BCNET 30 Years
Shared Services for Higher Education & Research

Privacy Impact Assessment

Kaltura Video Cloud Platform for Education

Table of Contents

Note to BCNET Member Institutions:

This Privacy Impact Assessment (PIA) has been created for the benefit of Member Institutions. Member Institutions should customize the contents of this PIA to ensure it accurately reflects their use of the system or program being assessed. Areas highlighted in red are for information only and should be deleted or replaced with the Member Institution's information.

PART 1: GENERAL INFORMATION

Initiative title:	Kaltura Video Cloud Platform for Education
Organization:	BCNET
Branch or unit:	
Your name and title:	Jo-Ann Bellamy Hooper Access and Privacy Consulting Ltd.

Your work phone:	250-208-3431
Your email:	jbellamy@hooperconsulting.ca
Initiative Lead name and title:	Devon Keys Senior Business Analyst, Shared Systems and Technology Office
Initiative Lead phone:	604-343-0506
Initiative Lead email:	devon.keys@bc.net
Privacy Officer:	Bev Hooper Hooper Access and Privacy Consulting Ltd.
Privacy Officer phone:	250-208-3431
Privacy Officer email:	bev@hooperconsulting.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:
BCNET has completed a PIA on AWS (Canada). <Member institutions should list any related PIAs they have completed.>

1. What is the initiative?

BCNET is a federally incorporated not-for profit services and information technology organization that represents the interests of its member institutions comprised of 25 publicly funded universities, colleges, institutes, and research organizations across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing, and IT services.

Kaltura Video Cloud Platform for Education is a single platform purposefully built to power real-time, live and VOD experiences for online programs and virtual learning. The Kaltura Video

Cloud Platform for Education includes a range of products for virtual classrooms, lecture capture, webinars and live events, and student outreach. The platform can be used by member institutions to store, process, and distribute videos and other information belonging to the institution or their users through their websites, apps, or other comparable means.

The Kaltura Video Cloud Platform is hosted on Kaltura's Canada Cloud which is hosted on AWS (Canada).

Kaltura Video Cloud Platform includes the following products/features:

Virtual Classroom

The Kaltura Virtual Classroom features include interactive tools such as whiteboards, screen sharing, breakout rooms, real time notes, and live quizzes. Instructors can manage their online classroom interactions with advanced moderation controls and use attention indicators to bring focus back to the content. With cloud recording and automatic transcription, course content is easily accessible. Editing tools and advanced analytics allow instructors to optimize content, repurpose, and maximize engagement.

Students can join virtual classrooms where they can interact face-to-face from anywhere and on any device. There are no downloads or installations required. As the Virtual Classroom can be integrated into the member's learning management system (LMS) students can quickly catch up on content they missed or review the material, directly in the LMS.

Lecture Capture

Lecture Capture makes it possible to create interactive videos, live or on-demand, and automatically publish them on an eLearning system. Videos, recordings, and screengrabs sync into the LMS or VLE. Recordings can be scheduled and managed on a single dashboard. Recordings can include 4 different streams and auto-detect slides and chapters. Recordings can include video quizzes, captions, chapters, and hotspots. Lecture Capture comes with built-in Kaltura's advanced analytics that provides data and insights on viewership, user-level heatmaps, and comparative analysis.

LMS/VLE Integration

The Kaltura LMS Video Integration provides instructors and students with a range of tools designed to support engaging and effective teaching and learning experiences in one central place. With Kaltura's Video LMS, instructors can extend the classroom through hybrid and flexible teaching options, without leaving the LMS/VLE environment.

Video Portal

The Kaltura Video Portal is a video solution that offers a flexible environment so members can unify their videos from the institution, using the institution's branding, workflows, and content. The platform can be customized to meet the video needs of every department.

Once created or uploaded, video can be enhanced with captions, interactive video quizzes, interactive content that changes based on user actions, chapters, slides, video calls to action, advertising, and more. With Kaltura's open platform, videos are then available in common video formats so members can use their videos anywhere.

Webinars and Townhalls

Town Halls provides end-to-end live streaming that can be recorded and viewed on-demand. Town Halls offers a plug-and-play streaming to create and manage webcasts from anywhere, at any scale, to any device. Real-time analytics are built in. Users can monitor and analyze quality of service, track viewer participation and engagement, and run post-event analysis to measure the event's success. Townhalls can be used directly from studio (RTMP, RTMPS, RTSP), desktop, or video conferencing solutions, including Kaltura Meetings, Zoom, Skype, and Webex. Events is hosted on a simple URL that's accessible from any device, all in the cloud. The cloud can also record the event so that it's available to watch later, on the same URL. Users can edit, add hotspots, captions, and translations.

Video Messaging

Using Video Messaging, users can create, send, and track videos messages directly out of their mailbox. Users can get real-time alerts and keep track of who's watching, when, and where. Users can adjust the webcam or record on their phone. Video Messaging automatically uploads the video to the cloud and creates a branded email and landing page that the user can send to anyone.

Live Streaming

Kaltura offers a flexible and reliable end-to-end live streaming platform that can broadcast events of any size. Users can create and manage webcasts that can be reliably delivered at any scale, to any device, anywhere. Users can choose full production support or self-serve broadcasting.

Machine Captioning for Video-on-demand Content

Video-on-demand gives users the freedom to view the content of courses, tutorials, etc. when they want and on their preferred device. Video-on-demand can also be used internally by member institutions for employee training modules and internal communication.

When a user interacts with the Kaltura platform through a member institution's account, Kaltura collects the user's personal information. Examples of activities where a user might interact with the Kaltura Platform include:

- Viewing videos on the Internet provided from a Kaltura Platform account
- Uploading content to the Kaltura Platform
- Appearing on videos hosted on the Kaltura Platform
- Using applications connected to the Kaltura Platform, logging in to applications connected to the Kaltura platform, or downloading a Kaltura mobile application
- Interacting with the Kaltura APIs
- Opening a free trial account or other partner account for the Kaltura Platform
- Downloading a Kaltura application from sites like the Apple App Store and Google Play

- Interacting with Kaltura on behalf of a member institution (for example, a business administrator or technical contact may provide contact information to Kaltura for service or billing purposes)

The personal information that is collected in the Kaltura platform is controlled by the individual member institutions. As such, each member institution is responsible for the protection of the personal information pertaining to their users.

2. What is the scope of the PIA?

This PIA addresses the collection, use, disclosure, storage, access, and security of personal information in the Kaltura Video Cloud Platform. BCNET has completed a PIA on AWS (Canada) which can be referred to for additional information.

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

<Member institutions should ensure the information elements listed below are accurate and complete for their use of the system or program.>

When using the Kaltura Platform as a User through an Account Owner's account, the following categories of Personal Information may be collected and processed:

- Information the user uploads – If the user is authorized to upload videos to a Kaltura account, the video content and metadata that is uploaded may potentially include Personal Information about the user and/or other third parties.
- Information provided by the Account Owner – The Account Owner may enter or create Personal Information about users on its account. For example, a user's information may be included in the Account Owner's authorized User lists, access permissions, or in audio or video content and/or metadata.
- Traffic information, instructions, and activity on the Kaltura Platform – When a user interact with the Kaltura Platform, the system collects the traffic information needed to deliver the user's actions and instructions over the Internet. Personal Information about the user may include IP addresses, and URLs used to deliver content to the user, and the Kaltura Platform may collect other system information such as MAC addresses to allow the system to recognize devices. The Kaltura Platform uses cookies to remember preferences and/or support the use of digital rights management systems.
- Passwords and login credentials – When users log in to the Kaltura Platform, Kaltura collects the user IDs and passwords used in order to access the Kaltura Platform. When the user logs in to other Account Owner systems that are connected to the Kaltura Platform (such as single sign-on systems or third-party portals), depending on the configuration of those systems, the Kaltura Platform may receive user login credentials or an anonymous identifier or token.

3.1 Did you list personal information in question 3?

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.

Yes.

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

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

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

5. Collection, use and disclosure

<Member Institutions may customize the table below to ensure it accurately reflects their collection, use and disclosure of personal information.>

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**
Step 1: Personal information is collected directly from students and faculty by the member institution at the time of the establishment of appropriate access credentials (LMS or other specific institution program/system of record)	Collection	26(c)	
Step 2: Students and faculty within each member institution securely log into Kaltura using the above noted credentials (passed securely from their LMS or system of record into Kaltura)	Use	32(a)	
Step 3: The personal information contained in the credentials authenticate the user and enable the individual to use the Kaltura platform products/features	Use	32(a)	
Step 4: Kaltura collects personal information when users interact with the Kaltura platform, e.g., viewing videos, uploading content, appearing in videos, using applications connected to the Kaltura planform, etc.	Use	32(a)	
Step 5: Kaltura may collect and process personal information when a user uses the Kaltura platform through a member institution's account, e.g., information that the user uploads or records, user account information that is provided by the	Use	32(a)	

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
member institution's authorized users, traffic information, passwords, and login credentials.			

6. Collection Notice

<Member Institutions are responsible for ensuring the appropriate notification is in place prior to the collection of personal information.>

PART 3: STORING PERSONAL INFORMATION

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

Yes.

- 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)?

No.

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

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

After you answer this question go to Part 5.

N/A

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada.

<**Note to Member Institutions:** Kaltura's Video Cloud Platform is hosted on AWS (Canada). Member Institutions must configure their access controls in Kaltura to ensure that personal information is stored only in Canada. Otherwise, Part 4 of this PIA must be completed.>

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

N/A

- 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.

N/A

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

N/A

- If yes, describe the contractual measures related to your initiative.

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

N/A

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

N/A

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

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.
N/A					

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

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

Yes.

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

No.

- If yes, you may want to append the security assessment to this PIA. Go to question 19
- If no, go to question 18

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

BCNET Member Institutions

<Member Institutions are responsible for ensuring the technical security of all data in their custody and/or control (including data at rest or in transit) and must meet applicable technical security standards required by their organization.>

Kaltura – Physical Security

Section 21, Section 15(1)(l)

Section 21, Section 15(1)(l)

For more information on AWS Data Center controls, see the BCNET PIA on AWS (Canada) or https://aws.amazon.com/compliance/data-center/controls/

Kaltura – Technical Security

Section 21, Section 15(1)(l)

19. Controlling and tracking access

<Member institutions are responsible for controlling and tracking access to information for their organizations using least privilege principles.>

Strategy	
We only allow employees in certain roles access to information	Yes or No
Employees that need standing or recurring access to personal information must be approved by executive lead	Yes or No
We use audit logs to see who accesses a file and when	Yes or No
Describe any additional controls: Section 21, Section 15(1)(l)	

PART 6: ACCURACY, CORRECTION AND RETENTION

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

<Member Institutions are responsible for ensuring personal information is accurate and complete.>

21. 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.

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

<Type "yes" or "no" to indicate your response. Member Institutions are responsible for ensuring a process is in place to correct personal information.>

21.2 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?

<Type "yes" or "no" to indicate your response. Member Institutions are responsible for ensuring a process is in place to document the request to correct or annotate the record.>

21.3 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?

<Type "yes" or "no" to indicate your response. Member Institutions are responsible for notifying other public bodies or third parties of the request for correction.>

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

Yes, Member Institutions may assess and grade videos created by students as part of their course work.

- If yes, go to question 23
- If no, skip ahead to Part 7

23. 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.

<Type "yes" or "no" to indicate your response. BCNET member institutions are responsible for having an information schedule in place.>

- If no, describe how you will ensure 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

24. Does your initiative involve an information sharing agreement?

No.

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

No.

PART 8: ADDITIONAL RISKS

26. Risk response

Possible risk	Response
Risk 1: Unauthorized individuals at BCNET or member institutions could access personal information and use or disclose it for personal purposes.	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 principles, permission restrictions, access controls, and monitoring.
Risk 2: Unauthorized individuals at Kaltura could access personal information and use or disclose it for personal purposes.	Employees, agents, and third-party service providers are required to act in a manner consistent with Kaltura's privacy policy. Kaltura ensures that the recipients of personal information provide appropriate safeguards, including by entering into data processing agreements incorporating, where required, standard contractual clauses or alternative mechanisms for the transfer of personal data.
Risk 3: Inherent risk in Kaltura's use of third-party service providers	Kaltura does not share information, including personal information, with any third parties other than their partners except in the limited circumstances. Kaltura's partners do not have permission to use personal information for any purpose other than to provide to Kaltura the services they require to serve their Account Owners.
Risk 4: User's personal information is compromised during transmission from member institution to Kaltura cloud	Section 15(1)(l)
Risk 5: Security breach at Kaltura	Kaltura follows an Incident Response Policy, which defines incidents, responsibilities, immediate responses and reporting chains, investigations, and communication plans.

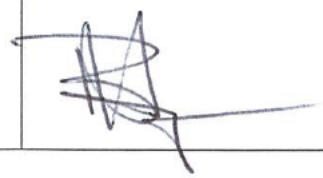
PART 9: SIGNATURES

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	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Bev Hooper Hooper Access and Privacy Consulting Ltd.		April 12/23

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
Head of public body, or designate Only required if personal information is involved	Dean Crawford Director, Shared Systems and Technology	Dean Crawford	17 April, 2023