Privacy Impact Assessment (PIA) for

LeaderFactor: Psychological Safety Training

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: #2025-012

Initiative title:	LeaderFactor – Psychological Safety Training
VCC Department / Program Area:	People Services
Link to VCC initiative website:	n/a
Link to vendor website:	https://leaderfactor.com
Link to vendor privacy policy:	https://www.leaderfactor.com/terms/privacy-policy-app
Your name and title:	Catherine North, Organizational and People Development Advisor
Your work phone and email:	cnorth@vcc.ca 604-871-7155
Initiative Lead name and title:	Catherine North, Organizational and People Development Advisor Elaine Pedersen, Director Recruitment & People Development
Initiative Lead phone and email:	epedersen@vcc.ca 604-871-7019

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?

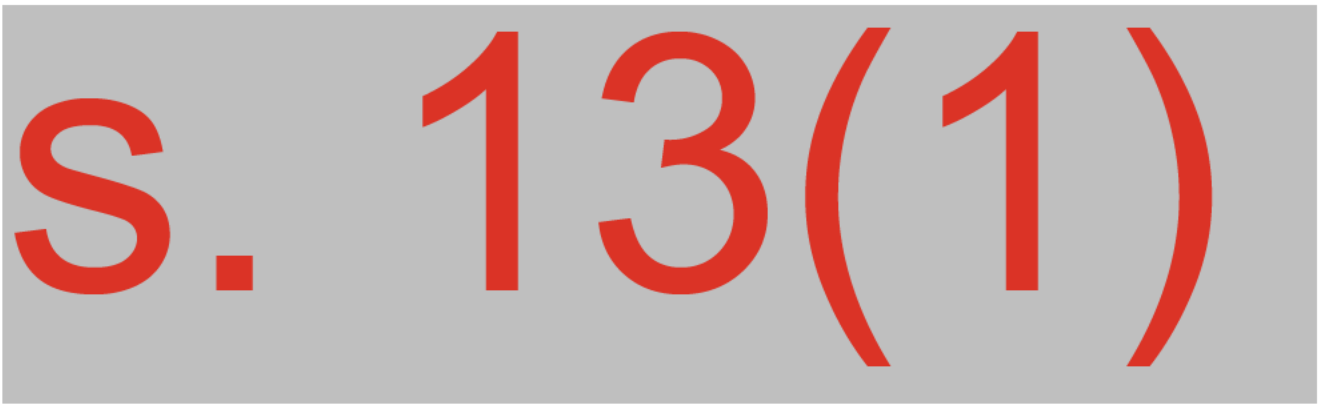
Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved, and when or how long your initiative runs. If this is a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

What are we doing?

Vancouver Community College (VCC) is committed to fostering a workplace culture that prioritizes mental health, well-being, and psychological safety. As outlined in the VCC Mental Health and Well-being Framework (2022–2026) and the Strategic Innovation Plan, the College is taking proactive steps to build a respectful, inclusive, and empowering environment for all employees.

Why is this important?

Psychological safety is the belief that one can speak up, share ideas, and express concerns without fear of negative consequences. Psychological Safety is foundational to employee well-being and organizational success. It supports open communication, innovation, and collaboration, while reducing turnover and workplace conflict.



Why LeaderFactor?

To meet the growing need for awareness, training, and support, VCC is launching Psychological Safety Training with LeaderFactor, a globally recognized leader in psychological safety training and organizational culture transformation.

After extensive research, LeaderFactor was selected for its evidence-based framework, practical tools, and alignment with VCC's values—at a cost that fits within our budget.

LeaderFactor is the creator of The 4 Stages of Psychological Safety™, a widely adopted model that helps organizations build inclusive, high-performing cultures. Their training programs are designed to help individuals and teams progress through four key stages:

1. Inclusion Safety – Feeling accepted and included
2. Learner Safety – Feeling safe to ask questions and make mistakes
3. Contributor Safety – Feeling safe to contribute ideas and work
4. Challenger Safety – Feeling safe to challenge the status quo

LeaderFactor offers licensing options and facilitator training, enabling VCC to scale the program internally.

By implementing Psychological Safety training with LeaderFactor, we aim to:

- Equip employees and leaders with the behavioural skills to foster psychological safety
- Promote employee well-being through increased awareness, shared language, supportive practices, and accountability

As VCC navigates budget constraints and potential staffing changes, investing in psychological safety is both a strategic and compassionate choice. It supports employee retention, reduces recruitment and training costs, and enhances overall performance by encouraging creativity, discretionary effort, and innovation.

Through this initiative, VCC reaffirms its commitment to creating a workplace where every employee feels safe, respected, and empowered to thrive.

How does it work?

LeaderFactor's Psychological Safety Training Program is built around the 4 Stages of Psychological Safety™, a model developed by Dr. Timothy R. Clark. The program is designed to help organizations foster a culture where individuals feel safe to be themselves, contribute, and challenge the status quo without fear of negative consequences.

The program framework is based on the 4 Stages of Psychological Safety™

1. Inclusion Safety – Feeling accepted and included as a valued member of the team
2. Learner Safety – Feeling safe to ask questions, experiment, and make mistakes
3. Contributor Safety – Feeling empowered to contribute meaningfully
4. Challenger Safety – Feeling safe to challenge the status quo without fear of retribution

LeaderFactor offers multiple formats:

- Cohort Workshops (virtual or in-person): 2–4 hour sessions for up to 25 participants
- Online Courses: Self-paced learning for flexible access
- Licensing Options: For organizations to scale the training internally

VCC is interested in the licensing option so VCC can provide workshops internally.

Each workshop includes:

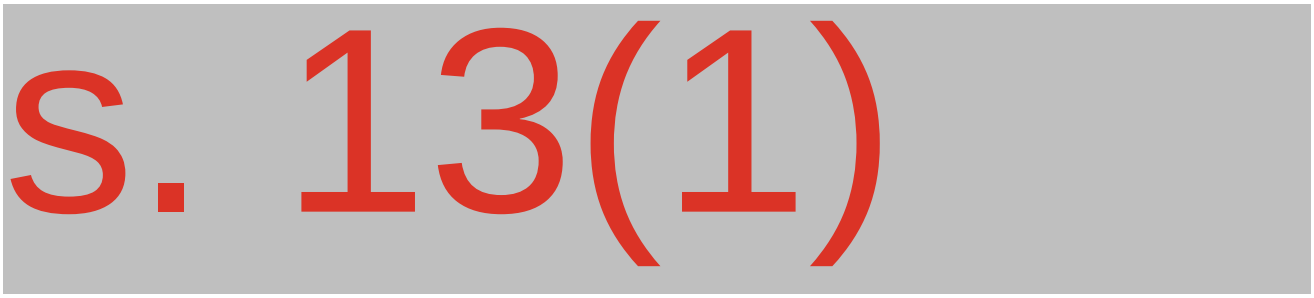
- Discovery-Based Learning: Interactive sessions exploring culture, vulnerability, and psychological safety.
- The Ladder of Vulnerability™: A self-assessment tool to understand personal and team dynamics.
- Digital Workbook: For guided reflection and action planning.
- Action Plan Debrief: Participants create a personalized plan to apply what they've learned.

Through the participants' engagement with the platform throughout the workshop, LeaderFactor calculates a "PSindex" score as a team assessment. This score is aggregated from all of the assessment responses. Individual participants are not identified by their responses. Participants in the team see how they score as a group as part of the workshop, but each participant's own use of the LeaderFactor platform is their own workbook and used for their own reference for sustained learning, but LeaderFactor will not use or access the individual workbook responses and plans otherwise.

LeaderFactor provides the following support:

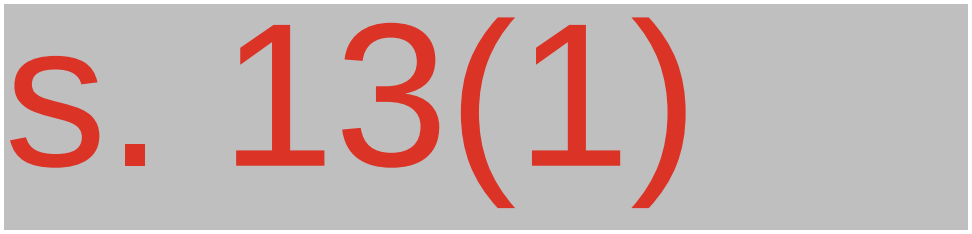
- Facilitator training for internal leaders
- Tools and technology to embed the 4 Stages into organizational culture
- Ongoing support for measuring and improving psychological safety

Who is involved?



When will it happen?

The estimated timeline is below:



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 within the **initial implementation phase** of VCC's Psychological Safety Training Initiative in partnership with LeaderFactor. This phase involves:

- The **use of LeaderFactor's digital tools and resources**, such as the 4 Stages of Psychological Safety™ framework, the Ladder of Vulnerability™ self-assessment, and digital workbooks.
- The **collection and use of participant feedback** data for the purpose of evaluating training effectiveness and informing future phases of the initiative.
- Any **data sharing or storage arrangements** between VCC and LeaderFactor related to training participation, assessments, or other support services.

This phase is focused on **awareness-building, skill development, and leadership training** to foster psychologically safe environments across the College. There is not anticipated to be any change in collection, use, or disclosure of personal information in any later use of LeaderFactor by People Services.

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.*

As part of VCC's implementation of psychological safety training with LeaderFactor, the following types of information may be collected, used, disclosed, stored, or accessed:

1. Participant Information (Employees)

Collected directly from users/participants during online registration or through use.

- Full name
- Work email address
- Workshop feedback or evaluation forms
- Passwords, password hints
- Device and usage information: IP address and/or browser and device characteristics, operating system, language preferences, location, etc.

Group: VCC employees

2. Training Interaction Data

Collected from participants through LeaderFactor's digital platform or tools during training delivery.

- Engagement metrics (e.g., time spent in modules, participation in activities)
- Responses to reflection questions or exercises
    - Questions in platform are directly related to learning material and may ask the participant in a workshop to apply learning material to their unique situations.
- Progress tracking through training modules

- Digital workbook entries (if stored online)
- Feedback (including comments)

Group: VCC employees participating in training

3. Aggregated and Anonymized Data

Generated by LeaderFactor or VCC People Services for reporting and evaluation purposes.

- Training completion rates
- Aggregate scores from assessments (used to calculate PSindex score)
- Themes or trends from feedback

Group: All training participants (aggregated)

Data Sources

Directly from participants via registration forms, assessments, and feedback tools

- LeaderFactor's training platform (if used)

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 (collection of names & work emails, personal reflections and opinions)

- If yes, are all of the personal information elements **necessary** for your initiative?

  Yes

  - 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**
VCC/LeaderFactor collects participants' name, work email to register users with VCC accounts on online platform.	Collection	26(c)	Low risk of misdirected collection (e.g., incorrect email entry. Mitigation: validation at point of collection. VCC will not permit the option of using third party (Google, Facebook) account.
Participants engage with the learning modules (including workbook entries, reflection responses, etc.) through the digital platform, as part of a team workshop. Only the participant has access to review their entries, responses, etc.	Collection	26(c)	Risk of over-collection of personal reflections: VCC should remind participants not to provide sensitive personal information (information would not be accessed by LeaderFactor but would be retained).
LeaderFactor platform uses aggregated data from all the team's assessment responses	Use	n/a	

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
to calculate the team's PSIndex score (no personal information involved in scoring).			
People Services only accesses participants' workshop progress/completion in LeaderFactor platform and records completion (for SOFI accounting purposes only).	Use	32(a)	
People Services collects and uses anonymized feedback and aggregated results to assess program effectiveness. People Services may reach out to participants for additional feedback.	Collection Use	26(e) 32(a)	Low. Mitigation: aggregate data before reporting.
LeaderFactor platform collects, anonymizes, and uses anonymized and aggregated feedback for service/workshop evaluation and improvements. People Services may provide feedback to LeaderFactor outside platform (no personal information involved).	Collection Use	26(e) 32(a)	

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:

Your personal information is collected under the authority of s. 26(c) and s. 26(e) of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). This information will be used to:

- facilitate account creation and logon process
- provide feedback to VCC on your experience
- evaluate and improve effectiveness of LeaderFactor experience
- facilitate your training and learning through LeaderFactor's program delivery and assess your progress and/or completion of the workshop.

Questions about the collection of this information may be directed to:

- Catherine North, Organizational and People Development Advisor cnorth@vcc.ca
- Elaine Pedersen, Director, Recruitment and People Development epedersen@vcc.ca

The collection notice will be posted on the **LeaderFactor digital platform at the point of registration and login**, ensuring participants are notified before providing their name, work email, or engaging with training tools.

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?

Be specific about the location where the personal information is stored (e.g. which state(s) or country/countries).

LeaderFactor uses **Amazon Web Services (AWS)** and/or Microsoft Azure data centers in the **United States** 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 (see Privacy Office comments)

- 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?

N/A

- 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)?

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.

YES

- If yes, go to question 19. If you have or will complete a security assessment during the development of your initiative, you do not need to answer the question about technical security.
- If no, continue to question 18.

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

Describe where the records, whether digital or physical, for your initiative are stored (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).

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

N/A - IT Services completing a security assessment.

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:	**YES**
Employees that need standing or recurring access to personal information must be approved by their managerial lead:	**YES**
We use audit logs to see who accesses a file and when:	**YES**
Describe any additional controls:	s. 15(1)(l)

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.

Participant details (name/email) verified at registration. Feeback and reflections are provided directly by participants and participants are responsible for verifying the accuracy of that information. Aggregated responses reviewed before finalization.

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?

Yes: Participants may request corrections through VCC People Services. Corrections are logged, and LeaderFactor notified if data resides in their system.

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?

Records within LeaderFactor cannot be annotated but People Services can document any requests for corrections.

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 - Personal information will not be disclosed to third parties through this initiative. VCC does not use some features and user information will not be disclosed to "Other Users" in public areas of Sites, including communications and viewing profiles (#3 in Privacy Policy).

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

No: assessment/evaluation is only for the user's personal learning. LeaderFactor provides a PSIndex score for the team based on aggregated data and not an individual, and neither the participant's interaction with the platform or the PSIndex score will not be used by VCC to make a decision about any individual. VCC People Services only tracks participants' progress and completion of training for SOFI accounting purposes only (no decisions are made about the individual).

- If no, skip ahead to Part 7

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?

N/A (see Risk response for account retention information)

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. Data is not stored in a way that creates a searchable personal information bank (it is used for training evaluation and aggregated reporting)

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
Perception of surveillance or monitoring of individual reflections.	Communicate that only aggregated/anonymous data will be used. LeaderFactor will remove any feedback items that include personally identifiable details or personal information.
Data breach at service provider.	s. 15(1)(l) Contractual protections (vendor signs PPS)
Employee reluctance to participate due to privacy concerns.	Transparent collection notice, emphasize voluntary sharing of personal reflections.
Cross-border storage subject to US legal access requests. (e.g., Patriot Act).	Limit data collected to low-sensitivity fields, contractual protections, data minimization. Employees should be reminded not to disclose sensitive personal information.
Retention of user accounts and user information	LeaderFactor keeps participants' information only while LeaderFactor is running their program or their company's subscription. When an account is closed, LeaderFactor removes the data from their active systems. (Backups and logs may be retained for a short period to meet security and legal reasons). • After training: by default, accounts stay active only while the customer (VCC)'s program/subscription is active. VCC can request that accounts be deactivated or deleted.

Possible risk	Response / mitigation strategies
	• s. 13(1)

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

The Privacy Office can sign off on this PIA based on the above and these additional notes from the vendor and People Services, with the understanding that this initiative does not involve sensitive personal information and employees will not be expected to disclose sensitive personal information. The vendor has confirmed:

- Vendor does not collect any data from public databases, marketing partners, or other outside sources (e.g. social media profile information) for this initiative and user information will not be disclosed to any other users (#3 in Privacy Policy does not apply to VCC's use).
- Questions/prompts/activities within the LeaderFactor training do not ask for the disclosure of any sensitive personal information. Employees involved in training should be reminded not to disclose sensitive personal information about themselves or others (e.g. health or medical information; ethnicity; sexuality; religious or political beliefs; specific details of complaints; accusations against others).
- All open-text feedback is aggregated and does not tie to a specific user. At times, users may respond with details that may incidentally identify them or others (i.e. "my boss Sarah…"); LeaderFactor will remove any personal information in feedback items prior to presenting it during training.

VCC People Services has confirmed that no individual assessment results will be shared with People Services or used to make any decisions that affect individual employees, and People Services does not have any access to any employees' individual reflections/quiz scores/other input from participating. LeaderFactor provides the "PSindex" score based on aggregated data from the team participating in the workshop. People Services will remind participants not to disclose their or others' sensitive personal information, as above.

There are no anticipated changes to the personal information involved in this initiative, but this PIA should be reviewed and updated if there are any significant changes or People Services finds there are aspects of LeaderFactor's platform that use personal information that were not captured in this PIA, including the collection of sensitive personal information.

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 08:47:05 -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	Catherine North Organizational & People Development Advisor	Catherine North Digitally signed by Catherine North Date: 2025.11.25 13:47:20 -08'00'	Nov 25, 2025
Contact Responsible for Systems Maintenance and/or Security	Elmer Wansink	Elmer Wansink Digitally signed by Elmer Wansink Date: 2025.11.17 17:36:04 -08'00'	Nov 17, 2025