Capilano University

Privacy Impact Assessment

Space Occupancy Monitoring

Table of Contents

PART 1: GENERAL INFORMATION

Initiative Title:	Space Occupancy Monitoring
Organization:	Capilano University
Branch or Unit:	Campus Planning
PIA Drafter Name:	Sarah Hoskins
PIA Drafter Phone:	
PIA Drafter Email:	Sarahhoskins@capilanou.ca
Initiative Lead Name and Title:	Sarah Hoskins, Campus Planning Manager
Initiative Lead Phone:	
Initiative Lead Email:	
Privacy Officer:	
Privacy Officer phone:	
Privacy Officer email:	

General information about the PIA:

Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner. NO ..
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner. 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.

The Space Occupancy Monitoring will allow us to gather data regarding how many people are in a space. The monitoring involves plugging small devices into electrical outlets into a room, and the device will calculate space occupants based on the number of electronic devices in use. There is a formula, based on the type of occupancy, which counts devices using Bluetooth or wifi, such as cellphones, laptops, smart watches, ear phones, etc. and calculates how many people are using a space. The information is gathered similar to traffic reporting on a map app on a smart phone: the number of devices in one space give an idea how many people are in the space.

The data will be used for multiple purposes: 1. Recognizing trends in room usage at specific days and times, 2. Determining if purpose built spaces are right sized (the spaces are at max occupancy or rarely at the max occupancy) 3. Use for students to view an area to see how busy it is in real time, for example, the library study rooms are empty, or the cafeteria is very busy at the moment. 4. Assist in determining staffing levels in certain areas, ex: Library is rarely used on Saturday mornings, perhaps less staff are required, or library hours should be altered.

The Library (POC: Christina Neigel) will be relying on this data to integrate with the Panorama System.

The devices operate by analyze Bluetooth Low Energy (BLE) and WiFi signal data to make minute by minute occupancy estimates with 95%+ accuracy
- Devices listen to BLE and WiFi probe request packets and normalize to a people estimate for a defined space
- Devices never connect to any WiFi or Bluetooth signal. Devices passively listen for unique signals that are in the vicinity
- BLE/WiFi MAC addresses are used to differentiate signals but are never stored on devices or anywhere else in the Vendor (Occuspace) platform

- MAC addresses are hashed and truncated on the devices in memory using SHA256 with a daily changing salt value
- Hashed data sent to the vendor (Occuspace) cloud at Amazon Web Services (AWS) every minute and is then immediately deleted off devices

Occuspace service is fully GDPR compliant. Occuspace data is completely anonymous and contains no personally identifiable information (PII). Occuspace does not connect to any consumer devices and cannot track individuals.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This scope is intended for the entire initiative. While we may add on to the system and gather information in different areas at different times, or add devices in the future to gather data on additional spaces, the type of information and its purpose will be the same as this initial phase.

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, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an attachment.

Data type	*Method*	*Device used*
BLE (Bluetooth Low Energy) and Wifi Signal Data	Hardware devices which connect to University Wifi	A Bluetooth Low Energy (BLE) and WiFi signal detection device with basic compute and network capabilities, encased in a plastic tamper proof case

Did you list personal information in question 3? Yes /No **NO**

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.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer (privacy@capilanou.ca) You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

Ensure that the hardware devices are not capable of collecting personal information

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

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

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**	**Other legal authority**
Step 1:			
Step 2:			
Step 3:			
Step 4:			

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Attach or link to the collection notice to be used.

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 / No. NO

8. Does your initiative involve sensitive personal information? Yes / No. NO

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)? Yes / No

FOIPPA Section 33(2)(f) states that a public body may disclose personal information if the information is made available to the public under an enactment that authorizes or requires the information to be made public.

- If yes, go to question 10
- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

Describe exactly where the personal information is being stored, e.g., on premise servers, data centres, and in what cities.

After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider? Yes / No.

- If yes, fill in the table below (add more rows if necessary) and 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. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

Does the contract you rely on include privacy-related terms? Yes / No.

- If yes, describe, attach or link to *contract and/or other* contractual measures related to your initiative.

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

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

17. 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 additional rows if necessary.

Privacy risk	Impact to individuals	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 head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

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 need to make sure that the personal information is safely secured in both physical and technical environments.

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

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30? Yes / No. if needed

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

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

Describe where the digital records for your initiative are stored (e.g., on your organization's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. 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.

If you have completed a security assessment, you may want to append it to the PIA.

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	**Yes/No**
We only allow employees in certain roles access to information	
Employees that need standing or recurring access to personal information must be approved by executive lead	
We use audit logs to see who accesses a file and when	
Describe any additional controls: *If you have methods for controlling and tracking access to personal information that are not listed in the table, add additional methods here.*	

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

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

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 **Do you have a process in place to correct personal information?** Yes / No.

22.2 **Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself?**

Describe how records will be corrected / how notes will be recorded

22.3 **If a request for correction is received from an individual and a disclosure of their personal information has occurred in the last year, FOIPPA requires notification to the other public body or third party of the request for correction.**

Describe how disclosures be tracked and notifications be made if necessary.

23. **Does the initiative use personal information to make decisions that directly affect an individual?** Yes / No

- If yes, go to question 25
- If no, skip ahead to Part 7

24. **FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. Is there an information schedule in place related to personal information used to make a decision?** Yes / No

- If no, describe how the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement? Yes / No NO

- If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA

  See Appendix B in this guide

26. Will your initiative result in a personal information bank? Yes / No. NO

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

- If yes, please complete the table below.

Describe the type of information in the bank:
Name of main organization involved: Capilano University
Any other ministries, agencies, public bodies, or organizations involved:
Business contact title and phone number for person responsible for managing the PIB:

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.

27. 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.

Privacy risk	Impact to individuals	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.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer 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	Signature	Date Signed
Privacy Officer / Privacy Office Representative			

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Signature	Date Signed
Initiative Lead	Sarah Hoskins		
Program/Department Manager	Sarah Hoskins		
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate			

Appendix B

Information Sharing Agreement Supplement

Information Sharing Agreements

If your initiative includes or will be part of a regular and systematic exchange of personal information with partners in or outside of government, you may require an information sharing agreement.

Please provide information about your ISA.

Description of ISA:
Name of main ministry or agency involved:
Any other ministries, agencies, public bodies, or organizations involved:
Business contact title and phone number for person responsible for maintaining the ISA:
ISA start date:
ISA end date: