

Privacy Impact Assessment

PIA# 23-0018 (file number will be assigned by the Privacy Office)

INSTRUCTIONS/INFORMATION:

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.

Do I have to answer all the questions?

Sections marked as “required” must have an answer. Specify *N/A (not applicable)* if appropriate. Other sections not marked mandatory should STILL be answered if the information is known. You will be contacted to answer any questions that are deemed relevant to this assessment so it’s best to be complete.

What if my initiative does not include personal information?

You still need to complete some parts of the PIA to ensure compliance with regulation. Under question “4. Elements of Information or Data”, specify “*no personal information collected*”. Sections that are marked as “*required*” still need to be answered.

What if I have questions?

If you have any questions about FOIPPA generally, you may contact the “*Privacy and Access Officer*” (privacy@tru.ca). For questions specific to this PIA, contact the “*Information Security Director*” (jcuzzola@tru.ca).

Initiative Preamble (Required)

Initiative/ Project/ Program Name:	Mentimeter Interactive live polling		
Name of TRU Department/Branch:	Bob Gaglardi SoBe Faculty		
PIA Drafter (you):	Joyce Shang		
Your Email:	jshang@tru.ca	Phone:	On Teams
Service/Vendor:			
Vendor Email:		Phone:	

Have you consulted IT Department for this Initiative/Project/Program?

_Yes_____ **No** **X** **N/A**_____

(If no, it is recommended to consult IT Department first to resolve any potential IT-related issues.)

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

Part 1 – General

1. Description of the Initiative (required)

Please provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc. We will be assessing the impacts of this initiative so please include details which help us understand its size/scale and reach.

Mentimeter.com is a website that allows users to create presentations, polls, quizzes, etc. I am seeking to use this tool as part of my teaching activities. Students and other audiences can vote and express their thoughts anonymously and Mentimeter provides live results.

2. Scope of this PIA (required)

This section should explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

This PIA covers the use of Mentimeter to seek answers to survey results. This PIA has been undertaken with the understanding that participation in these surveys will be voluntary, and users will fit under the “Audience” category as set out in Mentimeter’s Privacy Policy: [Interactive presentation software - Mentimeter](#)

The scope of this PIA is to identify personally identifiable information (PI) and to ensure that it is properly collected, used, and disclosed under FIPPA. Also, to ascertain whether the security measures in place are sufficient for the type of PIA that needs to be protected.

2-1. Is this initiative recurring in a regular interval, e.g., yearly, or biennially? (required)

I will be using this product continuously as part of my teaching and presentation activities.

3. Related Privacy Impact Assessments

No previous PIA.

4. Elements of Information or Data (required)

I will not be asking participants to provide any personal information, and will request that they not provide any personally identifying or other personal information in their responses. This is intended to be an anonymous process.

Questions put to participants using Mentimeter are mainly related to marketing topics and concepts. For example, I will ask students to choose the right concept for a given marketing example, use

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

keywords to describe their attitudes toward a given brand, express their thoughts on a marketing topic, etc.

Questions will vary, some will be in the form of a rating/scale, and others in the form of open text responses. For rating/scale, I may ask students to rank/rate brands. For open text responses, I may ask them to come up with a slogan for a brand or share their perceptions of brands.

I will not be storing any of the responses.

Participants will be asked to respond to a specific survey, and will fall under the “Audience” category of Mentimeter’s Privacy Policy:

Audience

We may process:	with the purpose to:	and the legal basis being:
Device Information	enable for you to vote/add replies to surveys and presentations and prevent abuse	contractual obligations
Contacts (email address)	enable for a User to send you the survey or presentation you have interacted with, which is optional	contractual obligations
Contacts (email address)	conduct direct marketing via email (if you have provided us your email address to receive a survey or presentation which is optional)	your consent
Cookie Information	conduct marketing activities and provide appropriate security measures, as examples, please read our full Cookie Policy for more information	legitimate interest and your consent

Mentimeter’s Cookie Policy ([Interactive presentation software - Mentimeter](#)) provides that cookies will only be used with consent:

“When you visit our websites, you have the right to have access to certain information, for example how cookies are used by us and the purpose of the cookies. **You also need to consent to our use of cookies. You consent by allowing cookies or categories of cookies in the cookie banner that appears when you visit the website.** If you do not consent to the use of cookies, it may affect your user experience and you may not get full access to all features and functions on our websites.

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

In case you have given your consent to the use of cookies, you may easily withdraw your consent and choose to block and/or delete the cookies. For more information on how to block or erase cookies, please see the “*Cookie Preferences*” section below.”

I will advise participants in the collection notice that they are not required to provide any consents to Mentimeter in order to participate in my quizzes/ surveys. If they choose to consent to cookies, they are entering into an agreement directly with Mentimeter – TRU will not be collecting this information.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

Per Mentimeter’s Privacy Policy:

“Mentimeter offers multi-regional hosting. **By default, customer data at rest is hosted in the EU. We may transfer limited data to countries outside of the EU/EEA. Such transfers are either conducted under the provisions of the European Commission’s Standard Contractual Clauses as of 4 June 2021 or in accordance with a European Commission's adequacy decision.** ”

5-1. Is a service provider(s) involved? If so, where is the provider located (e.g. Canada, U.S., or other country)? (required)

Mentimeter’s Privacy Policy provides that they do use service providers in a number of countries, including countries in the EU, the United States:

“A full list of the service providers that process our users’ data, along with details of their location, is available [here](#). Our users' privacy is of utmost importance to us, and we do everything we can to ensure that all our sub-processors have implemented appropriate safeguards to protect the personal data they process on our behalf by for example having contractual obligations in place for them to process such data in compliance with applicable data protection laws. Importantly, we only use processors to the extent necessary to enable us to provide the best services possible, and we never have and will never sell any personal data to third parties.”

Privacy Impact Assessment

PIA# 23-0018 (file number will be assigned by the Privacy Office)

6. Common or Integrated Program or Activity (required)

If you answer yes, please contact the *Privacy and Access Officer*

If you answer “yes” to <u>all</u> 3 of these questions, your initiative qualifies as “a common or integrated program or activity,” and you must comply with requirements under FOIPPA.	
1. This initiative involves a program or activity that provides a service (or services);	no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

7. Data-linking Initiative* (required)

If you answer yes, please contact *Privacy and Access Officer*

If you answer “yes” to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under FOIPPA.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no

8. Provide a diagram, flowchart, and/or table that shows how your initiative will collect, use, and/or disclose personal information.

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. If the authority comes from other legislation, please identify the applicable act(s) or regulation(s), including specific section references.

Personal Information Flow Table.

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Faculty member creates a free account and generates a survey designed to gather anonymous responses.	N/A	N/A
2	Survey is displayed to group and a code is assigned to allow participants to access the survey as “audience” members.	N/A	N/A
3	Participants engage with the survey by providing responses to questions. Mentimeter collects device information for the purpose of enabling users to vote / add replies to surveys and presentations and to prevent abuse.	Collection	26(c)
4	Responses are displayed as they appear and are visible to the group. While I will be advising participants not to provide personal information in their response, there is some chance PI will be included in these responses.	Use	32(a), s.32(b)

9. Risk Mitigation Table (required)

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please identify the likelihood (rare, unlikely, possible, likely, almost certain) and the degree of impact (insignificant, minor, moderate, major, catastrophic).

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

Risk Mitigation Table					
	Risk	Mitigation Strategy	Likelihood	Impact	Exposure
1	s.13				
2					
3					

Privacy Impact Assessment

PIA# 23-0018 (file number will be assigned by the Privacy Office)



s.13

→ Exposure rating of *high* or *critical* is of concern. Please contact Director, Information Security to discuss possible solutions.

s.13

Risk Exposure Matrix

Risk Exposure Matrix		IMPACT				
		Insignificant	Minor	Moderate	Major	Catastrophic
	Almost Certain	Low	Medium	High	Critical	Critical
	Likely	Low	Medium	High	Critical	Critical
	Possible	Insignificant	Low	Medium	High	High
	Unlikely	Insignificant	Low	Low	Medium	Medium
	Rare	Insignificant	Insignificant	Insignificant	Low	Low

10. Collection Notice

If your initiative collects personal information directly from any individuals, you must ensure that all individuals involved are told the following:

1. The purpose for which the information is being collected
2. The legal authority for collecting it, and
3. The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

Please contact *Privacy and Access Officer* for assistance on this.

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

Standard Collection Notice Statement

This should be presented to participants at or before the time of collection (participation in survey):

“Thompson Rivers University (TRU) collects, uses, discloses and retains personal information in compliance with the BC Freedom of Information and Protection of Privacy Act (FIPPA). TRU is using Mentimeter to conduct surveys. Participation is completely optional.

If you choose to participate, Mentimeter will collect basic device information to enable you to participate in the survey and to prevent abuse. Your responses will be displayed to the group once you submit them using Mentimeter – **please do not include personal information or information that would identify you, these surveys are intended to be anonymous.** This collection is permitted under s.26(c) of FIPPA. Mentimeter may ask for your consent to use cookies, or for your email address – you are under no obligation to accept, and if you choose to accept you are entering into a separate agreement with Mentimeter.

For further information about how your personal information is being collected, please contact:

Dr. Joyce Shang, Chair & Associate Professor, Department of Marketing Bob Gaglardi School of Business and Economics. Email: jshang@tru.ca . Phone: 778 471 8465.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

- Physical access to Mentimeter's office premises is restricted to staff individually and on a need to have basis.
- Physical access to where the Services are performed shall log physical access related events such as date, time, proximity card-id, door-id, access denied, or access granted. Entries are monitored by security cameras.

12. Please describe the technical security measures related to the initiative (if applicable).

- separation/segregation of duties to prevent error and fraud by ensuring that at least two individuals are responsible for separate parts of any task so that no single role or account can access, modify or use data without authorization or detection.
- log important events, which enable us to monitor and follow up on suspicious or malicious activity.

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

- Mentimeter maintains the principle of least privilege (PoLP), meaning that every module (such as a process, a user, or a program, depending on the subject) must only have access to the information and resources that are necessary for its legitimate purpose.
- Losses, theft, damages, tampering, or other incidents related to IT-assets that compromise security must be reported as soon as possible to the Security Officer.
- Data encrypted at rest: Mentimeter uses strong encryption of all Data "at-rest", including AES 256-bit encryption for Customer data stored in Mentimeter's production environment.
- Data encrypted in transit: We use standard TLS >=1.2, ie. Encryption of data "in-transit, and are rated A+ by 3rd party vendor, SSL Labs. Privacy and protection of user data are of the highest importance to us and we both have technical and operational support in place to ensure this. We also leverage all protection through <https://heroku.com/policy/security>.
- service provider's physical infrastructure is hosted and managed within Heroku's and Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.
- Mentimeter stores Data on AWS (an Amazon service <https://aws.amazon.com/compliance/>) servers. We logically separate customer data in order to ensure integrity and confidentiality. Mentimeter utilizes ISO 27001, SOC2 and FISMA certified data centers managed by Amazon.
- Amazon's data center operations have been accredited under:
 - ISO 27001
 - SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
 - PCI Level 1
 - FISMA Moderate
- Mentimeter has multi-regional hosting and have configured our data to be stored in the regions; EU-West-1 EU (Ireland) and US-East-1, North Virginia, US.
- Sarbanes-Oxley (SOX) - As a publicly-traded company in the United States, salesforce.com is audited annually and remains in compliance with the Sarbanes-Oxley (SOX) Act of 2002.

13. Does your branch/department rely on any security policies? (required)

- Mentimeter Security Policy: [Interactive presentation software - Mentimeter](#)
- Mentimeter Privacy Policy: [Interactive presentation software - Mentimeter](#)
- Mentimeter Acceptable Use Policy: [Acceptable Use Policy - Mentimeter](#)
- Mentimeter Cookie Policy: [Interactive presentation software - Mentimeter](#)
- Mentimeter Third Party Code of Conduct: [Interactive presentation software - Mentimeter](#)
- Amazon security is covered here (<https://aws.amazon.com/security/>)
- Heroku security is covered here (<https://www.heroku.com/policy/security>)

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information. (required)

- I will be the only one administering the survey. Results will be displayed as they are submitted, but these will not be saved. I may make notes of the responses, and will ensure these do not contain any personally identifying information.

15. Please describe how you track who has access to the personal information. (required)

- I will be the only one with access and will not be sharing any personal information with other individuals.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's personal information updated or corrected? If it is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated.

N/A, basic device information collected by Mentimeter. Responses collected by me with instructions not to provide personally identifying information.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain (required).

No

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate, complete and up-to-date.

For example: check to see that the information was obtained from a reputable source such as another government agency.

N/A

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please contact Manager, Information Services.

N/A.

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

For example: your initiative involves a regular exchange of personal information (both collection and disclosure) with other government(s) and/or other agencies in order to provide services to your clients.

No.

Please check this box if the related Information Sharing Agreement (ISA) is attached. **If you require assistance completing an ISA, please contact Legal Services.**

☐

21. Does the program involve access to personal information for research or statistical purposes? If yes, please explain.

For example: your initiative involves disclosing information to PhD students so that they can conduct research.

No.

Please check this box if the related Research Agreement (RA) is attached. **If you require assistance completing an RA, please contact Privacy and Access Officer.**

☐

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

No.

Part 6 – Canada's Anti-Spam Legislation (CASL) Compliance

23. Please confirm if you plan on emailing, texting, or instant messaging as part of your project. (required)

No.

24. If you answered yes to question 23, please explain the purpose(s) of the messages you intend to send. Be sure to note any messages involving promotional activities, including links to the TRU

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

public website or other Internet site(s). The purpose(s) you provide will help us identify whether the overall communication is a commercial electronic message (CEM¹)?

N/A

25. If your communication message does fall under CEM rules, you must comply with the unsubscribe mechanism and identification requirements under CASL. Please confirm your method of unsubscribe mechanism that must be processed within 10 business days and how you will meet the identification requirements?

N/A

26. If you do meet the definition of CEM, please confirm that you have a records retention schedule that will ensure that consent communications, both paper and electronic, are stored appropriately and retained for three years after the last communication?

N/A.

Part 7 – Common Vulnerabilities and Exposures (CVE) Assessment

(This section to be completed by the **Information Security Office**). If your initiative involves the transmission of personal data between TRU and the vendor, or from the vendor to 3rd parties, then TRU may ask for the name of the software used to determine if there are applicable CVEs.

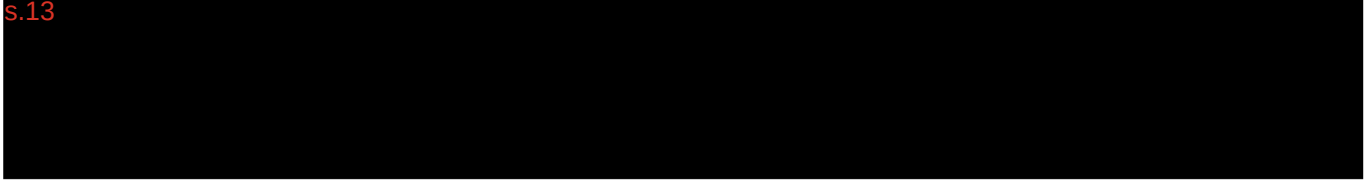
¹ If your initiative or program sends commercial electronic messages (CEMs), such as emails promoting a product or service, you must comply with CASL's requirements to: (1) obtain consent, (2) provide identification information, and (3) include an unsubscribe mechanism in each message. Please note that an electronic message that contains a request for express consent is also considered to be a CEM under CASL.

Privacy Impact Assessment

PIA# 23-0018 *(file number will be assigned by the Privacy Office)*

Part 8a – Information Security Director Comments

s.13

A large black rectangular redaction box covering the majority of the content in the 'Part 8a' section.

John Cuzzola

s.22

A black rectangular redaction box covering the signature of John Cuzzola.

2023-11-28

Information Security Director

Signature

Date

Part 8b – Privacy Officer Comments

Privacy and Access Officer

Signature

Date

Privacy Impact Assessment

PIA# 23-0018 (file number will be assigned by the Privacy Office)

Part 9 – Program Area Signatures

Program/Department Manager	Signature	Date
John Cuzzola		2023-11-28
Information Security Director	Signature	Date
Senior Manager, Program Area/Division	Signature	Date
General Manager	Signature	Date
General Manager	Signature	Date

A Final Copy of this PIA (with all signatures) shall be kept on record by the program area responsible for this project. The signed original record will be retained by the FOI and Privacy Office. ***If you have any questions about FOIPPA generally, you may contact the “Privacy and Access Officer” (privacy@tru.ca). For questions specific to this PIA, contact the “Information Security Director” (jcuzzola@tru.ca).***