



Privacy Impact Assessment

Padlet

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

Padlet is an online collaboration tool that allows instructors, staff, and students to create and contribute to shared digital boards ("padlets"). Users can post text, images, links, files, and comments in real time to support engagement, brainstorming, teaching, workshops, and College-related collaboration.

CMTN will pilot Padlet for a one-year period from October 21, 2025 to October 21, 2026.

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 October 21, 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 Padlet at CMTN during the one-year pilot period, for purposes related to College business.

- Classroom engagement and learning activities
- Workshops, meetings, and events
- Brainstorming, feedback collection, and collaboration

Padlet supports:

- Anonymous participation (default option where configured)
- Identified participation (e.g., name, username, or account-based participation)

The scope includes:

- Collection and use of participant content (posts, comments, uploads)
- Potential collection of personal information (e.g., names, usernames, content submitted)
- Real-time display of content to other participants
- Storage of data within Padlet's cloud infrastructure
- Optional downloading/exporting of content by instructors and facilitators

Padlet also allows facilitators to control privacy and permissions (e.g., restricting access to specific users or requiring moderation before posting).

3. Data or Information Elements Involved in Your Initiative:

Personal information is limited and may include:

- Name or username (if enabled)
- Content submitted by users (text, files, images, comments)
- Account information (for licensed users)

By default, participation can be anonymous; however, users may self-identify through submitted content.

3.1 Did you list personal information in question 3?

Personal information may be collected through Padlet depending on how the tool is configured and used.

Personal information may be collected where:

- Participants enter a name or username when contributing to a Padlet
- Users access the platform through an account associated with their identity (e.g., College email)
- Participants self-identify within posted content, including text, images, files, or comments

All content submitted to a Padlet is visible to the facilitator and, depending on the access settings, may also be visible to other participants. As a result, even where names are not required, there is a risk that individuals may be identifiable through the content they provide.

Padlet provides users with information regarding how their data is collected and displayed through its platform notice and privacy policy. However, participants should also be informed by the College that:

- Contributions may be visible to others in the session
- Personal information should not be included unless necessary
- Anonymous participation is preferred where appropriate

The collection of personal information is limited, user-driven, and context-dependent, and should be minimized through configuration settings (e.g., enabling anonymous posting, restricting access, and using moderation where appropriate).

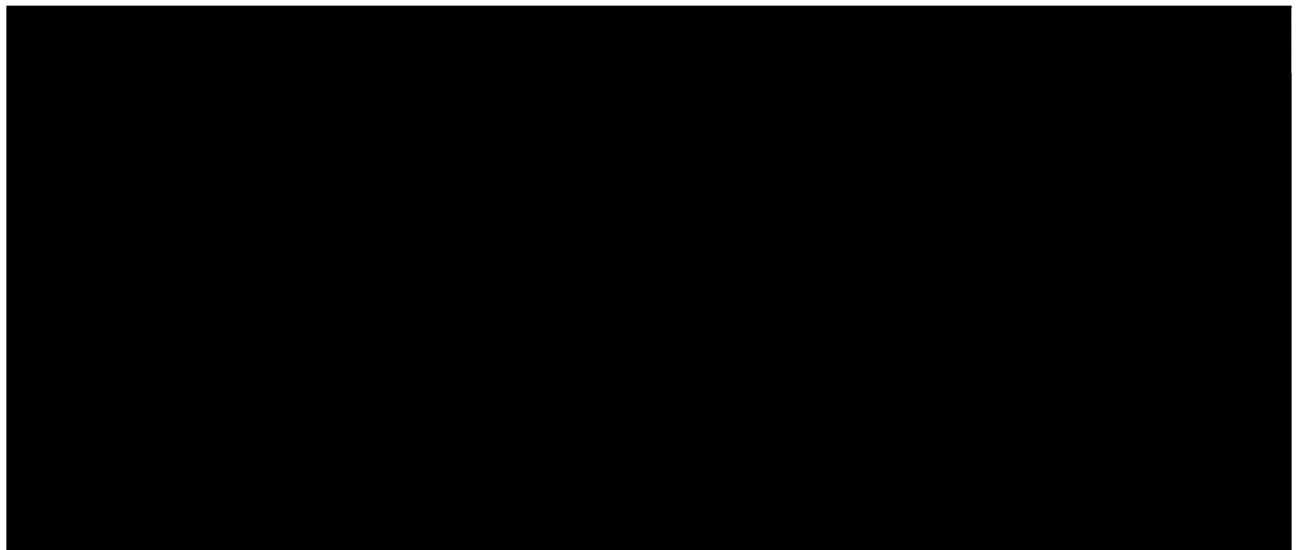
2. Reducing the Risk of Unintentionally Collecting Personal Information

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 Padlet presents a risk of unintentionally collecting personal information, particularly through user-generated content such as posts, comments, images, and file uploads.

While the initiative is intended to support engagement and collaboration, participants may self-disclose personal or sensitive information in their contributions. As content may be visible to others (depending on settings), this creates a risk of broader disclosure.

To reduce this risk, 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 a defined 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.

Movement of Personal Information Through Your Initiative		Information Collection, Use, and Disclosure	FOIPPA Authority	Other Legal Authority
Step 1	Instructor or facilitator creates a Padlet board for an instructional or College-related activity.	Use	Section 26 (c)	Not applicable
Step 2	Participant accesses the Padlet board through a link, QR code, or invitation.	Collection and Use	Section 26 (c) and Section 32(a)	Not applicable
Step 3	Participant may enter a name, username, or account information, depending on the settings used.	Collection and use	Section 26 (c) and Section 32(a)	Not applicable
Step 4	Participant submits content to the Padlet board, such as text, comments, images, links, or files. Content may include personal information if the participant self-identifies.	Collection and Use	Section 26 (c) and Section 32(a)	Not applicable
Step 5	Submitted content is displayed on the Padlet board and may be visible to the instructor, facilitator, and other participants, depending on the board settings.	Use and potential Disclosure	Section 32(a) and Section 33 (2)(d)	Not applicable
Step 6	Instructor or facilitator monitors the Padlet board and may remove content that includes personal, sensitive, inappropriate, or unrelated information.	Use	Section 32(a) and Section 30	Not applicable

Movement of Personal Information Through Your Initiative	Information Collection, Use, and Disclosure	FOIPPA Authority	Other Legal Authority
Step 10	Padlet content is deleted when no longer required for the identified College purpose.	Retention and Disposal	Section 31
Not applicable			

15 (1)(l)

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).

Padlet provides general privacy information through its platform and privacy policy; however, it does not provide a FOIPPA-compliant collection notice specific to Coast Mountain College.

As such, a College collection notice must be provided (e.g., verbally at the start of the session or included on a presentation slide):

Personal information (such as your name, if enabled, or content you choose to submit) is collected by Coast Mountain College under section 25(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, usernames, and user-generated content) may be stored outside of Canada through Padlet, including in jurisdictions such as the United States and Singapore.

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

Personal information is stored within Padlet's cloud-based platform on servers located outside of Canada. Where content is downloaded, it must be stored on College-approved Canadian systems (e.g., secure network or SharePoint).

7.3 Does your initiative involve sensitive personal information?

No, the initiative is not intended to collect sensitive personal information. Personal information is limited to low-sensitivity data (e.g., names and user-generated content). However, there is a risk of incidental disclosure if participants include sensitive information in their posts.

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

No, sensitive personal information is not intended to be collected or disclosed. 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 in this initiative is limited to low-sensitivity data (e.g., names, usernames, and user-generated content) and may be stored by Padlet on cloud-based infrastructure located outside of Canada (e.g., United States and Singapore).

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

No sensitive personal information is stored. Limited personal information may be stored by a third-party service provider (Padlet).

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 is stored within Padlet's cloud-based platform and is accessible to authorized users (e.g., instructors and participants) based on the board's access settings.

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

The College is using a one-year licence agreement. No customized data residency or enterprise agreement is 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 through Padlet privacy settings, including limited sharing links, password protection, and moderation controls. Access is further limited to authorized users (e.g., instructors and participants) and College-managed accounts where applicable.

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

Access to Padlet boards is controlled by the creator (instructor or facilitator). Licence assignment is managed by COLT. Where applicable, a College-controlled tracking document (e.g., OneDrive spreadsheet) is used to monitor licence access.

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 include personal or sensitive information in user-generated content.

These risks are mitigated by limiting the collection of personal information, using anonymous participation where possible, restricting access through platform settings, enabling moderation, 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 involves the use of Padlet, a cloud-based digital tool used to facilitate engagement and collaboration. 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 and user-generated content, where applicable) and relies on vendor security controls and College administrative safeguards.

Reasonable safeguards include:

- Limiting access to authorized users only
- Using anonymous participation where possible
- Restricting collection to the minimum necessary information
- Utilizing Padlet privacy and moderation settings
- 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 Padlet is stored on third-party cloud infrastructure outside College servers.

Where Padlet content 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/facilitators)	Yes

Use of College email accounts for access	Yes
Role-based access (administrator assigns licences)	Yes
Use of Padlet privacy settings (e.g., restricted links, passwords)	Yes
Moderation controls to review/remove content	Yes
Tracking of licence assignment (e.g., OneDrive spreadsheet)	Yes
Limiting collection through anonymous participation	Yes
Secure storage of downloaded data on College systems	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 Padlet is limited and may include participant-provided names, usernames, or user-generated content. 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 for engagement and collaboration purposes only 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, it will be directed to the Registrar's Office for appropriate handling in accordance with established College procedures. Due to the nature of the platform, correction may involve removal or deletion of content rather than amendment within the system.

- 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 shared or downloaded Padlet content), 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 posts, comments, or uploads	Participants will be provided with a verbal and/or written privacy reminder not to include personal or sensitive information. Instructors and facilitators will design activities that do not prompt such disclosures.
Content is visible to unintended participants due to broad sharing settings	Padlet boards will be configured with appropriate privacy settings (e.g., restricted access, password protection, limited sharing links).
Identifiable information is visible to other participants during collaboration	Anonymous participation will be used wherever possible. Where identification is enabled, participants will be informed in advance that their content may be visible to others.
Unauthorized access to padlets or content	Access is restricted through Padlet permissions, moderation settings, and, where applicable, College-managed accounts.
Storage of personal information outside of Canada	Personal information may be stored on servers outside Canada and subject to foreign laws. Risk is mitigated by limiting collection, avoiding sensitive information, and using anonymous participation.

Possible Risk	Response
Participants upload files or images containing personal or sensitive information	Clear guidance will be provided to avoid uploading personal or sensitive content. Instructors and facilitators will monitor and remove such content where necessary.
Inappropriate or unauthorized content remains visible	Instructors and facilitators have authority to monitor and remove content promptly. Moderation features may be enabled where appropriate.
Downloaded Padlet content is stored insecurely	Any downloaded content must be stored on College-approved systems with access limited to authorized staff.
Retention of Padlet content beyond what is necessary	Content will be deleted when no longer required for the intended purpose, in accordance with College practices.
Use of Padlet outside of approved College purposes	Use will be limited to College-related activities, with guidance 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 Padlet to support engagement and collaboration in instructional and other College-related activities. The collection of personal information is limited and primarily user-generated, with anonymous participation available.

The overall privacy risk is assessed as low to moderate, primarily due to the potential for incidental disclosure of personal or sensitive information through user-generated content, visibility of content to other participants, and the storage of data on cloud infrastructure located outside of Canada.

Any material changes to the scope, functionality, or use of the tool, including the collection of additional personal information or integration with other systems, 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.

13 (1)

Part 10 – Signatures

Aman Kang		27/05/2026	22 (1)
Privacy Officer		Date	
Tracey Woodburn		27/05/2026	
Program/Department Manager		Date	
Tracy Boyde		28/05/2026	
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.