Privacy Impact Assessment (PIA) for FootfallCam + Bookable Academic Space Occupancy

Before you start 1

PART 1: GENERAL INFORMATION 2

PART 2: COLLECTION, USE, AND DISCLOSURE 10

PART 3: STORING PERSONAL INFORMATION 12

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 12

PART 5: SECURITY OF PERSONAL INFORMATION 12

PART 6: ACCURACY, CORRECTION AND RETENTION 14

PART 7: PERSONAL INFORMATION BANKS 15

PART 8: ADDITIONAL RISKS 16

PART 9: SIGNATURES 18

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: #2025-014

Initiative title:	Footfall Cam + Bookable Academic Space Occupancy
VCC Department / Program Area:	IT Services; VP Administration
Link to VCC initiative website:	n/a
Link to vendor website:	https://www.footfallcam.com/
Link to vendor privacy policy:	n/a
Your name and title:	Mary Corbett, Privacy Coordinator
Your work phone and email:	marcorbett@vcc.ca
Initiative Lead name and title:	Elmer Wansink, Associate VP IT & CIO Ian Humphreys, VP Administration & International Development
Initiative Lead phone and email:	ewansink@vcc.ca / ihumphreys@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: 2025-014-1 (Addendum – Library FootfallCam)	

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.

This initiative concerns VCC IT Services and the VP Administration and International Development (VP Admin)'s use of FootfallCam people-counting systems to collect data about the current utilization of bookable academic spaces across VCC's two campuses that will assist with current and future campus planning and space allocation and optimization. This PIA considers how personal information is involved in the initiative, and other potential privacy risks and mitigation strategies for using this kind of system.

Objective: The purpose of the initiative is to gather data about the number of individuals (based on counts of individuals entering and exiting) utilizing bookable academic spaces at both of VCC's campuses, and to compare this against existing room booking data, which will allow VCC to track and analyze resource usage to inform strategic decisions, justify budgets, improve efficiency and optimize resources for campus planning. IT Services and the VP Admin are the leads of this initiative and determined that a people-counting system would be the best method of collecting this data; other methods did not actually capture the number of individuals utilizing a space (EMS room booking data; keycard access data, as rooms are unlocked by Security staff when booked for classes), and only indicated that rooms were booked or intended to be used.

VCC's use of FootfallCams began with IT Services' need to determine the occupancy of computer labs and understand when students were using computer labs and needed IT support in 2023. IT Services selected Keverest Technologies as the vendor to support this initiative, and selected FootfallCam as a people-counting system as the best option to collect and analyze this data. The Library also started to use FootfallCam at this time; this initiative is assessed in PIA 2025-014-1.

The VP Admin determined that the use of FootfallCam could be expanded in order to provide data about the VCC community's utilization of bookable academic spaces. IT Services and the VP Admin have determined that this data is necessary for planning for VCC's current and future campus, as it will assist with creating a population plan for VCC's new buildings and assist with further plans for space allocation in new buildings. VCC now works directly with FootfallCam (Vendor). It is an operational requirement for VCC to optimize the use of its spaces and to plan accurately for future buildings or space needs.

VCC is currently building the new Building C at the Broadway campus, and room occupancy data from Building A and B will assist with plans for relocating people and spaces into the new Building C and provide data about space that may be needed in an additional Broadway campus building, especially to accommodate Building A and the plan to eventually remove Building A.

The data from this initiative will also support redevelopment at the Downtown campus and better utilization of space at the Downtown campus s. 13(1)

IT Services started to install FootfallCam devices at the Broadway and Downtown campuses in September 2025. Cameras were temporarily disabled on October 23, 2025, pending the completion of the Privacy Impact Assessment.

The information in this PIA is taken from FootfallCam documentation and VCC contracts with Keverest Technologies and FootfallCam, and the Privacy Office's discussions and communications with VCC VP Admin, VP IT & CIO, and Manager, Safety & Security.

Duration of Initiative: IT Services and the VCC Library employed FootfallCam for people-counting prior to this initiative, for collecting data on the number of visitors to computer labs and to the Library

locations (Library's use is ongoing; see PIA 2025-014-1). This initiative began in September 2025, with the installation of devices at the Broadway and Downtown campuses.

The initiative is intended to run until a point after Building C is completed and programs and people are relocated to Building C s. 13(1) Data from Buildings A and B at the Broadway campus will provide useful data about the movement into the new building and the residual use of space in Buildings A and B; data about remaining use of Building A space and Downtown buildings will provide key data about the capacity needed to be built for in a future Broadway campus building. Devices will be removed over time if it is determined that data is not useful or no longer needed for the initiative.

Initiative Participants: IT Services; VP Admin; Keverest Technologies; and FootfallCam (Vendor)

Responsibilities:

- Vendor is responsible for installing and configuring the Devices and maintaining and monitoring the security of Devices.
    - Devices are installed in partnership with X10 Technologies
- IT Services creates custom reports, VP Admin uses custom reports, and reviews security of Devices.
- IT Services and VP Admin review and determine locations for installation of Devices.

Systems:

FootfallCam People Counter as the people-counting system utilized for this initiative. VCC specifically uses the FootfallCam 3D Pro2 (Device); these are managed and data is accessed through the use of the FootfallCam Analytics Manager V9 (Platform) on the FootfallCam Cloud Server.

Footfall Cloud Server: The Footfall Cloud Server (Server) consists of four major components:

- FootfallCam Analytics Manager V9 (Platform): the web-based platform that allows user to view and generate analytics report, manage sites and devices, and manage access controls and other features.
- FootfallCam Database Engine: stores configuration data, user access data, and log data for the Platform
- Real Time Data Engine: a collection of services that uses Apache Technologies to communicate, collect, process, and aggregate event-driven data from FootfallCam Devices via Websocket protocol and output information to Druid Database.
- Druid Database: A storage medium for Real Time Data Engine to perform read/write operation with highest efficiency and speed possible. FootfallCam also uses this to create an end point that allows the Platform to access, manage, and present the data in the dashboard.

Devices: Each FootfallCam Device features a 160 degree lens and a 2X 5 MP camera (a standard surveillance camera with two 5-megapixel sensors).[1] The Devices identify the presence of an individual by immediately processing the camera's live feed into a 3D depth map and then analyzing that to count the number of individuals present and only store and transmit the data related to the "people count"

[1] FootfallCam 3D Pro2 Specs: https://www.footfallcam.com/Content/data/documents/Download-Page/Spec-Sheet/FootfallCam-3D-Pro2-%282025-edition%29-Datasheet.pdf

(number entering or exiting) for each Device's location. This data is securely transmitted to the Server via HTTPS.

These Devices utilize 3D counting rather than analysis of the video feed itself. Each FootfallCam Device uses the 3D depth map generated from its dual stereoscopic lens to count with high accuracy. The 3D depth map is comprised of grey pixels and contains information relating to the distance of the surfaces of scene objects from a viewpoint. 3D image processing occurs within the Device, where it produces a count of individuals. Low-resolution videos are used for calibration and verification.[2] The Device recognizes and analyzes the height of shape to recognize the individual as one person to count. The default minimum counting height is 1.3 metres. Devices are positioned to view from above and generally do not view individuals' facial features because of this positioning, but it may be possible if individuals look up or are seated or positioned in other ways in the Device's field of view.

Any data collected for further use by the Device is non-visual and is all processed on the Device; any personal information is removed through processing on the Device and only the aggregated data in text format of the people count, location, and time is transmitted from each Device to the Server. The Device does not by default store or transmit any personal information.

VCC's Devices only employ the "Counting Data" option (in/out counting at entrances). Other counting module add-ons must be enabled and VCC is not using any other modules (e.g. Wi-Fi/Bluetooth data counting). This counting data only counts the number of individuals entering and exiting a space's defined doorway.

s. 15(1)(l)

Platform: The FootfallCam Analytics Manager V9 (Platform) is the SaaS platform that is used for configuring and managing Devices, receiving and analyzing data transmitted from the Devices, and generating reports from the data. The Platform is administered by the Vendor and Devices are configured through the Platform by the Vendor. VCC can access reporting data including the in/out counts, location of Devices, and time only on the Platform. The Platform can also be accessed through a mobile app.

- *Live View Mode:* The Platform allows administrators to view a Device's live feed remotely, in order to determine that the cameras are configured properly, to troubleshoot, or to verify the accuracy of the Device's people-counting. The frame rate is 25 fps and the live stream displays at 1027x780 to reduce bandwidth sent to the FootfallCam database for verification purpose. Platform administrators have the option of recording video from the live feed to be used to confirm the accuracy of the data from the Footfall system. Recordings may be up to 30 minutes and are held only on the Device. s. 21(1) 21

  VCC employees do not have access to the Live View Mode (live feed) in the Platform; this is only used for calibration by the Vendor, during set up and then only to calibrate/test accuracy if VCC notices any errors or issues during use.

[2] https://www.footfallcam.com/Home/Faq#Cat_1-General_Questions

Additional features: The Device offers additional modules or features that VCC and its Vendor are not employing, including: Wi-Fi Data Collection; heat mapping; demographic analysis (when used through different systems and different Device configuration); profiling unique visitors (within last 15 minutes); path tracking; customer engagement; behaviour categorization; automatic staff exclusion. FootfallCam is originally designed for the purpose of tracking and analyzing the behaviour of customers in retail spaces and so most features do not apply to and will not be utilized in VCC's initiative.

Retention: Data (of people counts, not video) will be collected and store in two levels for a specific period of time before it is deleted.[3]

	Device Level (Store in hardware)	Server Level
Raw Data (Counting data – Ins and Outs)	7 days (regardless online or offline)	Per Device: 90 days Per Site: 90 days Per Area: 90 days
Minutes Data	7 days (regardless online or offline)	1-minute Data: 90 days
Hourly Data (Aggregated)	30 days	Per Site: Permanent Per Area: Permanent
Daily Data (Aggregated)	-	Per Site: Permanent Per Area: Permanent

Any videos created by the Vendor during calibration (one-time only, when devices are set up) are retained on the Platform for 30 days before automatic destruction.

Installation: Devices will be installed to count individuals entering and exiting "bookable academic spaces," including: general use classrooms, some labs (when not dedicated spaces), Learning Centre, computer labs, and multi-purpose spaces like meeting rooms (only if used as academic spaces). Devices will not be installed in any dedicated academic spaces (e.g. auto service; heavy mechanical; biology-only labs) because those spaces can only be booked by the applicable department. Devices will also not be installed in any other non-academic spaces (e.g. prayer rooms).

As of October 2025, VCC has installed s. 15(1)(l) Devices at the Broadway campus and s. 15(1)(at the Downtown campus. IT Services and the VP Admin are committed to reviewing all locations of installed Devices and confirming that the information and data they collect are necessary and directly related to this initiative and ensuring this is true for any Devices installed in the future. **s. 15(1)(l)**

VCC intends to install Devices to collect data about all bookable academic spaces in all current buildings in both campuses. s. 15(1)(l) Devices are connected and powered via ethernet (POE).

s. 15(1)(l)

[3] https://www.footfallcam.com/people-counting/knowledge-base/about-the-product/#duration-of-date-collected-store-in-device

Placement: Devices are installed on the ceiling, to view individuals from above, and placed primarily in doorways, to count the number of individuals entering and exiting through that doorway. At times, this may capture some areas of bookable spaces

The field of view of the Devices does sometimes include other areas of classrooms, such as lockers in classroom entryways or desks, if only able to be installed not in the doorway but farther into the classroom. This depends on the mounting height of the Device; mounted at 3.5 m, the Device views about 5.25 m in width.[4] Some Devices may be placed farther into the hallway but are calibrated only to view the doorway and collect entrance/exit data, and not that of passersby.

It is the Vendor's responsibility to ensure that Devices are capturing the entrance/exit (doorways) and to adjust/configure the Device to ensure that the Device will provide accurate data. Devices have a wide field of view that cannot be reduced. If Devices cannot be placed in a way that only captures the required information (i.e. number of individuals entering or exiting a room), the Devices should not be installed.

Operational Hours: Devices are configured to only count and transmit data during the operating hours defined for the site or individual Device. VCC's Devices collect only during College operating hours.[5]

Reports: VCC creates reports using PowerBI based on data collected from FootfallCam Devices and Platform and data from VCC's EMS Room Bookings system.

VCC is able to access counts of entrances and exits of individuals, location (room number associated with Device) and time on the Platform's Dashboard and other Reporting features, and can manually export this data. VCC also receives daily reports from the Vendor detailing individuals in and out of rooms only during College opening hours, with specifically the following:

- Location, e.g. 01 BWY
- Room Number, e.g. RM 1227-B
- Date & Time Ending, e.g. 10/19/2022 11:00 AM
- Coming/Ins, e.g. 16
- Going/Outs, e.g. 0[6]

Reports can be generated based on the time aggregations of minutely (15-minute aggregations), hourly, daily, weekly, and monthly, with a defined date range or by month. The Data Aggregation level can be by Site or by Counter (specific Device identified by its specific room number). VCC collects the hourly aggregation.

IT Services only uses data from the EMS room booking system to indicate whether a room was booked at the time (booked/not booked). Reports overlay this value onto data from FootfallCam to compare whether a room was in use (number of individuals in or out) to whether the room was booked in the EMS system (intended to be occupied in that time). The reports can also compared the total number of

[4] https://www.footfallcam.com/Industries/IndependentRetailersFAQs

[5] Operating hours are the same as listed for Broadway campus: https://www.vcc.ca/about/college-information/contact-us/broadway-campus/ and Downtown campus: https://www.vcc.ca/about/college-information/contact-us/downtown-campus/

[6] Source: Keverest GSA74700 / Compliance Table (FootfallCam) with Final Requirements

hours booked to the total number of hours that rooms were used on a higher level. The Vendor has no access to EMS data.

Reports are only received and used by VP Admin to identify when bookable academic spaces are occupied, to what extent, and if this occurs when rooms are booked. This data will help inform future planning for VCC and to understand how many academic spaces are needed in future buildings; the needs of types of spaces and times for academic bookings; how space may be distributed in the future across buildings; and even what kind of buildings VCC will need to build to support VCC's need for bookable academic spaces. Data may assist in understanding VCC's space allocation needs, for numbers and sizes of rooms; additional space needs like break-out rooms and whether they are actually used when booked; or in supporting other space and scheduling optimization initiatives (e.g. booking space for hybrid classes, to ensure that space is being used at all times).

Reports are only accessed by IT Services (creators) and VP Admin. Data will not be used to make any decisions that affect individuals, or be used in any way that would follow up on an individual's behaviour or on class attendance (e.g. questioning an employee about a room booking where no one showed up) -- the collected data will only help to reveal where space is needed and how bookable academic spaces are utilized.

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 for VCC's use of the FootfallCam people-counting system within the initiative to collect and analyze data about the uses and occupancy of VCC bookable academic spaces (e.g. classrooms or other multi-purpose bookable spaces, but not dedicated labs or meeting rooms, or other non-academic spaces).

Other uses of FootfallCam fall outside the scope of this PIA and are assessed separately, excluding technical and security specifications of the FootfallCam system unless different. This includes the Library's use of FootfallCams to gather aggregated data about counts of visitors to both the Downtown and Broadway Libraries.

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.*

- Live video feed of individuals entering or exiting space (collected directly from VCC employees; students; community members)
- Temporarily-retained recordings generated from live feed for accuracy auditing/calibration
- Aggregated data of people count of entrances and exits (number of individuals), location (Building and room number of Device), and time (during open hours; reported by hour)
    - Transmitted to Footfall Cloud Server and accessed through the Platform's dashboard.
- Room booking data received from EMS system (value of room booked/not booked only)
- User/log-in credentials for IT Services access; FTP server information
- Floor plan of sites (where Devices installed)

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 .

There is limited personal information involved in this initiative due to the function of the Devices. Personal information includes:

- Live video feed of individuals entering/exiting space
- Potential: Any recording of live feed (created for calibration/accuracy testing by Vendor and temporarily retained)
- Potential: Data reflecting small numbers of individuals (0, 1) in relation to room bookings – information could become identifiable.

- 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 column 4 if there are any specific potential risks related to each step. Change the information flow and add more rows as necessary. The red text below is an example – input the steps and relevant authorities to reflect your initiative's flow.

For the most common FIPPA authority references to assist with completing this chart, please see Section 1 of the Guidance Document, or consult the full text of Part 3 of FIPPA.

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**
Devices temporarily collect live video feed to convert to data that is used to count unique individuals entering/exiting space.	Collection	s. 26(c)	Device will record data for any number of recognized individuals; Footfall will provide reports of 0 or 1 individual entering/exiting.
Vendor makes temporary recordings of live feed (Live View Mode) for troubleshooting, configuration, or verifying accuracy of	Collection Use	s. 26(c) s. 32(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
count. Automatic deletion of recordings after 30 days.	Disposal	s. 31	

s. 15(1)(l)

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.*

Collection Notice:

VCC is using the FootfallCam people-counting system to gather aggregated data about the number of individuals who enter and exit classrooms and other bookable academic spaces for the purpose of campus planning and space optimization. FootfallCam immediately processes video data and removes personal information on the local device. Your personal information is collected under the authority of s. 26(c) of FIPPA and is not retained by the device. Personal information may only be temporarily retained in FootfallCam's server in the event that FootfallCam/VCC IT Services create a recording to audit a FootfallCam device's counting accuracy, and any recording will be destroyed after that use. Your personal information will not be used or retained for any other purpose. Questions about the collection of your information can be directed to the Privacy Office at privacyandfoi@vcc.ca.

The collection notice will be posted online, on IT Services' website, with an additional FAQ about how the system works. A communication (either email or internal news post) will direct VCC employees and students to the notification and information.

6. 2 Consent

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 – but only any temporary recordings made from the Devices' live feed for calibration/accuracy testing by the Vendor.

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

The FootfallCam servers are located either in Germany, the UK, or Malaysia. Privacy Office did not receive any confirmation of which location.

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 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

[Questions 11-16 removed – not applicable to this initiative]

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 (confirmed by IT Services).

- 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.

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 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:	VCC: Yes – only certain roles in IT Services are approved to access Platform and only the user with administrative privileges on client side can add, modify or delete the user accounts (not Vendor). Vendor: Yes – based on privileges and role[7]
Employees that need standing or recurring access to personal information must be approved by their managerial lead:	Vendor: Yes VCC: Yes
We use audit logs to see who accesses a file and when:	Yes: s. 15(1)(l) [redacted]
Describe any additional controls:	VCC does not have access to the Live Feed or set-up for Devices. VCC s. 15(1)(l) [redacted]

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.

Personal information is collected directly from the individual (collected by Device's camera) and immediately processed into a 3D depth map on the Device, which is analyzed and produces a count of individuals without retaining any visual data, including individuals' personal information.

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.

[7] https://www.footfallcam.com/Content/data/documents/Download-Page/Policy/FootfallCam-Data-Privacy-Policy.pdf

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

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

N/A - Personal information is only momentarily collected to be converted to data and cannot be corrected.

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 – Personal information will not be disclosed to a third party as part of this initiative.

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

No. Data is being collected only to gather information about current usages of space and to plan for developing new buildings and allocating space in the future. There is the potential for data to be combined with other data and result in personal information (especially with relation to EMS data – e.g. 1 individual present when room booked by 1 individual would be identifiable) but this is not the intention or within the scope of this initiative, and data will not be used to support any other use or decisions.

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 – See Question 1 for Device/Platform 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.

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
Vendor inappropriately accesses personal information through Devices' live feeds and uses or discloses it for unauthorized purposes.	• Contractual privacy protections (Privacy Protection Schedule signed with VCC) and Vendor's access controls and employment agreements. • After set-up, Vendor should only access live feeds at the request of VCC for accuracy testing/calibration as needed.
Vendor could create recordings of Devices' live feeds.	• Vendor employment agreements and role-based access • Vendor should not access the live feed without VCC indicating that there may be an issue with counting accuracy or the Device. • Vendor signed Privacy Protection Schedule as part of contractual obligations.
s. 15(1)(l)	s. 15(1)(l)
Requests for access to personal information by individual, College, or third party.	• Vendor signed Privacy Protection Schedule and would need to confirm that there are no recordings responsive to a request. Personal information from Devices otherwise not stored and would not be responsive to a request, and EMS data used in this initiative does not include any personal information. • Access to information requests follow regular FIPPA procedures (including law enforcement, People Services, etc.).

Possible risk	Response / mitigation strategies
Vendor could utilize new or additional features available on Devices without notifying VCC (e.g. Wi-Fi counting; demographic analysis)	• VCC will review and audit Devices periodically to ensure that no new settings or features are enabled. • s. 13(1) [redacted] .
s. 15(1)(l) [redacted]	s. 15(1)(l) [redacted]
Potential for re-identification of people-counting data (e.g. 0 or 1 individuals recorded) if combined with other personal information held by VCC (e.g. work schedules; class lists; room bookings information) **and used for other purposes** (e.g. surveillance or tracking employees; following up with employees about room bookings)	• Reports are provided to VP Admin and used only for data-gathering and informing decisions about academic space resources and planning for future space allocations and campus buildings. • EMS data is only used for a booked/not booked value, and to assess whether that data accurately reflects use of space. No other EMS data (e.g. class size; name of room booker; any other identifiable information) is integrated in the FootfallCam/EMS report generated by IT Services. • VCC FIPPA Policy & FIPPA obligations: Employees cannot use information available through this data-gathering in a way that it could be identifiable (e.g. combining it with other room booking data or schedules) or use this information for any other purpose, including making decisions that would directly affect an individual. • If another use for this information arises, the initiative leads should advise the Privacy Officer and the PIA should be revised as needed.
VCC employees and students feel uncomfortable and surveilled by the presence of cameras installed in classrooms	• Marketing & Communications provided internal myVCC updates in October 24 and November 28, sharing status of PIA and disabled Devices with College community for transparency. • VCC will provide a collection notice and FAQ per Question 6, with communication to the College to direct the community to there for more information and a contact for any questions.

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

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

s. 15(1)(l)

Possible risk	Response / mitigation strategies
and feel distrust toward VCC.	• Communications will detail how initiative works, specific features of Devices, purpose of initiative, etc. • VCC employees and students follow Privacy Breaches & Complaints procedures to appropriately address concerns.
VCC employees, students, and community members could make complaints to OIPC or news outlets about privacy concerns, leading to potential investigation of complaints and impact of VCC public image.	• Completion of PIA before restarting the initiative/data collection. • Communication with OIPC regarding breach and confirmation that VCC's mitigation strategies are meeting our obligations under and compliance with FIPPA (received January 2026). • Proper notice and communications to College around initiative per Question 6 • VCC will ensure that use of FootfallCam is limited to where it is necessary and directly related to this initiative and not expand scope without review. • College (including all employees) will follow FIPPA Policy & Procedures to immediately report and manage any breaches if they occur in the future. • VCC employees will direct concerns or complaints to the Privacy Office and follow guidance.
VCC could expand use of FootfallCam beyond collecting data about bookable academic spaces.	PIA may need to be revised and reassessed and new notification given; any changes to the initiative must involve consultation with the Privacy Officer. Other initiatives involving FootfallCam can be assessed as addenda PIAs.
s. 15(1)(l)	s. 15(1)(l)

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

s. 13(1)

s. 13(1) [redacted]

s. 13(1) [redacted] the Privacy Office can recommend this PIA for approval, but only if the initiative follows the strategies identified in this PIA. The Privacy Office also discussed these mitigation strategies with the OIPC, who confirmed that they were satisfied with them, and with IT Services and the VP Admin, who are committed to implementing these strategies and agree that:

- the locations of installed Devices have been reviewed by IT and the VP Admin and they all support this initiative; Devices will only be installed if the data they collect is necessary for this initiative; and Devices will be removed when that data is no longer required for the initiative;
- IT will review the security and settings of all installed and new Devices s. 15(1)(l) [redacted] and IT will audit periodically to ensure these settings are not altered;
- The initiative will continue to take steps not to re-identify individuals through data and will never use information from this initiative to make decisions that directly affect individuals, or the initiative leads will need to revise the PIA if the initiative changes;
- VCC will provide a collection notice and communications for the College that provide details on how the FootfallCam system works, including with personal information, and details of the initiative, so that College members are appropriately informed and understand how data will and will not be used, and how to appropriately respond to any privacy breaches or concerns.

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		Jan 29, 2026

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:

N/A

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Ian Humphreys VP Administration & International Development		Jan 30, 2026
Contact Responsible for Systems Maintenance and/or Security	Elmer Wansink AVP IT & CIO		Jan 29, 2026

Privacy Impact Assessment (PIA) for FootfallCam – VCC Library

PART 1: GENERAL INFORMATION 1

PART 2: COLLECTION, USE, AND DISCLOSURE 3

PART 6: ACCURACY, CORRECTION AND RETENTION 4

PART 9: SIGNATURES 4

PART 1: GENERAL INFORMATION

PIA file number: 2025-014-1 (Addendum to PIA 2025-014)

Initiative title:	FootfallCam – VCC Library
VCC Department / Program Area:	VCC Library
Link to VCC initiative website:	Library.vcc.ca
Your name and title:	Mary Corbett, Privacy Coordinator
Your work phone and email:	marcorbett@vcc.ca
Initiative Lead name and title:	Shirley Lew, Dean, Arts and Sciences and Library
Initiative Lead phone and email:	604.871.7007 / slew@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: 2025-014 (FootfallCam + Bookable Academic Space Occupancy)	

1. What is the initiative?

The initiative is an addendum to PIA 2025-014, which assesses the VP Administration and IT Services' initiative to use FootfallCam as a people-counting system to gather data about classroom occupancy, in order to support campus planning initiatives. PIA 2025-014 considers the specific details of the FootfallCam system and devices, including how it collects and converts personal information into aggregated data.

The FootfallCam devices were installed in the two Library entrances in 2023 during IT Services' initial use of the system to assess the use of computer labs at VCC. The Library's use of FootfallCam is separate from the initiative assessed in PIA 2025-014, as it involves a different purpose of collection, but all technical and security specifications are the same unless otherwise addressed in this PIA addendum.

The VCC Library uses FootfallCam as a people-counting system to gather statistics about the number of individuals entering and exiting the two Library locations (Downtown and Broadway campus). This initiative is ongoing as there is a continuous need for the Library to collect this data.

FootfallCam Devices are installed at the Libraries' entrances. The Library is responsible for two Devices in total.

Data from the Library's use of FootfallCam is used to improve services by identifying the busiest times and days in the Library, and is used to report on the annual total number of visits. The Library receives reports for each Device's data from IT Services; data is reported hourly for each device during the Library's open hours (device, date, time, count of entrance/exit). See: https://library.vcc.ca/about-us/hours-and-locations/.

The Library's reports include hourly, monthly, and annual data that are then shared with Library staff or leadership and may be compared with past occupancy data, but not with any sources of personal information. The aggregated data is not combined with any other data that could be identifying and, as a public entrance/exit, there is virtually no risk of identification of individuals through hourly data.

2. What is the scope of the PIA?

This PIA considers the Library's use of the FootfallCam people-counting system only.

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

- Live video feed of individuals entering or exiting space (collected directly from VCC employees; students; community members) -- immediately converted and analyzed to recognize the

presence of and count individuals on FootfallCam Device.

- Temporarily-retained recordings generated from live feed for accuracy auditing/calibration
- Aggregated data of people count of entrances and exits (number of individuals), location (Library Device), and time (during open hours; reported by hour)
    - Transmitted to Footfall Cloud Server and accessed through the Platform's dashboard.

3.1 Did you list personal information in question 3?

Yes .

There is limited personal information involved in this initiative due to the function of the Devices. Personal information includes:

- Live video feed of individuals entering/exiting space
- Potential: Any recording of live feed (created for calibration/accuracy testing by Vendor and temporarily retained)

PART 2: COLLECTION, USE, AND DISCLOSURE

5. Collection, use, and disclosure flow

Personal information flow is identical to PIA 2025-014.

6. Collection Notice and Consent

6. 1 Collection Notice

The VCC Library is using the FootfallCam people-counting system to gather aggregated data about the number of individuals who enter and exit the Library during its operating hours. FootfallCam immediately processes video data on the local device and only retains and transmits aggregated data about the people count. Your personal information is collected under the authority of s. 26(c) of FIPPA and is not retained by the device. Personal information may only be temporarily retained in FootfallCam's server in the event that FootfallCam/VCC IT Services create a recording to audit a FootfallCam device's counting accuracy, and any recording will be destroyed after that use. Your personal information will not be used or retained for any other purpose. Questions about your information and the Library's use of FootfallCam may be directed to Library Systems and Technical Services at librarystems@vcc.ca.

The Library will provide this collection notice either by posting signage at the Library's entrances and/or adding the notice to the Library's website. The Library may also point to the FootfallCam FAQ (prepared for PIA 2025-014) that will be posted on IT Services' internal website. That FAQ will also indicate that the Library is the other VCC initiative using FootfallCam.

PART 6: ACCURACY, CORRECTION AND RETENTION

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

FootfallCam does not use personal information to make decisions about individuals. The Library's use of FootfallCam is solely to count people entering/exiting the Library and is not used in any decision about individuals, or combined with any information that could potentially affect an individual.

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

This PIA is recommended for approval.

Privacy Office Signatures

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

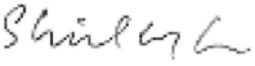
Role	Name	Electronic signature	Date signed
Privacy Officer	Caralee Maloney		Jan 29, 2026

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:

N/A

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Shirley Lew, Dean of Arts & Sciences		Feb 3, 2026