Privacy Impact Assessment for Non-Ministry Public Bodies

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Yuja (video platform)
Organization:	Vancouver Island University
Branch or unit:	Centre for Innovation and Excellence in Learning
Your name and title:	Jacqueline Kirkham, Learning Technology Application Developer
Your work phone:	(250) 753-3245 x2916
Your email:	Jacqueline.Kirkham@viu.ca
Initiative Lead name and title:	Maxwell Stevenson, Director of the Centre for Innovation and Excellence in Learning
Initiative Lead phone:	(250) 740-6513
Initiative Lead email:	Maxwell.Stevenson@viu.ca
Privacy Officer:	William Boyt
Privacy Officer phone:	(250) 740-6564
Privacy Officer email:	William.Boyte@viu.ca

General information about the PIA:

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:
No other PIAs have been completed on Yuja. However, BCNET has begun a PIA on Amazon Web Services (AWS) Canada. BCNET has completed PIAs for Zoom and D2L.

1. What is the initiative?

The Centre for Innovation and Excellence in Learning supports online and digitally enhanced teaching and learning at Vancouver Island University by selecting and supporting learning tools and platforms that are available to all instructors and students at the institution. A key part of this work is ensuring that VIU employees and students have access to platforms that are hosted, accessed, managed, and protected within a secure environment in accordance with the Provincial Freedom of Information and Privacy Protection Act (FIPPA).

From 2017 to 2022, VIU's video hosting needs were met by a shared Kaltura video platform acquired by BCNET and hosted by the University of British Columbia. This service is at end of life and will be permanently disabled in September 2022. Through an open, competitive procurement process, VIU has selected the Yuja video platform as the replacement for this service.

The Yuja video platform is a digital asset management system to be used by VIU employees and students who increasingly rely on video for teaching and learning in online, blended, and face to face courses. Video is used both to make course materials available in an asynchronous way to give students flexibility, but also by students to demonstrate knowledge and skills required in their learning. Since 2020, the use of video in teaching and learning at VIU has increased significantly. As of April 2022, VIU has over 55,000 video assets on the Kaltura platform. In the past 12 months we have had over 4,000 unique viewers watching nearly 3,000,000 minutes of recorded content.

Yuja is used by post secondary institutions across Canada including the University of Calgary, University of Windsor, and Trent University as well as many universities and colleges in the United States.

Yuja offers a cloud hosted VPaaS (Video platform as a service) environment hosted on AWS Canada. The Yuja platform can be accessed both as a central, standalone portal and integrated with existing platforms in use at VIU including Zoom and the D2L Brightspace Learning Management System to provide a seamless experience for students and employees who need to create, share, or consume video content.

2. What is the scope of the PIA?

This PIA covers the collection, use and disclosure of personal information from VIU students and employees to the Yuja platform. This PIA is intended to cover the services, and operational controls in place for both Yuja and AWS as it relates to Privacy, Security, and Data protection in British Columbia. This PIA will also cover integrations between Yuja and D2L Brightspace as well as the cloud recording integration available between Yuja and Zoom.

This PIA does not cover every possible site or situation that could arise from end users sharing the media files hosted on the Yuja platform. End users must take responsibility for protecting their own content and any personal information (theirs or others') within that media content in accordance with VIU's policies and BC laws.

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

To access and use Yuja, students and employees must have a user account. User accounts will contain the following personal information which will be saved into the Yuja platform from the VIU directory at the time of first login with the system. Users who interact with Yuja through the LMS will be logged in to Yuja automatically through the integration.

User Accounts will contain:

- user ID (student number for students, username for employees)
- full name
- email address (employees only)

When a user interacts with the platform by watching media, taking a video quiz, leaving a comment etc. additional information may be captured including the user's activity, course membership, and IP address. Analytics data for individual videos is available to the owner of the video and system admins. Information about course membership of users is used to give access to shared course galleries of media but is not otherwise made available to any end users of the platform.

Employees who use the Zoom cloud recording function will have their institutional Zoom account connected to their Yuja account to allow Zoom cloud recordings to be automatically imported to Yuja and deleted from the Zoom cloud. Specific Zoom settings have been locked at the account level for all VIU institutional accounts to balance the need for flexible recording options and participant privacy. See Appendix A.

Additional personal information may be captured in the media that is uploaded to the platform including recordings of individuals' or audio of their voices, names, and other potentially sensitive information. Individual media creators and uploaders will need to control this data in accordance with guidelines from VIU.

Once a media file (video, audio, or image) is uploaded to Yuja, access to this media is controlled by the media owner. By default, only the media owner and CIEL staff who are system administrators for Yuja will have access to the media. Users may choose to share their media by link or embed it in a course page or other website. Access to the information contained in that media item will be governed by where the media is shared.

3.1 Did you list personal information in question 3?

Yes.

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

Video platforms by nature of their functionality always carry a risk of unintentionally gathering personal information from individuals who did not freely choose or consent to their likeness, voice, name, or other personal information being uploaded to the platform. Student and Employee use of the Yuja platform falls under the Use of Information Technology Policy (45.01) which outlines for students both VIU's responsibilities (section 3) and end user obligations when using technology at VIU (section 4).

When an employee records a Zoom meeting, a disclaimer appears informing participants they are being recorded and giving an option to opt out of the meeting (see Appendix A).

PART 2: COLLECTION, USE AND DISCLOSURE

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**	**FOIPPA authority**	**Other legal authority**
Account Creation Username/student number, full name and email are required to create unique user accounts.	collection		
Media Uploaded End users may upload recordings (video or audio) that include the voice and image of themselves or others.	collection		
Media Shared / Viewed End users may stream their own videos or share videos with other individuals. Anyone given access to a video will have access to all personal information contained in that media file.	Use/disclosure		
Media Analytics When a person views or interact with (such as leaving a comment or taking a video quiz) a media object through Yuja, their name (if they	Collection/use		

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**	**FOIPPA authority**	**Other legal authority**
are an account holder), ip address, and details of their interaction will be captured and visible to the owner of the video as well as system admin.			
Integration with D2L Brightspace Employees and students who access a Yuja media file through their online course space will have their interactions with that item captured in the analytics. If they had not previously accessed Yuja, an account would be automatically created in order to track that interaction.	Collection/use		
Integration with Zoom Cloud Recording VIU employees who have a Zoom account under the VIU institutional license will be able to record to the Zoom cloud provided they agree to their media being automatically transferred to their Yuja user account and deleted from Zoom's cloud infrastructure. Zoom recordings may contain personal information from participants and hosts.	Collection/use		

6. Collection Notice

The Centre for Innovation and Excellence in Learning has a website where students and employees can find resources to help them with using the learning technologies at VIU. We have added a page on our Student Support Resources section titled “How VIU Online Learning Tools Manage Your Data” which explains to students what information each tool gathers, where it is stored, who has access to it, and how long that data is retained. When students access our Learning Management System (VIULearn) for the first time, they are presented with an information page where they are required to acknowledge they have read and agree to abide by the linked policies in order to access the system. A data section has been added to this page with a link to the aforementioned page on CIEL’s website.

For employees, a unique page for each tool describing what data is collected by that tool from employees and from students, how that data is accessed, and for how long the data is retained will be added to the support hub for that tool. CIEL will have these pages on https://ciel.viu.ca no later than August 1, 2023.

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?

No.

8. Does your initiative involve sensitive personal information?

- No

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

Type “yes” or “no” to indicate your response.

- If yes, go to question 10

- If no, go to Part 4

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

Personal data will be stored by Yuja on AWS Canada.

~~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?~~

~~Type "yes" or "no" to indicate your response.~~

- ~~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.~~

~~13. Does the contract you rely on include privacy-related terms?~~

~~Type "yes" or "no" to indicate your response.~~

- ~~If yes, describe the 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 new 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

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

Digital records for Yuja will be stored by Yuja who uses AWS Canada server infrastructure. Both Yuja and AWS have data security practices in place to prevent unauthorized access to data.

See Appendix B for a copy of the information obtained from Yuja about their data security practices during the procurement process.

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	
We only allow employees in certain roles access to information	X
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:	Within VIU, only CIEL staff who require access to support Yuja will have access to all uploaded content. Role permissions within the tool and with the LMS will allow access for students and instructors to be limited to only media they own or media they require access to for teaching and learning purposes within specific courses.

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?

Personal information sent to Yuja when a user's account is created or when a user with an account interacts with a video is sourced from the official VIU information systems (HR systems for employees and Student Record System for students). Students and employees can request corrections or updates to their data through official systems and if this information does not automatically update in Yuja, CIEL staff can assist with correcting the data in the video platform.

22. Requests for correction

Requests to correct information in a user's account in Yuja can be submitted to learnsupport@viu.ca and CIEL staff will update the user's account to match official records for that user. If official records are incorrect, the user must first work with the relevant department at VIU to correct the official record.

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

Yes.

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

If a request to correct information stored on Yuja cannot be fulfilled, CIEL staff will note this in our internal ticketing system so there is a written record of the request and why it could not be fulfilled.

22.3 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?

N/A

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

Yes. Video content stored on the Yuja platform may be used in assigning grades or making other institutional decisions.

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

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

It is CIEL's intention to implement a process in Yuja to delete videos that are more than two years old. We have not refined the exact details of this process yet. We currently perform a cleanup process with our LMS that deletes all courses two full academic year after they concluded (annually in July) allowing VIU to retain all instructional materials and student work for a minimum of 1 year after the course concluded. We are intending a similar process with Yuja but will need an opt-out option for videos that do not contain personal information for students or community members (such as instructional videos) and do not need to be deleted to protect user information.

CIEL is working on a process for data destruction and archiving for this service. However, we need to understand the technical options in the system before we can finalize a process that will enable VIU to retain and remove media assets. This process will be in place and communicated to the users no later than August 1, 2023.

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?

No.

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

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

Yes

Describe the type of information in the bank
Usernames/student numbers, full names, employee email, course enrolments, media file names and metadata are all stored in Yuja. Media files can be searched for by unique media ID, course affiliation, title, and owner. This inherently means that individual users can be searched for by their name or user ID as well as by their media. Only those authorized to view a user's content would be able to find the user through searching.
The Centre for Innovation and Excellence in Learning

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.

Add new rows if necessary.

Possible risk	Mitigation
Risk 1: Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes (within VIU)	Employee Code of conduct and Non-disclosure agreements; Use of Information & Technology Policies, password protected access, user access to system, based on need to know basis, permission restrictions, controls, and monitoring.
Risk 2: Authorized individuals could access the personal information in the Yuja platform and use or disclose it for personal purposes	Confidentiality Agreement between Yuja and VIU, Employee Code of conduct and non-disclosure agreements; Use of Information & Technology Policies, password protected access, user access to system, based on need to know basis, permission restrictions, controls, and monitoring

Possible risk	**Mitigation**
Risk 3: Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes (within Yuja)	Contractual privacy protection between VIU and Yuja as well as internal security and privacy standards at Yuja.
Risk 4: Yuja security breach	Breach protocols are in place to reduce risks to client data in the event of a security breach. Yuja will notify VIU in the event of a breach within 24 hours so VIU can take appropriate action.
Risk 5: AWS Cloud Security Breach	AWS breach protocols are in place to reduce risks to client data in the event of a security breach.
Risk 6: Personal information data is compromised during transmission from end user to Yuja.	All data transmission is encrypted.

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

Primary comments were provided in the preliminary draft of this PIA and have been incorporated into this version.

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 / 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	Electronic signature	Date signed
Initiative lead			
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate Only required if personal information is involved			

APPENDIX A

1. Locked Recording Settings

In order to balance employees' needs for flexibility in what video streams they obtain from a Zoom meeting with our need to protect student and community member privacy Cloud Recording is configured so it captures the following:

- **Active speaker and shared screen** - captures shared screen and thumbnail of video for current speaker. Users whose video is turned off will have only their voice (not name or image) captured.
- Separate videos for the following (if available)
  - **Active speaker**
  - **Gallery** (excludes anyone who has video off)
  - **Shared Screen** (no user video, just the content shared)
  - **Audio only**
- **Audio transcript** - generated after the video is uploaded, includes speaker names and machine generated transcript of all audio captured.
- **Closed captions** - only generated if closed captions are on and displayed by the host during the meeting.
- **Participant names in the recording (disabled)** - participant names are not displayed on their video (if enabled) or anywhere else in the video feed. Names will still be included in the Transcript file for anyone who speaks during the recorded portion of the meeting.

In addition to locking what can be included in a recording we have locked the following settings:

Automatic Recording (disabled) - employees must choose to record meetings manually rather than automatically recording every meeting that they host.

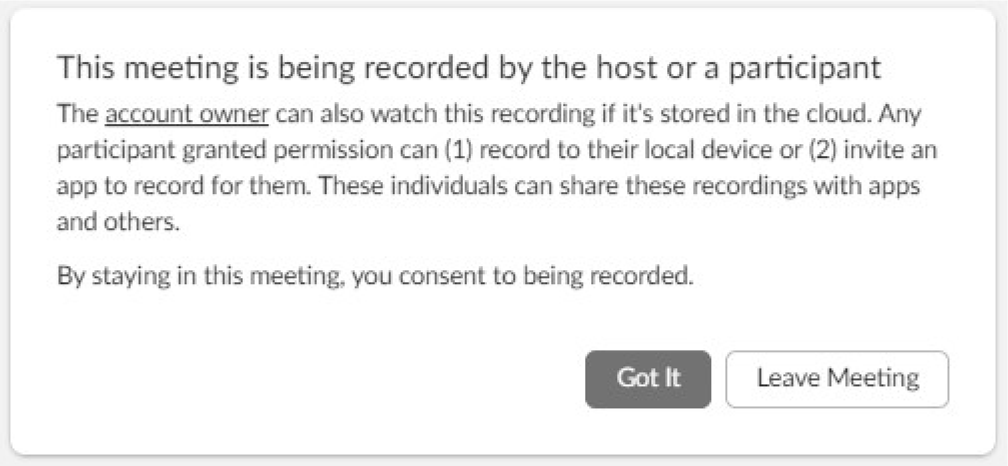
Allow cloud recording sharing (disabled) - employees can access their own cloud recordings on Zoom but cannot share them by link. In order to share a cloud recording, they must download the recording and upload it to another platform or share the source file.

Auto delete cloud recordings after X days- to allow recordings to be moved to the trash after 7 days if they are still in a user's Zoom cloud recording collection at that time. All users who have access to Cloud Recording on Zoom will also have a connection set up between their Zoom account and YuJa which will automatically import recordings within 24 hours. Recordings that have been imported into YuJa will be moved to the Trash in Zoom 1 day after the import to YuJa is complete. Videos in trash are permanently deleted 30 days after being moved to trash. Videos imported to Yuja will be kept in accordance with the VIUTube retention process CIEL will finalize no later than August 1, 2023.

Hosts can delete video - Individual employees can choose to manually delete their recordings at any time.

2. Recording Disclaimer

When a recording is begun on Zoom, a disclaimer shows for all participants alerting them that a recording has begun and allowing them to choose to remain in the meeting or leave the meeting. The disclaimer text as of June 2022 reads



This meeting is being recorded by the host or a participant

The account owner can also watch this recording if it's stored in the cloud. Any participant granted permission can (1) record to their local device or (2) invite an app to record for them. These individuals can share these recordings with apps and others.

By staying in this meeting, you consent to being recorded.

Appendix B. Yuja-provided security policy withheld under s. 15(1)(l) and s. 21(1).

[redacted]

[redacted]