Table of Contents

PART 1: GENERAL INFORMATION

Initiative title:	AppArmor Mass Notification System and Mobile Safety Tool aka Langara Safe App
Organization:	Langara College
Branch or unit:	Safety, Security and Emergency Management department
Initiative Lead contact information:	Cynthia Fudgell, Manager, Health and Safety department 605-323-5706; cfudgell@langara.ca
Privacy Officer:	Joanne Rajotte, Manager, Records Management and Privacy
Privacy Officer phone:	604-323-5660
Privacy Officer email:	jrajotte@langara.ca

Is this initiative a data-linking program under FOIPPA? 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:

Not applicable.

1. What is the initiative?

Langara College's Safety, Security and Emergency Management (SSEM) department has identified the need to supplement existing channels of communication with students and employees about safety and emergency matters with an online mass notification and mobile safety tool. Currently, the Communications and Marketing departments sends mass notifications by email and by publishing notices to Langara's public-facing website.

In January 2022 SSEM purchased an enterprise software license for the AppArmor mass notification system (including the AppArmor Cloud Dashboard and AppArmor Alert) to manage mass notifications and provide information resources and services. SSEM licensed the software from CutCom Software Inc. DBA AppArmor, a Canadian company based in Toronto, Ontario. AppArmor will also provide system configuration and ongoing support services.

The department will also use AppArmor to collect information from individuals involved in safety or security incidents who choose to use the app to report incidents. SSEM will store online reports in the department's SharePoint site, and will enter (and eventually import) the information into the Workday Health and Safety module.

AppArmor uses Microsoft Azure data centres located in s.15(1)(l); s.21(1)

s.15(1)(l)

In July 2022 SSEM made AppArmor (rebranded as Langara Safe App) available to employees for review and comment. This PIA is being done during the review phase. The department plans to officially launch the app in fall or winter 2022 at which time students will be able to download the free app from Apple iTunes or Google Play store and install it on their mobile devices.

2. What is the scope of the PIA?

This PIA covers the collection, use, and/or disclosure of the personal information of students and employees who choose to download and install AppArmor, use features such as Virtual Safe Walk/Walk with a Friend, use the app to report security and safety incidents to SSEM, or are mentioned in incident reports as witnesses or respondents. Reports may also include the personal information of non-students and non-employees involved in an incident.

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

Department	Purpose	Data or Information Elements
• Safety, Security and Emergency Management and Communications and Marketing* *In the unlikely event that neither SSEM nor C&M are able to send notifications in a timely manner, the Manager, SSEM will direct the Security dispatcher of the contracted service provider (currently Paladin Security) to send the notification. *The Virtual Safe Walk/Walk with a Friend feature connects users to onsite Campus Security staff. Users may also choose to connect with a friend or relative.	**Mass Notifications and Alerts:** Collect and use device IDs to push notifications about emergencies and other important safety and security matters, e.g. active threats, snow days, etc. to students and employees who have installed the Langara Safe App.	Device identification.
	Virtual Safe Walk/Walk with a Friend* Collect and use mobile device location information to connect in real time with a student or employee who has initiated the safe walk service.	Device location.
	Safety or Security Incident Report: Collect, use, and disclose personal information of students or employees who have completed and submitted an online incident report. Reports may include the personal information of other individuals involved in an incident.	Name, email address, phone number, incident details (which may include personal information). Optionally, photograph of the reporting individual or other individuals.

3.1 Did you list personal information in question 3?

Yes.

PART 2: COLLECTION, USE AND DISCLOSURE

4. Collection, use and disclosure

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Safety, Security and Emergency Management (SSEM) will collect the personal information of students and employees directly when they: • download and install AppArmor (Langara Safe App). Specifically, users' device identification is stored in the app; • initiate a virtual walk with department staff, a member of Campus Security, or a friend. Specifically, users' device location is stored in the app as long as the user chooses, i.e., only during the walk or indefinitely; • complete and submit an online security incident report. The department may collect personal information about other individuals involved in an incident (witnesses, respondents) indirectly when the person reporting the incident provides the information in the online incident report.	Collection	26(c)
2.	Safety, Security and Emergency Management (SSEM) will use personal information to: • send mass notifications about safety and security matters to students and employees who have downloaded and installed the app **and** agreed to receive notifications. Users may download/install the app to use other services without having to receive notifications. Communications and Marketing may also send mass notifications.; • assist users who initiate a Virtual Safe Walk with the department or Campus Security; • review and respond to online security incident reports; and • file online report in department's SharePoint repository, and enter (and eventually import) information from incident report into Workday ERP's Health and Safety module.	Use	32(a)
3.	SSEM may disclose, with consent, relevant personal information about individuals involved in reported	Disclosure	33.2(d)

	security incidents to employees in other departments, including support areas such as Student Conduct and Academic Integrity, or to law enforcement when required to assist in a specific investigation.		
4.	SSEM may disclose, without consent, relevant personal information about individuals involved in reported security incidents to law enforcement when required to assist in a specific investigation.	Disclosure	33.3(d)

Risk Mitigation Table

	Risk	Mitigation Strategy	Likelihood	Impact
1.	Employees could access personal information and use or disclose it for a purpose other than the reason it was collected.	Physical and technical access to the app is restricted to authorized employees who use personal information about individuals to provide services and information and review security incident reports. In addition, employees are expected to abide by College policies related to ethical conduct, computer and computing use, and access to information and privacy.	Low	Medium
2.	The service provider's (AppArmor) employees could access personal information and use or disclose it for purposes other than the reason it was collected or disclosed.	As stated in the service provider's software and configuration support agreement with the College, AppArmor: • s.15(1)(l); s.21(1) • • •	Low	Medium
3.	Personal information could be compromised during transmission	s.15(1)(l); s.21(1)	Low	Medium

	from Langara College to the Microsoft Azure data centre.	s.15(1)(l); s.21(1)		
4.	Personal information stored in the Microsoft Azure data centre used by the service provider could be compromised.	Agreement between AppArmor and Langara requires the service provider s.15(1)(l); s.21(1)	Low	Medium

5. Collection Notice

Langara College collects personal information stored on and entered into the Langara Safe App under the statutory authority of the *Freedom of Information and Protection of Privacy Act*, s. 26(c) for the purpose of providing safety and security-related services and information to students and employees. Personal information is stored in an online system located in Canada. For questions about the collection, use and disclosure of your personal information, contact the Manager, Safety, Security and Emergency Management at safety@langara.ca.

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

PART 3: STORING PERSONAL INFORMATION

6. Is any personal information stored outside of Canada?

No. Personal information in AppArmor (Langara Safe App) will only be stored and accessed in Canada in s.15(1)(l); s.21(1)
s.15(1)(l); s.21(1) . The service provider may access and use the personal information only for the purposes specified in its Software Configuration and Support Agreement with Langara College.

s.15(1)(l); s.21(1)

7. Does your initiative involve sensitive personal information?

Yes. The following categories of sensitive personal information may be collected, used, and disclosed when individuals choose to disclose the information during completion of online security incident reports:

- Gender orientation or expression
- Race or ancestry
- Disability

8. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

9. Where are you storing the [sensitive] personal information involved in your initiative?

Information will be stored in Canada (see #6 for details).

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

PART 4: ASSESSMENT FOR DISCLOSURES OF SENSITIVE PERSONAL INFORMATION OUTSIDE OF CANADA

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

Not applicable.

11. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

Not applicable

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

Not applicable.

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

Not applicable.

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

Not applicable.

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

Not applicable.

PART 5: SECURITY OF PERSONAL INFORMATION

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

Yes, AppArmor is a cloud-based mass notification and mobile safety app.

16.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

No.

16.2 Security and Privacy Certifications

s.15(1)(l)
s.15(1)(l) , Microsoft claims the following certifications:

- **SOC 2 (Type II)** – a widely recognized auditing standard issued by the American Institute of Certified Public Accountants (AICPA).
- **ISO 27001** – standard for information security management
- **FedRAMP** – a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- **General Data Protection Regulation (GDPR)** compliant

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

In using Microsoft Azure to store data, including personal information, AppArmor shares security and compliance responsibilities with Microsoft. AppArmor controls how it architects and secures the tool and the data put on the infrastructure, Microsoft Azure is responsible for providing services on its highly secure and controlled platforms and providing a wide array of additional security features.

17.1 Technical security measures related to this initiative consist of:

According to information in AppArmor's Software License Configuration and Support Agreement, technical security controls include:

- s.15(1)(l); s.21(1)

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

- s.15(1)(l); s.21(1)
-
-
-

According to Microsoft's s.15(1)(l); s.21(1)
s.15(1)(l); s.21(1)
s.15(1)(l); s.21(1) technical security controls at
Microsoft Azure data centres include:

- s.15(1)(l); s.21(1)
-
-

17.2 Physical security measures related to this initiative consist of:

According to information in AppArmor's Software License Configuration and Support Agreement, physical security controls at the service provider's premises include:

- s.15(1)(l); s.21(1)

According to information available at s.15(1)(l); s.21(1)
s.15(1)(l); s.21(1) Microsoft s.15(1)(l); s.21(1)
s.15(1)(l); s.21(1) , to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources s.15(1)(l); s.21(1)

- s.15(1)(l); s.21(1)
-
-
-
-
-

18. Controlling and tracking access

Strategy	
We only allow employees in certain roles to have access to information	s.15(1)(l)
Employees that need standing or recurring access to personal information must be approved by executive lead	No. See above.
We use audit logs to see who accesses a file and when	s.15(1)(l)

PART 6: ACCURACY, CORRECTION AND RETENTION

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

The app automatically collects device identification and location information when students and employees download the app and use certain features; this information is considered accurate and complete. Students and employees provide personal information when reporting safety or security-related incidents directly to Langara by entering it into AppArmor. If necessary, employees will verify that the information is accurate and complete by confirming it with the individual.

20. 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.

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

As noted in #20 above, employees will confirm personal information during their review and response to safety and security-related incident reports, and will correct information when necessary.

20.2 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. Will you document the request to correct or annotate the record?

Not applicable.

20.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA 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?

Yes, Langara will notify other public bodies or third parties that disclosed personal information was corrected.

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

Yes, Safety, Security and Emergency Management, Student Conduct and Academic Integrity, and People and Culture may use personal information to make decisions about students, employees, and other individuals involved in incidents reported in the online security incident report.

22. Do you have an information schedule in place related to personal information used to make a decision?

Yes, according to the College's Recorded Information Management Policy B5010, departments must establish and adhere to retention and disposal schedules that ensure that they retain records used to make a decision about an individual for at least one year. Departments' retention schedules must also meet operational and legislative requirements, which typically results in their retaining such records longer than one year. At this time, Langara retains security incident reports for 7 years.

PART 7: AGREEMENTS AND INFORMATION BANKS

23. Does your initiative involve an information sharing agreement?

No.

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

No. Information in AppArmor is not stored or accessed by a personal identifier such as name or identification number.

PART 8: ADDITIONAL RISKS

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.

Not applicable.

PART 9: SIGNATURES

Privacy Office Comments

This PIA is based on a review of the material provided to the Manager, Records Management and Privacy by Safety, Security and Emergency Management or obtained from AppArmor and Microsoft as of the date below. If in future any substantive changes are made to the scope of this PIA, Safety, Security and Emergency Management will contact the Manager, Records Management and Privacy who will complete a PIA Update.

s.22(1)

Joanne Rajotte, Manager
Records Management and Privacy

Dec. 13, 2022
Date

Program Area Signatures:

Role	Signature	Date signed
Initiative Lead & Department Manager: Cynthia Fudgell, Manager, Safety, Security and Emergency Management	s.22(1)	12/12/2022
Head of public body, or designate: Michael Koke, Vice-President, Administration and Finance		12/12/2022