Privacy Impact Assessment (PIA) for Humanitix

Before you start

- This Privacy Impact Assessment (PIA) form is used by VCC to assess whether a new initiative, or proposed significant change to an existing initiative, meets the privacy protection requirements of the B.C. *Freedom of Information and Protection of Privacy Act.* FIPPA's protection of privacy requirements. A PIA is a legislative requirement (FIPPA s. 69(5.3)) and mandatory before implementing an initiative.
- You/Your refers to the individual responsible for drafting this PIA, who should be an individual from the relevant department or program area with sufficient knowledge to do so. The PIA must be signed by the role within the program area with the appropriate position to hold accountability for this initiative.
- Please include references to other documents when applicable, but do not insert or embed any documents to/in this assessment form.

- Please review the initial assessment questions and contact the Privacy Office at privacyandfoi@vcc.ca before you begin the form, if you have not already. See more guidance about the PIA process, including the supplementary Guidance Document, on the myVCC Privacy website.

PART 1: GENERAL INFORMATION

PIA file number: 2025-010

Initiative title:	Humanitix ticketing platform
VCC Department / Program Area:	Centre for Teaching, Learning, and Research
Link to VCC initiative website:	
Link to vendor website:	https://humanitix.com/ca
Link to vendor privacy policy:	https://static.humanitix.com/pdfs/privacy_and_cookie_policy.pdf https://static.humanitix.com/pdfs/organiser_terms.pdf
Your name and title:	Fionna Chong, Instructional Associate, Center for Teaching Learning, and Research
Your work phone and email:	fchong@vcc.ca
Initiative Lead name and title:	Tannis Morgan, AVP, Academic Innovation
Initiative Lead phone and email:	tmorgan@vcc.ca

General information about the PIA:

Is this initiative a data-linking program under FIPPA? See the definition in Schedule 1 of FIPPA. If this PIA addresses a data-linking program, the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Is this initiative a common or integrated program or activity? See the definition of Schedule 1 of FIPPA. Under section FIPPA 69 (5.4), the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No

Does this initiative involve a regular or systematic exchange of personal information between organizations? If yes, this initiative may require an [Information Sharing Agreement](#).	No
Related PIAs, if any:	

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved, and when or how long your initiative runs. If this is a change to an existing initiative, please also explain the change and the benefits of the change.

Humanitix is a SaaS product that provides a self-service ticketing platform for event organisers. Humanitix is a not-for-profit funded by the Atlassian Foundation and a range of other philanthropists. Humanitix does not charge event hosts any fees for free events and charges low fees for any ticketed events, with reduced rates for non-profits and schools. Humanitix is a "100% for-purpose entity and a registered charity that donates 100% of profits to social impact projects." Humanitix includes options for event hosts to host paid events (payment is offered through a connected Stripe account) and functions to communicate with attendees through Email Tools.

VCC's CTLR occasionally organizes events that are open to the public and require online registration by attendees. An example is the yearly VCC Teaching, Learning, and Research Symposium (ongoing). These events are available to educators outside of VCC. The events are free-of-cost to participants, and do not require participants to share sensitive information.

CTLR intends to use Humanitix as a ticketing/registration platform for these free, public events, in order to collect attendees' contact information and details relevant to participating in a particular event, and to use that contact information to communicate with attendees about any necessary information related to that event. Humanitix is a free and simple platform and provides CTLR with all registration functions that they require.

Humanitix allows hosts to create events that participants can register for without needing to create an account. The host then can communicate with attendees through the platform or export this information about attendees to a .csv file and use this for communications.

CTLR exports the attendees' information and holds this on an MS Teams site used for the coordination of events like the VCC TLR Symposium. CTLR uses this information only for the purposes of contacting the participants to provide the weblink to the MS Teams meeting, if the event is online, and to request feedback after the event. CTLR does not use this information to contact participants for any marketing purposes or about future events; attendees must register for each event each time.

2. What is the scope of the PIA?

Your initiative might be part of a larger initiative or might be rolled out in phases. What part of the initiative is covered by this PIA? (An initiative may require multiple PIAs.) What is out of scope of this PIA?

This PIA covers the collection, use, and disclosure of personal information in CTLR's use of Humanitix, specifically for free events and for events that do not require the collection of sensitive personal information.

CTLR does not intend to use Humanitix's Email Tools function or any function related to payment and both are outside the scope of this PIA. CTLR's use of the M365 environment for the management of event attendee information once exported from Humanitix is also outside the scope of this PIA.

This PIA could cover other departments/program area's use of Humanitix if the use is within the scope of this PIA as detailed above.

3. What are the data or information elements involved in your initiative?

*Please list **all** the elements of information or data that you might **collect, use, disclose, store, or access** as part of your initiative (**including but not limited to personal information**). Please:*

- *include where the information is coming from (e.g. collected directly from users, pulled from existing databases, etc.);*
- *group different categories of people together (e.g. students, employees, alumni, etc.) if your initiative involves large quantities of information or datasets.*

From CTLR (event host): Information is collected directly at the creation of the account and will only include business contact information (VCC email), username, password.

Event information: CTLR provides details about the nature of the event when they create the event within Humanitix.

From Attendees: Personal information is collected directly from attendees at registration. Attendees do not need to create an account to use Humanitix.

- Participant registration information:
  - First Name, Last Name, Email, Mobile (CTLR does not use – can be made optional through Humanitix's advanced settings)
- CTLR Event Registration Questions ("Conditional Check Out Questions" in Humanitix):
  - What institution/organization are you with?
  - What is your role/job?
  - When you register for this VCC event, you must agree to follow the code of conduct.
  - Please share how you heard about the symposium (optional). (text)
- Attendees may opt-in to receive marketing emails from Humanitix.

CTLR does not need to request any information about participants' accommodations; CTLR offers ASL interpretation by default at events.

Device information, Cookies and Analytics: Humanitix collects standard device information from users' devices and web browsers when using the platform (IP address, device ID, app ID), and cookies and non-personal information for third-party analytics when users use Humanitix. Users may choose to only use strictly necessary cookies.

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. This includes, but is not limited to:

- *Names, home addresses, emails, and telephone numbers of the individual or their guardians and family members (this includes student names and emails!);*
- *Images of an individual;*
- *Identifying number (e.g. student number, employee number, health care number);*
- *An individual's personal views or opinions, or anyone else's opinions about an individual;*
- *Educational, medical, medical, criminal, financial, or employment history.*

Yes. (Most information will likely be business contact information, but not necessarily)

- If yes, are all of the personal information elements **necessary** for your initiative?
  - Yes, then skip question 4 and continue to Part 2

4. If you answered "no" to question 3.1: How will VCC reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in a privacy breach or other privacy incident. After you answer this question, submit this PIA to the Privacy Office. You do not need to complete the rest of the PIA template.

N/A

PART 2: COLLECTION, USE, AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use, and disclosure flow

Describe the information flow of your initiative in the chart below. The table explains the movement of personal information throughout your initiative (column 1) and identifies each time personal information is collected, used, or disclosed (column 2) and under which corresponding FIPPA authority (column 3).

- ***Collection:*** *Describe the steps in collecting personal information from individuals by VCC and/or the vendor (clarify which party is collecting the information).*
- ***Use:*** *How does VCC and/or the vendor use personal information (clarify which party is using the information)?*
- ***Disclosure****: When, if ever, would VCC and/or the vendor provide the personal information to an internal or external third party that does not normally have access to the personal information?*

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FIPPA authority or other legal authority**	**Specify any potential risks**
CTLR creates host account (only VCC email; no PI) and creates event. Event is public (searchable on Humanitix) or the link can be distributed.	N/A	N/A	
Participants register online by providing the required personal information.	Collection	26(c)	
CTLR exports the attendees list and report from Humanitix and holds the .csv file in CTLR's Teams to use for communication with attendees (sending weblink or other event information; request for feedback).	Disclosure	33(2)(d)	Access to personal information of registrants: only event organizers have access to attendees' list information downloaded from Humanitix.
CTLR deletes events with attendees' information following the end of the event and any requests for feedback.	Disposal		

6. Collection Notice and Consent

6. 1 Collection Notice

If you are collecting personal information directly from an individual the information is about, FIPPA s. 27(2) requires that you provide a collection notice (except in limited circumstances). If your vendor is *collecting personal information on behalf of VCC, the vendor must also provide a collection notice. FIPPA requires that you notify the individual of:*

- *the legal authority,*
- *purpose(s) and use of their personal information (including any third party disclosures), and*
- *contact information or someone who can answer questions about the collection and use.*

Review the template collection notice below and update as applicable.

Collection notice template (complete or replace with your notice):

Your personal information is collected under the authority of s. 26(c) of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). This information will be used for the purpose of registering you for this event and contacting you solely about this event and for feedback after the event. Questions about the collection of this information may be directed to the VCC Centre for Teaching, Learning, and Research at s. 15(1)(l)

The collection notice will be posted in the description of each event on Humanitix.

Any other user of Humanitix must replace the contact information with an appropriate contact for that event's organizer.

6. 2 Consent

If you are obtaining consent for the use or disclosure of personal information (indicated by the FIPPA authorities you used in Question 5), add any consent language here.

N/A

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

Yes

- If no, skip to Part 5.

8. If you answered yes to Question 7: Where are you storing the personal information involved in your initiative?

s. 15(1)(l)

9. Does your initiative involve sensitive personal information that will be stored outside of Canada?

Sensitive personal information is not defined in FIPPA. Personal information may be considered sensitive depending on the type of information and the context in which it is collected, used, disclosed, or stored. Common sensitive personal information could include: personal health or medical information; financial information; criminal records; disciplinary or complaint history; unique government issued identifiers (passport number, driver's license, personal health number, SIN); racial or ethnic origins; sexual orientation; religious or philosophical beliefs; etc. Please see the above link for more guidance or consult with VCC's Privacy Office.

No

- If yes, go to question 10
- If no, skip ahead to Part 5

10. If you answered "yes" to Question 9: Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public (FIPPA section 33(2)(f))?

N/A

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section **only if you answered yes to Question 9: you are disclosing sensitive personal information to be stored outside of Canada**. This section will require consultation with a representative from IT Services.

11. Is the sensitive personal information stored by a service provider?

[Answer: Yes or No]

- If yes, fill in the table below (add more rows if necessary) and then go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. If you answered “no” to Question 11: Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

This should include reference to the location and method of storing the personal information (e.g. location of data: Atlanta, GA, USA. Method of storing data in Atlanta, GA, USA: e.g. specify that the information is stored in a data storage facility).

[Answer]

13. Does the contract you rely on include privacy-related terms?

[Answer: Yes or No]

- If yes, describe the contractual measures related to your initiative.
  - [Answer]
- Is VCC’s Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services appended to the initiative’s contract? [Answer: Yes or No]

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

Describe technical, security, administrative and/or policy measures that are in place to protect against the unauthorized collection, use, disclosure or storage of sensitive personal information, including preventing or managing access to sensitive personal information. If your initiative uses a cloud-based service provider, also consider controls at each layer: software, platform, and infrastructure.

See Section 2 of the Guidance Document for examples of these measures and consult with IT Services to answer this question.

[Answer]

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

Describe how you will know if the sensitive personal information is accessed, including access by service providers (e.g. logging access to data). Consult with IT Services to answer this question.

[Answer]

16. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence, and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary. See Section 3 of the Guidance Document for examples of privacy risks and risk responses and more guidance for how to complete this table, or see the Guidance on Disclosures Outside of Canada.

Privacy risk	**Impact to individuals (low, medium, high)**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**

Outcome of Part 4

The outcome of Part 4 will be a **risk-based decision made by the role designated accountable for the initiative on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 16.

Is the outcome to proceed with the initiative? [Answer: Yes or No]

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5, you will share information about the privacy aspect 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 and/or your vendor need to make sure that the personal information is safely secured in both physical and technical environments.

17. Does your initiative involve digital tools, databases, or information systems?

Yes

- If yes: Are these digital tools, databases, or information systems new to VCC?
  - Yes

17.1 If you answered "yes" to Question 17: Do you or will you have a security assessment to ensure the initiative meets the security requirements of FIPPA s. 30?

Consult with VCC IT Services to complete a security assessment that will ensure that the initiative has reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or disposal of personal information.

No

- If no, continue to question 18.

18. What technical and physical security do you have in place to protect personal information?

Describe <u>where the records, whether digital or physical, for your initiative are stored</u> (e.g., on your organization's LAN, on your computer desktop, in a filing cabinet, etc.) and the technical and/or physical security measures in place to protect those records. (Please consult the policies for any software/cloud services/etc. but please do not just copy and paste).

- *<u>Technical security</u> measures include secure passwords, encryption, firewalls, etc.*
- *<u>Physical security</u> measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.*

Humanitix:

- Humanitix is hosted on Amazon Web Services and offers SOC 1, SOC 2, and SOC 3 compliance.

s. 15(1)(l) [redacted]

- Humanitix supports email and password-based authentication for hosts. Event attendees do not maintain a logged-in account.

s. 15(1)(l) [redacted]

VCC: CTLR uses a password-protected account as the event host that will only be accessible by CTLR event organizers. s. 15(1)(l) [redacted]

19. Controlling and tracking access

Please respond to each strategy that describes how you or your vendor limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. To *effectively protect privacy, access to personal information should be limited to authorized employees who need the information to do their jobs. Insert your own strategies if needed.*

Strategy	
We only allow employees in certain roles access to information:	VCC: Yes, only event organizers Humanitix: Yes
Employees that need standing or recurring access to personal information must be approved by their managerial lead:	VCC: No (CTLR determines who is the event organizer and that information is only available within CTLR) Humanitix: Yes.
We use audit logs to see who accesses a file and when:	Humanitix: No information available.
Describe any additional controls:	Access to CTLR's Humanitix account is exclusive to CTLR event organizers and only these individuals (usually a small group of CTLR members and a representative or two from other departments such as the Library) can access Humanitix account or exported data. All will be employees of VCC with access to Teams.

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.

20. How will you make sure that the personal information is accurate and complete?

FIPPA s. 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete. For example: verifying information with the person it is about prior to recording it.

Attendees are responsible for ensuring the accuracy of the personal information they provide at registration. Attendees must register for each unique event.

21. Requests for correction

FIPPA s. 29 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.

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

Attendees are able to correct their personal information through the "Manage Order" option in their order confirmation email, or attendees can contact the event host (CTLR) to correct their personal information if needed.

21.2 Sometimes it's not possible to correct the personal information. FIPPA s. 29 requires that you make a note on the record about the request for correction if you are not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA s. 29 requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A – This initiative does not involve disclosing personal information to third parties.

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

No.

23. If you answered "yes" to Question 22: Do you have a records retention schedule in place related to personal information used to make a decision?

FIPPA s. 31 requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. Please consult the VCC Records Retention Schedule to assist you in answering this question.

N/A, but events in Humanitix should be deleted as soon as the event has finished and attendee lists are no longer needed. Attendees can also request deletion of their personal information from Humanitix (under the Privacy Policy).

PART 7: PERSONAL INFORMATION BANKS

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

A personal information bank is a collection of personal information that is organized and retrievable by the name of the individual or an identifying number, symbol or other identifier.

No.

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

25. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response / mitigation strategies
Attendee lists containing personal information are kept permanently in Humanitix and/or in Teams.	CTLR (or any Humanitix user) must delete events' attendee lists when no longer needed for the purpose for which they were collected (communication and follow-up after the specific event).
VCC event host uses Humanitix for paid events or asks attendees for sensitive personal information.	These uses are out of scope of this PIA. VCC users should use a different platform for paid events or this PIA can be revised.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to the Privacy Office for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer	Caralee Maloney	Caralee Maloney Digitally signed by Caralee Maloney Date: 2025.11.18 08:50:00 -08'00'	Nov 18, 2025

Program Area Signatures

The PIA must be signed by a role that is able to hold accountability for a PIA, proportionate to the sensitivity of personal information and/or the risks of the initiative. This signature confirms that this PIA accurately documents data elements and information flow at the time of signing. If there are any changes to the overall initiative, including the way personal information is collected, used, stored, or disclosed, the program area will contact Privacy and, if necessary, complete a PIA update.

Program Area Comments:

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Tannis Morgan, AVP, Academic Innovation	Tannis Morgan Digitally signed by Tannis Morgan Date: 2025.11.19 10:32:40 -08'00'	Nov 19, 2025
Contact Responsible for Systems Maintenance and/or Security	Elmer Wansink	Elmer Wansink Digitally signed by Elmer Wansink Date: 2025.11.17 17:35:13 -08'00'	Nov 17, 2025