

Part 1 – General

Name of Department/Branch:	Langara College, Educational Technology		
PIA Drafter:	Joanne Rajotte, Manager, Records Management and Privacy		
Email:	irajotte@langara.ca	Phone:	604-323-5660
Program Manager:	Patricia Cia, Director, Academic Innovation		
Email:	pcia@langara.ca	Phone:	604-323-5243

1. Description of the Initiative

In 2018, Langara College’s Educational Technology (EdTech) department entered into an agreement with Zoom Video Communications (Zoom), a company headquartered in San Jose, California, to purchase remote video conferencing software to support remote teaching and learning. Zoom is a Software as a Service (SaaS) platform that uses cloud-based data centres located throughout the world. Refer to Section 5 for storage and access information.

Due to the COVID-19 crisis and the need for physical distancing, in March 2020 Langara College moved its educational services and administrative operations online. The shift to working and teaching remotely required the rapid deployment and adoption of tools and services to support online operations. As a partial response to the crisis, Langara purchased more Zoom licenses to support all courses that moved instruction online. Langara is using Zoom primarily for remote instruction. Staff and administrators also use Zoom to conduct meetings, although Microsoft Teams is more common.

2. Scope of this PIA

This PIA covers the collection, use, disclosure and storage of the personal information of students, faculty and staff who use the Zoom video conferencing system to conduct classes, webinars or meetings online.

3. Related Privacy Impact Assessments

None.

4. Elements of Information or Data

Meeting Hosts (Langara account holders):

Name
Langara College email address
Image, i.e., profile photo and/or on-screen image (optional)
Department
IP address
Network type, i.e., wired or wireless
Device type, i.e., Windows, Mac, Android
Connection Type
Equipment type, i.e., speaker, microphone, camera
Device location (city and/or country name)
Meeting start and end times

Participants (non-account holders):

First name or Full name (if provided) or Anonymous identifier
Image, i.e., profile photo and/or on-screen image (optional)
IP address
CPU usage
Zoom version used
Network type, i.e., wired or wireless
Device type, i.e., Windows, Mac, Android
Connection Type
Equipment type, i.e., speaker, microphone, camera
Device location (city and/or country name)
Meeting join and leave times

Both hosts and participants may disclose personal information during Zoom sessions through audio conversations, written chats/messages, or through their web cameras.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Langara currently uses Zoom’s standard configuration, which stores data on servers outside of Canada. In mid-April, EdTech directed Zoom to provision the College’s enterprise account from the Amazon Web Services (AWS) Canada (Central) Region data centre located in Toronto to ensure that all data, including personal information, is stored in Canada.

Until such provisioning occurs, EdTech has enabled a newly introduced feature that allows account holders to select the data centre region in which meetings and webinars are hosted. EdTech has set the Canada (Central) Region as the default.

6. Data-linking Initiative*

<p>In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.</p>	
<p>1. Personal information from one database is linked or combined with personal information from another database;</p>	<p>No</p>
<p>2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;</p>	<p>No</p>
<p>3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.</p>	<p>No</p>
<p>If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.</p>	

7. Common or Integrated Program or Activity*

<p>In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.</p>	
<p>1. This initiative involves a program or activity that provides a service (or services);</p>	<p>Yes</p>
<p>2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;</p>	<p>No</p>
<p>3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.</p>	<p>No</p>
<p>Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.</p>	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table – Instructional Use			
	Description/Purpose	Type	FOIPPA Authority
1.	Instructor emails students to participate in a Zoom meeting or webinar. In the future, instructors may be able to email students directly from the Brightspace learning management system.	Use	32(a)
2.	Students accept invitation and log on to Zoom session. Students may choose to log on with their full name, partial name or an anonymous identifier. Log on name or identifier is stored on Zoom servers outside of Canada.	Collection (only when user name is personally identifiable)	26(c)
3.	Instructor and students participate in the Zoom session. Real-time data transmitted between participants during the session is routed through the AWS Canada Region data centre.	Collection (only when user name is personally identifiable), Disclosure	26(c) 33.2(a)
4.	Instructor may record Zoom session; the recording is stored locally on the instructor’s computer. Recordings may include personal information of the instructor and students captured during discussions.	Collection (if recorded), Use	26(c) 32(a)
5.	Metadata about Zoom session participants is stored on Zoom servers located outside of Canada.	Collection (only when user name is personally identifiable), Disclosure	26(c) 33.1(1)(p.2)

Personal Information Flow Table – Administrative Use			
	Description/Purpose	Type	FOIPPA Authority
1.	Host emails invitations to Zoom meeting to fellow employees at the Langara College email addresses.	No personal information used because emails are business contact information.	Not applicable
2.	Host emails invitations to Zoom meeting to external participants at their business email addresses.	No personal information used because emails are business contact	Not applicable

		information.	
3.	Internal and/or external participants accept invitation and log on to Zoom session.	No personal information collected because emails are business contact information.	Not applicable
4.	Participants communicate during the Zoom session. Real-time data transmitted between participants during the session is routed through the AWS Canada Region data centre.	Disclosure (only if oral or written discussion between participants contains personal information).	33.2(a)
5.	Host may record Zoom session; the recording is stored locally on the host's computer. Recordings may include personal information of the participants captured during discussions.	Collection (if recorded), Use	26(c) 32(a)
6.	Metadata about Zoom session participants is stored on Zoom servers located outside of Canada.	Collection (if participants use their personal computer/device), Disclosure	26(c) 33.1(1)(p.2)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Personal information is compromised during transmission to and from Zoom, and while stored on servers in the AWS datacentre.	According to Zoom's Privacy and Security Whitepaper, Zoom ^{s.15(1)(l); s.21(1)} s.15(1)(l); s.21(1)	Low	High
2.	Meeting host records session that contains confidential or sensitive personal information, e.g. Counselling or Accessibility Services student sessions, or employee disciplinary or grievance sessions.	Student-related sessions: If recording is necessary to provide subsequent advising services, host must offer students the option to identify themselves with a non-personal identifier. Administrative-related sessions: Host	Low	Medium

		should not record session that discusses or discloses sensitive personal information.		
3.	Meeting host discloses session recording with unauthorized third parties. Recording may contain personal information.	Employees know of, and are expected to abide by, College policies related to ethical conduct, computer and computing use, access to student computer records, and access to information.	Low	Medium
4.	Meeting invitee shares emailed invitation and link with unauthenticated user(s), which may lead to unauthorized access to personal information.	Faculty and staff are encouraged to use Zoom's Waiting Room feature to control access to session and can remove an attendee and prevent them from re-joining the session.	Low	Low
5.	Students and employees already have a pre-existing account on the Zoom app.	Users who already have the app have consented to Zoom's terms and conditions, including having their personal information stored outside of Canada. Other than meeting hosts, participants can attend Zoom meetings without an account.	Medium	Low
6.	Employees do not have appropriate security controls in place on their personal computing equipment.	Langara provides Zoom training and resources on cyber-security and working remotely.	Low	Low

10. Collection Notice

Although there is no Zoom meeting-specific personal information collection, use and disclosure notification, the College's [application for admission](#) forms notify students of the purpose for collecting and using their information, the legal authority for collection and the contact information of someone to answer questions. In addition, instructors offer students the option to identify themselves with a non-personal identifier such as a pseudonym (e.g., first name only or a nickname).

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

According to Zoom, the provider uses the following physical security measures:

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

12. Please describe the technical security measures related to the initiative (if applicable).

According to Zoom, the provider uses the following technical security measures:

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

Security and Privacy Certifications

On its website, Zoom claims the following certification and compliance:

- **SOC 2 (Type II)** – a widely recognized auditing standard issued by the American Institute of Certified Public Accountants (AICPA).
- **FedRAMP (Moderate)** – a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
- **GDPR, CCPA, COPPA, FERPA and HIPAA Compliant**
- **Privacy Shield Certified (EU/US, Swiss/US, Data Privacy Practices)**
- **TrustArc Certified Privacy Practices and Statements**

13. Does your branch/department rely on any security policies?

Langara College has a policy and associated procedures that govern the collection, use, access, storage, disclosure and disposal of personal information (Access to Information, B5001) as well as a Computer and Computing Use Policy, B5002 and its associated procedures.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Not applicable. It is not anticipated that recorded Zoom sessions will contain personal information that could be updated or deleted.

15. Please describe how you track who has access to the personal information.

Not applicable.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

Students may participate in Zoom sessions anonymously if they wish. If they choose to provide personal information about themselves, they are responsible for ensuring that it is accurate. Once stored in Zoom servers, personal information cannot be updated or corrected.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No. Faculty and staff will maintain any record of a decision that directly affects an individual, e.g., student or employee, in repositories under the College's custody and control, in paper or electronic format as applicable.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Not applicable.

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Not applicable.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No.

<i>Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).</i>	<input type="checkbox"/>
--	--------------------------

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No.

<i>Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).</i>	<input type="checkbox"/>
--	--------------------------

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

No.

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Manager, Records Management and Privacy by Educational Technology or obtained from Zoom’s online information resources as of the date below. If in future any substantive changes are made to the scope of this PIA, Educational Technology will contact the Manager, Records Management and Privacy who will complete a PIA Update.

s.22(1)

Joanne Rajotte, Manager
Records Management and Privacy

June 18, 2020
Date

Part 7 – Program Area Signatures

s.22(1)

Patricia Cia, Director, Academic Innovation

June 18, 2020

Date

s.22(1)

Marg Heldman, Vice-President, Academic (Interim)

June 18, 2020

Date

s.21(1)

Relationship Management

s.21(1)

Billing

s.21(1)

Infrastructure

s.21(1)

Updates

As our business grows and evolves, the Subprocessors we utilize may also change. We will provide the owner of Customer's account with notice of any new Subprocessors to the extent required under contractual agreement, along with posting such updates here.

Appendix II – Required Settings for Selected Zoom Features at Langara College

Category	Description	Locked Setting (Cannot be Changed by Meeting Host)	Default Setting (Can be Changed by Meeting Host)
Scheduling Meeting	Host video - Start meetings with host video on.	s.15(1)(l)	
	Participants' video - Start meetings with participant video on. Participants can change this during the meeting.		
	Join before host - Allow participants to join the meeting before the host arrives.		
	Enable Personal Meeting ID - A Personal Meeting ID (PMI) is a 9 to 11 digit number that is assigned to your account.		
	Use Personal Meeting ID (PMI) when scheduling a meeting		
	Use Personal Meeting ID (PMI) when starting an instant meeting		
	Require a password for Personal Meeting ID (PMI)		
	Only authenticated users can join meetings - The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.		
	Only authenticated users can join meetings from Web client - The participants need to authenticate prior to joining meetings from web client.		
	Require a password when scheduling new meeting - A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.		
	Embed password in meeting link for one-click join - Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.		
	Require password for participants joining by phone - A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.		
Mute participants upon entry - Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.			
In Meeting (Basic)	Require Encryption for 3rd Party Endpoints (H323/SIP) - Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).		
	Chat - Allow meeting participants to send a message visible to all participants.		
	Chat - Prevent participants from saving chat.		
	Private chat - Allow meeting participants to send a private 1:1 message to another participant.		

<p>Auto-saving chats - Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.</p>	<p style="font-size: 2em; color: red;">s.15(1)(l)</p>
<p>File transfer - Hosts and participants can send files through the in-meeting chat.</p>	
<p>Feedback to Zoom - Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting.</p>	
<p>Co-host - Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host.</p>	
<p>Screen sharing Allow host and participants to share their screen or content during meetings. Who can share? Host Only or All Participants Who can start sharing when someone else is sharing? Host Only or All Participants</p>	
<p>Disable desktop/screen share for users - Disable desktop or screen share in a meeting and only allow sharing of selected applications.</p>	
<p>Annotation - Allow participants to use annotation tools to add information to shared screens.</p>	
<p>Whiteboard - Allow participants to share whiteboard during a meeting.</p>	
<p>Remote control - During screen sharing, the person who is sharing can allow others to control the shared content.</p>	
<p>Allow removed participants to rejoin - Allows previously removed meeting participants and webinar panelists to rejoin.</p>	
<p>Allow participants to rename themselves - Allow meeting participants and webinar panelists to rename themselves.</p>	
<p>Hide participant profile pictures in a meeting - All participant profile pictures will be hidden and only the names of participants will be displayed on the video screen. Participants will not be able to update their profile pictures in the meeting.</p>	

	<p>Report participants to Zoom - Hosts can report meeting participants for inappropriate behavior to Zoom's Trust and Safety team for review. This setting can be found on the Security icon on the meeting controls toolbar.</p>	<p>s.15(1)(l))</p>
	<p>Remote support - Allow meeting host to provide 1:1 remote support to another participant.</p>	
	<p>Closed captioning - Allow host to type closed captions or assign a participant/third party device to add closed captions.</p>	
	<p>Save Captions - Allow participants to save fully closed captions or transcripts.</p>	
<p>In Meeting (Advanced)</p>	<p>Far end camera control - Allow another user to take control of your camera during a meeting.</p>	
	<p>Virtual background - Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.</p>	
	<p>Identify guest participants in the meeting/webinar - Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants' list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.</p>	
	<p>Auto-answer group in chat - Enable users to see and add contacts to 'auto-answer group' in the contact list on chat. Any call from members of this group will be automatically answered.</p>	
	<p>Select data centre regions for meetings/webinars hosted by your account Include all data centre regions to provide the best experience for participants joining from all regions. Opting out of data centre regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.</p> <p style="text-align: center;"> Australia Canada China Europe Hong Kong China India Japan Latin America United States </p>	
	<p>Waiting Room - When attendees join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing attendees to join before host.</p> <p>Choose which participants to place in the waiting room: All participants or Guest participants only</p>	

	<p>Show a "Join from your browser" link - Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited.</p> <p>Allow live streaming meetings</p> <p>Phone - Mask phone number in the participant list - Phone numbers of users dialing into a meeting will be masked in the participant list. For example: 888****666</p> <p>Blur snapshot on iOS task switcher - Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window. This snapshot displays as the preview screen in the iOS tasks switcher when multiple apps are open.</p>	<p>s.15(1)(l))</p>
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Recording</p>	<p>Local recording Allow hosts and participants to record the meeting to a local file. Hosts can give participants the permission to record locally.</p>	
	<p>Cloud recording - Allow hosts to record and save the meeting / webinar in the cloud.</p>	
	<p>Automatic recording - Record meetings automatically as they start.</p>	
	<p>Recording disclaimer - Show a customizable disclaimer to participants before a recording starts (as follows): I understand that the instructor/facilitator may record this session for teaching/learning purposes, and that the instructor/facilitator will inform students before the recording begins.</p>	
	<p>Multiple audio notifications of recorded meeting - Play notification messages to participants who join the meeting audio. These messages play each time the recording starts or restarts, informing participants that the meeting is being recorded.</p>	