Table of Contents

Summary

In spring 2023, Records Management and Privacy, the Office of Student Conduct and Academic Integrity, and IT Cyber Security collaborated to complete a privacy impact assessment of the ConfidenceLine E-Web Reporting System to be licensed under an agreement with Xpera HR Services, a subsidiary of SCM Insurance Services. SCAI will use ConfidenceLine to provide students with a secure, and optionally anonymous, means of reporting incidents of sexualized violence or misconduct.

The primary information resources used to complete the PIA were vendor documentation and internally identified operational requirements.

The assessment identified moderate risks related to the collection, use, and disclosure of an anticipated low volume of reports that will include information about incidents of sexualized violence or misconduct, and may include sensitive personal information if students choose not to report anonymously. It also identified moderate risks related to the transfer to and storage of personal information in a cloud-based third-party data centre (Rogers Data Centres). However, these risks are mitigated because the data centre is located in Canada, and both Xpera / SCM and Rogers have comprehensive physical and technical security measures in place to protect clients' data both at rest and in transit.

PART 1: GENERAL INFORMATION

Initiative title:	ConfidenceLine E-Web Reporting System
Organization:	Langara College
Branch or unit:	Office of Student Conduct and Academic Integrity
Initiative Lead contact information:	Maggie Ross, Director, Office of Student Conduct and Academic Integrity 605-323-5151; maggieross@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:

This PIA relates to:

- PIA2022-0004 AppArmor (Langara Safe App) completed in December 2022 because individuals will connect to the ConfidenceLine online incident report form from a link located on the Langara Safe App.
- PIA2016-0001R1 Symplicity Advocate completed in November 2022 because SCAI will use Advocate to file incident-related information and records.

1. What is the initiative?

The Xpera HR Services ConfidenceLine E-Web Reporting System (ConfidenceLine) is a cloud-based software system that Langara College's Office of Student Conduct and Academic Integrity (SCAI) will use to allow students to confidentially/anonymously report experiences of sexualized violence. This system will allow students to log into a web-based platform to receive a random alpha-numeric access number. Under this random-access number, a student may report details of an incident to Langara College while remaining anonymous, if they wish. The student may continue to communicate with the College through this platform to receive support and guidance around complaint options. ConfidenceLine contributes to the College's goals under BC's *Sexual Violence and Misconduct Policy Act* by improving a student's reporting and response options around sexualized violence.

SCAI will use ConfidenceLine under a software license agreement between Langara College and Xpera HR Services, a subsidiary company of SCM Insurance Services, which is based in Canada and headquartered in Edmonton, Alberta. Xpera itself is based in Burnaby, British Columbia. Xpera / SCM uses the Rogers Data Centres located s.15(1)(l); s.21(1) s.15(1)(l); s.21(1) in the Rogers Data Centres s.15(1)(l); s.21(1). Xpera / SCM will use these two data centres to store Langara's data and information.

2. What is the scope of the PIA?

This PIA covers the collection, use, and disclosure of the personal information of students who report incidents of sexualized violence or misconduct that will be stored in the ConfidenceLine E-Web Reporting System. It may also include the personal information of other individuals involved in incidents such as respondents and witnesses.

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

Department	Purpose	Data or Information Elements
• Office of Student Conduct and Academic Integrity	**Case Management:** Collect, use, and disclose information about incidents of sexualized violence or misconduct involving students.	**Required:** • Description of incident(s) and/or behaviour **Optional*:** • Name • Langara Student Identification Number • Contact information (email address, phone number, • Name, and/or contact information and/or student identification number of respondents or witnesses *Students can report anonymously, so most personal information provided is optional.

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.	Student Conduct and Academic Integrity will collect personal information about students when they report incidents by clicking on a link in the Langara Safe App which will take them to ConfidenceLine. If students choose to report anonymously, SCAI will not collect personal information through ConfidenceLine. SCAI may collect personal information about respondents and witnesses included in the incident report.	Collection	26(c)
2.	When reports are not anonymous, Student Conduct and Academic Integrity will use personal information about students, respondents and witnesses to: • Investigate incidents • Provide or recommend services, supports or resources.	Use	32(a)
3.	When reports are not anonymous, and with consent, Student Conduct and Academic Integrity may disclose personal information about students to authorized employees in student services departments such as Counselling or Accessibility Services so they can access support services.	Disclosure	32(a)
4.	When reports are not anonymous, Student Conduct and Academic Integrity may disclose personal information about students without consent to external agencies when required by law.	Disclosure	33.2(i)

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 system is restricted to authorized employees who use personal information about students to review cases and enter incident-related information.	Low	High

		In addition, employees are expected to abide by College policies related to ethical conduct, computer and computing use, and access to information and privacy.		
2.	The service provider's (Xpera / SCM Insurance Services) employees could access personal information and use or disclose it for purposes other than the reason it was collected.	Contractual privacy clauses in agreement with the service provider restrict access to personal information.	Low	High
3.	Personal information could be compromised during transmission from Langara College to the Rogers data centre.	s.15(1)(l); s.21(1)	Low	High
4.	Personal information stored in the Rogers data centre used by the service provider could be compromised.	s.15(1)(l); s.21(1)	Low	High

5. Collection Notice

The Office of Student Conduct and Academic Integrity collects personal information under the authority of the *Freedom of Information and Protection of Privacy Act*, section 26(c) for the purpose of responding to incidents of sexualized violence or misconduct and will use it for this purpose. Information is maintained in an online reporting system located in Canada. For questions about the collection, use and disclosure of your personal information, contact the department at studentconduct@langara.ca.

PART 3: STORING PERSONAL INFORMATION

6. Is any personal information stored outside of Canada?

No.

7. Does your initiative involve sensitive personal information?

Yes. When reports are not made anonymously, the following categories of sensitive personal information may be collected, used, and disclosed during any phase of managing incidents:

- Gender orientation or expression
- Race or ancestry
- Medical/Health information
- Citizen status

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.

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, ConfidenceLine is a cloud-based incident reporting system.

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?

Yes, the IT Cyber Security team has reviewed and assessed the system's security features.

16.2 Security and Privacy Certifications

Yes.

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

As stated s.15(1)(l); s.21(1) SCM Insurance Services (Xpera HR Services' parent company) uses s.15(1)(l); s.21(1) to help protect it from unauthorized access, use and disclosure.

In using Rogers Data Centres to store data, including personal information, SCM Insurance Services shares security and compliance responsibilities with Rogers. s.15(1)(l); s.21(1)

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

17.1 Technical security measures related to this initiative consist of:

Safeguard	At Langara College	At Third Party
Authentication control: Strong Password Management	s.15(1)(l)	s.15(1)(l); s.21(1)
Authentication control: Multi-Factor Authentication (MFA)		
Role-based access		
Encrypted in transit		
Encrypted at rest		
Isolation Control: Application		
Isolation Control: Network		
Isolation Control: Database		
Vulnerability Scan		
Vulnerability Penetration Testing		
Configuration Management		

Patch Management	s.15(1)(l)	s.15(1)(l); s.21(1)
Technical Control: Perimeter firewalls		
Technical Control: Web application firewalls		
Technical Control: Distributed denial of service		
Technical Control: Intrusion prevention systems to control traffic flow		

17.2 Physical security measures related to this initiative consist of:

Safeguard	At Langara College	At Third Party
Restricted access to property (i.e. key card access)	s.15(1)(l)	s.15(1)(l); s.21(1)
Security monitored buildings		
Locked doors		
Locked filing cabinets		
Chain of custody process		
"Clean desk" practices		
Other:		

17.3 Administrative security measures related to this initiative consist of:

Safeguard	At Langara College	At Third Party
Agreement / Contract	s.15(1)(l)	s.15(1)(l); s.21(1)
Privacy / Data Protection Policy		
Documented business practices and processes for proper collection and management of personal information		
Privacy training for employees		
Staff Security Awareness Training		
Dedicated Information Security Staffing		
Information Security Policy		
Compliance and Certifications (i.e. ISO, SOC Type II, CSA)		
Security Incident Response Plan		

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.
The vendor uses audit logs to see who accesses a file and when	s.15(1)(l); s.21(1)

PART 6: ACCURACY, CORRECTION AND RETENTION

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

When students do not report anonymously, Student Conduct and Academic Integrity collects personal information directly from individuals involved in incidents of sexualized violence or misconduct.

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?

Yes, students may request their information to be updated or corrected by submitting the request in writing to the Director, Student Conduct and Academic Integrity (or delegate) and identifying the specific information they wish updated or corrected.

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, Student Conduct and Academic Integrity 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, personal information may be used to make decisions about a respondent when an investigation determines that they have engaged in sexualized violence or misconduct against others.

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. Student Conduct and Academic Integrity intends to retain online reports for 12 months.

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?

Yes. FIPPA-required personal information bank descriptors consist of:

Name: ConfidenceLine E-Web Reporting system
Data elements: Use of ConfidenceLine includes all data and personal information as outlined in section 3 (above) when students do not report anonymously
Authority: FIPPA section 26(c)
Purpose: Collected, used, and disclosed to manage reports of sexualized violence or misconduct in the ConfidenceLine system
Users: Used by employees in the Office of Student Conduct and Academic Integrity. SCAI may disclose limited personal information to authorized employees in other departments, or to external agencies as required by law.

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 Student Conduct and Academic Integrity or obtained from Xpera HR Services / SCM Insurance Services as of the date below. If in future any substantive changes are made to the scope of this PIA, Student Conduct and Academic Integrity will contact the Manager, Records Management and Privacy who will complete a PIA Update.

s.22(1) _____ MAY 11, 2023

Joanne Rajotte, Manager
Records Management and Privacy

Date

Program Area Signatures:

Role	Signature	Date signed
Initiative Lead & Department Manager: Maggie Ross, Director, Office of Student Conduct and Academic Integrity	s.22(1)	May 17/2023
Contact Responsible for Systems Maintenance and/or Security: Charles Boname, Associate Director, Cyber Security		MAY 17, '23
Head of public body, or designate: Deborah Schachter, Associate Vice-President, Students		May 18, 2023