participation in instructional or College-related activities.

- 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. This initiative does not use personal information to make decisions about individuals.

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
Participants unintentionally include personal or sensitive information in open-text responses	Participants will be provided with a verbal and/or written privacy reminder not to include personal or sensitive information. Instructors and facilitators will design questions to avoid prompting such disclosures.
Identified participation (name collection) results in visibility to others during live sessions	Anonymous participation will be the default. Where names are collected, participants will be informed in advance that their name may be visible to the facilitator and, in some cases, other participants.
Unauthorized access to session data within the platform	Access is restricted to licensed users through College email accounts. Licence assignment is managed by an administrator, and access is limited to the account holder.
Storage of personal information outside of Canada	Personal information may be stored on cloud infrastructure outside Canada and subject to foreign laws. Risk is mitigated by limiting collection to names only, using anonymous participation by default, and avoiding sensitive information.

Possible Risk	Response
Downloaded reports containing personal information are stored insecurely	Instructors and facilitators will be required to store any downloaded data on College-approved systems (e.g., secure network or SharePoint) with appropriate access controls.
Retention of session data longer than necessary	Session data will only be retained as long as necessary for the intended purpose. Instructors and facilitators will be encouraged to delete data when no longer required.
Use of the tool outside of approved College purposes	Use of Mentimeter will be limited to College-related activities. Guidance will be provided to instructors and facilitators on appropriate and compliant use.

Part 9 – Privacy Officer Comments

This Privacy Impact Assessment has been reviewed based on the information provided as of April 29, 2026.

The initiative involves the use of Mentimeter to support engagement in instructional and other College-related activities. The collection of personal information is limited, with anonymous participation as the default and the optional collection of names where enabled by the instructor or facilitator.

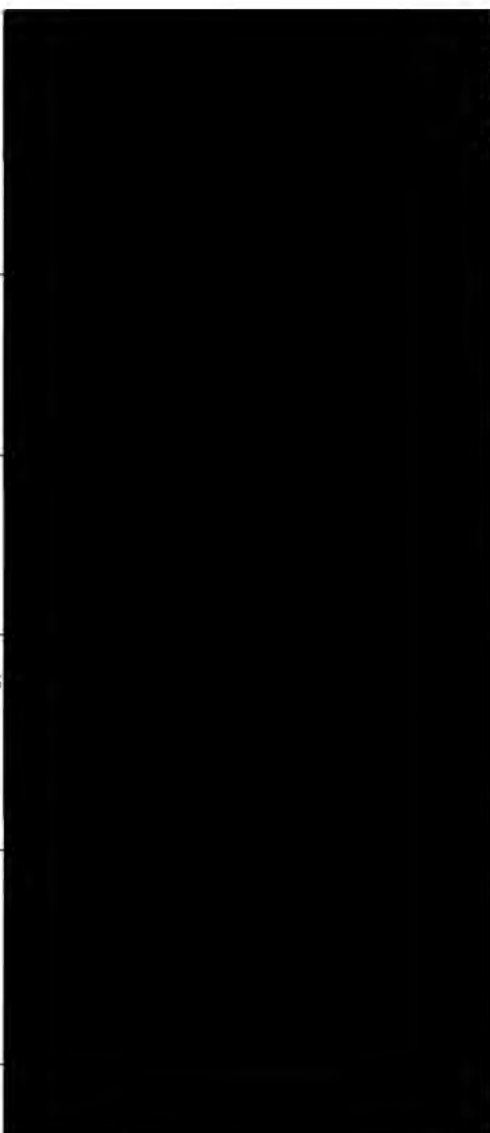
Overall, the privacy risks associated with this initiative are assessed as low, provided that the recommended mitigation measures are consistently applied. Key risks include the potential for incidental disclosure of personal or sensitive information in open-text responses, visibility of participant names during live sessions, and the storage of limited personal information on cloud infrastructure located outside of Canada.

13 (1)

Any material changes to the scope, functionality, integration with other systems, or types of personal information collected (including expanded use of identified participation or use for evaluative or decision-making purposes) will require a review and update of this PIA.

Ongoing monitoring is recommended to ensure compliance with FOIPPA, including reinforcing guidance to instructors and facilitators on appropriate use, privacy notices, and data minimization practices.

Part 10 – Signatures

Aman Kang		27/05/2026	22 (1)
Privacy Officer		Date	
Tracey Woodburn		27/05/2026	
Program/Department Manager		Date	
Tracy Boyde		01/06/2026	
Director, IT & CIO		Date	
Dr. Titi Kunkel		27/05/2026	
Vice-President, Academic, Students and International		Date	
Michael Doyle		27/05/2026	
Vice-President, Corporate Services & CFO		Date	
Dr. Laurie Waye	27/05/2026		
President & CEO	Date		

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