CAPILANO UNIVERSITY

PRIVACY IMPACT ASSESSMENT (PIA)

ProctorU – Meazure Learning

A. GENERAL INFORMATION			
PIA File Number:	PIA-25-05		
Department/Faculty:	Faculty of Business and Professional Studies		
Office/School:	The School of Legal Studies and Applied Behavioural Analysis		
Project Manager / PIA Drafter:	Dr. Brit Paris, PhD	**Title:**	Director, Teaching and Learning
Email:	britparis@capilanou.ca	**Phone:**	604-983-7540 local 7540
PIA Drafter:	Polina Makedonskaya		
Privacy Officer:	Jacquetta Goy		
Email:	jacquettagoy@capilanou.ca	**Phone:**	604-984-4915
Related PIAs, if any:	None		

1. Description of the Initiative:

To the best of your ability, please provide a detailed description of the initiative, its main objectives, the context in which it functions, the business need for it, and how the objective will meet that need.

Capilano University is employing ProctorU, a third-party remote proctoring service, to enable secure administration of online exams. The objective is to uphold academic integrity in remote learning environments by monitoring students through webcam, microphone, screen activity, and AI-based flagging of suspicious behaviors.

ProctorU will be using proprietary or third-party software, webcams and/or live persons to ascertain whether the examinee complies with the requirements of Capilano University during the exam and to use industry-accepted processes to authenticate that the named examinee is the individual taking the exam. Designated Capilano University administrators will be given access to on-demand data reports for examinees scheduled and completed exams. This is essential due to the increase in online and hybrid learning formats.

2. Scope of this PIA:

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA? Describe what parts of the initiative you are assessing. If a project will be implemented in phases, be sure to explain which phase is being documented in the PIA. Subsequent updates or amendments can be made for other phases as they are developed

This PIA covers the use of ProctorU for remote proctoring of online examinations by Capilano University students. It includes initial phases of implementation in select departments (Legal Studies and Applied Behavioural Analysis).

3. Elements of Personal Information:

To the best of your ability, please list all the data or information that will be collected, used, processed, stored, disclosed, or accessed as part of the initiative (not just the personal information). This will allow the Privacy Officer to assess all the information involved against what FIPPA considers to be personal information. For example, if conducting a survey, list the different elements of the information being collected as well as a summary of the other types of questions.

ProctorU proctoring service collects, creates and stores a wide variety of personal information that will/may include:

- First and last name,
- Address,
- Institution name,
- Phone number,
- Student number,
- Government-issued photo ID
- IP address
- Browser and system configurations
- Username,
- Student images,
- Password,
- Email address,
- Real-time video and audio viewing,
- Notes regarding student's behaviour during the exam,
- Visual identification (photo matching),
- Keystroke and mouse activity,
- Exam responses,
- Viewing student’s computer screens and systems,
- 360° testing environment scanning when requested,
- Real-time monitoring of all applications, windows, and monitors that are being utilized on student’s computer during the exam, to prevent unauthorized viewing of content during the exam.

ProctorU requires a picture ID before the test starts, but ProctorU destroys images of ID’s in their system after 7 days.

4. Sensitive Personal Information:

	YES	NO
Will sensitive personal information be collected, stored, used, or disclosed as part of this initiative?	☒	☐
Will the sensitive personal information be stored outside of Canada? If so, please fill out Section E.	☒	☐

Sensitive personal information is not defined in FIPPA. Some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is *improperly collected, used, or disclosed. Personal information may be considered sensitive depending on the type of information and the context in which it is collected, used, disclosed, or stored.*

Examples of sensitive personal information may include:

- *Personal health information*
- *Genetic and biometric data*
- *Personal financial information*
- *Geolocation data*
- *Criminal records*
- *Counselling records*
- *HR records*
- *Payroll records*

Sensitive personal information includes biometric data (facial image and video), government-issued ID, and potentially geolocation metadata. ProctorU stores data in cloud servers located in the United States.

The ProctorU Platform only collects information that's necessary to verify a test-taker's identity, like name, email address, or educational institution. ProctorU requires a picture ID before the test starts. According to Meazure Learning, ProctorU securely destroys any images in their system after 7 days.

B. COLLECTION & USE OF PERSONAL INFORMATION

1. Description (either a narrative or flow chart) of the linkages and flows of personal information collected, used, and/or disclosed:

Provide a step-by-step description from beginning to end showing how personal information is collected, circulated, processed, stored, and used, as part of this initiative, and if it is disclosed to any third parties. Please include all formats (paper and electronic) from creation or collection until final disposition. This can be demonstrated either via a flow chart, or a numbered list.

Please see below.

PERSONAL INFORMATION FLOW TABLE:

Description/Purpose		**Type** *(Collection, Use, Retention or Disclosure)*	**FIPPA Authority**
1.	Student accesses online exam through the LMS, ProctorU extension or app is launched, and student is required to verify identity using government-issued photo ID.	Collection, Use, Disclosure	26(c), 32(a), 33.1(1)(b)
2.	ProctorU uses a third-party processor to handle payments for their services but does not store student's credit card information itself.	Use, Disclosure	32(a), 33.1(1)(b)
3.	System checks for active webcams, microphones, and screen-sharing permissions.	Use	32(a)
4.	ProctorU begins live monitoring during the exam, recording video, audio, and screen activity.	Collection, Use	26(c), 32(a)
5.	ProctorU may flag behavior for review and generate an incident report.	Use	32(a)

6.	Once an exam session ends, the proctoring session data is stored in US-based encrypted servers (AES 256). The screen recordings and webcam audio/video are accessible to the institution or organization for a period determined by the institution. It is unclear what has been determined as the retention period for Capilano University, this is addressed in the Risk Mitigation Table.	Storage	31
7.	Access to flagged sessions is limited to authorized Capilano University staff for academic integrity review. It is unclear who that is at Capilano, at the moment, this is addressed in the Risk Mitigation Table.	Disclosure	33.1(1)(b)
8.	The default retention period for exam session recordings is one year, per NIST 800-88 guidelines, after which they are automatically deleted. This period can be shortened if requested by the institution. The images of student IDs are securely destroyed after seven days.	Storage	31

2. Collection Notification:
Will you be collecting personal information directly from the individual the information is about?
If so, please see below the sample of the collection notice you're required to provide.
Please indicate the location and placement of the notice (e.g., a form).

Example of collection notice:
"Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA), as the information relates directly to and is necessary for an operating program or activity of the University. Questions about the collection of this information may be directed to the Privacy Officer at privacy@capilanou.ca".

The following notice will appear (currently don't have one, and this is addressed in the Risk Mitigation Table) on the exam launch page and/or in course outlines for courses that use ProctorU:
"Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA), as the information relates directly to and is necessary for an operating program or activity of the University. Questions about the collection of this information may be directed to the Privacy Officer at privacy@capilanou.ca."

3. Direct / Indirect Collection (Section 27(1)):
If, for the purposes of the initiative, the personal information will only be collected directly from the individual the information is about, please identify when and where that collection will take place. If the initiative will collect personal information indirectly (e.g., website cookies, public database) please provide details.

Direct collection of personal information occurs when ProctorU gathers information from the test-taker, such as during identity verification or when recording exam sessions. Indirect data such as IP address and system settings are also collected through automated system scans.

4. Authorization for Collection (Section 26):
Please describe why it is necessary to collect personal information, in order to fulfill the identified purpose(s) of the initiative. The collection of personal information should be limited only to those information items that are strictly necessary.

Collection is necessary to ensure academic integrity, verify student identity, monitor the exam environment, and investigate potential cheating behaviors.

5. Authorization for Use (Section 32):
List the uses of personal information:

- Identity verification
- Live or recorded proctoring of online exams
- Academic integrity investigations
- Flagging and reporting suspicious activity
- Incident resolution and appeals process

The primary use of personal information is to verify the identity of the test-taker and monitor the exam session. ProctorU uses the collected information to ensure the security and integrity of the exam process.

Please respond to the following statements:	**YES**	**NO**
Will the information be used only for the purpose(s) for which it was obtained?	X	
To prevent the use of collected personal information for secondary purposes, safeguards are /will be in place on access to both electronic and hard copies.	X	
Data will not be anonymized or aggregated at any point for planning or reporting purposes.		X

6. Marketing Uses:
Please identify any anticipated uses of personal information for marketing purposes. All marketing via commercial electronic message (email, text message, etc.) must comply with the rules of Canada's Anti-Spam Law (CASL). All marketing via telephone must comply with the National Do Not Call List (DNCL) Rules.

There will be no use of personal information for marketing purposes.

C. ACCESS, DISCLOSURE & STORAGE OF PERSONAL INFORMATION

1. Access to Personal Information:
Identify who will have access to personal information as a result of this project (e.g., teams, roles, or individuals, including any third party service providers, contractors, etc.), what type of personal information will they be privy to, the purposes for which they will have access, and how information will be made available to them/user access assigned?

Who?	Type of PI?	Purpose(s)?	How?
- ProctorU personnel	- Identity details, audio/video recordings, exam behaviors, flags, reports	- Monitoring, academic integrity investigations, decision-making	- Access through secure ProctorU dashboard with role-based permissions and audit trails
- Capilano University instructors	flags, reports	academic integrity investigations, decision-making	Access through secure ProctorU dashboard with role-based permissions. However, there are no

			audit trails, which is also addressed within the Risk Mitigation Table.
- Academic integrity staff	flags, reports	academic integrity investigations, decision-making	Access through secure ProctorU dashboard with role-based permissions. However, there are no audit trails, which is also addressed within the Risk Mitigation Table.

Please respond to the following statements:	YES	NO	N/A
Access to personal information is based on a need-to-know basis.	X		
If you're utilizing third party for storage/processing of personal information, do you have controls in place to monitor access?		X	
Is there an ongoing audit process that can track access (e.g., who accessed and/or updated personal information records and when)?		X	

Provide details about how you will track and monitor access to personal information (e.g., audit trails or physical sign-in and sign-out of files)?

On ProctorU, proctors cannot access students' computer files without their knowledge. Everything the proctors do will be shown on students' screen and proctors cannot perform any "hidden" actions. This access is only granted with students' explicit permission and after students clicked a button to confirm.

Proctors have the ability to view the screen and utilize the mouse and keyboard as if they were sitting next to the student. Once the exam starts, the proctor will monitor everything on the students' computer screen but can no longer utilize students' mouse and keyboard.

During the entire process, a chat box is running on students' computer, and students can see what permissions the proctor currently has at any time. The entire chat session log is saved, including a permanent record of what actions the proctor took while accessing students' computer.

In terms of access of files at Capilano University, there isn't a process set out, at the moment, with established persons holding admin controls and monitoring access, this is addressed within the Risk Mitigation Table.

Is there a defined approval process in place for granting access? Is there a person (title) who will authorize and/or revoke access? How/how often will the approval authorities be reviewed to ensure they are current?

No, currently, there is not a defined approval process in place, this is recorded within the Risk Mitigation Table.

Identify who (title) has the authority to add, change or delete personal information. Is this power limited to a specific individual(s) or anyone with access can add, change, or delete personal information?

Role-based access restricts editing/deletion of personal information to authorized personnel only. However, currently, there is not a defined approval process in place, this is recorded within the Risk Mitigation Table.

What controls are in place to prevent unauthorized access to personal information (e.g., locked cabinets, key cards, passwords)?

Meazure Learning's infrastructure is built upon Amazon Web Services (AWS) for all application hosting and data storage. AWS operate in the United States and feature industry-leading digital and physical security. AES 256 bit encryption for data-at-rest and TLS 1.2 connections for data-in-transit.

At Capilano University, only authorized users can access ProctorU portal/dashboard. However, at the time of writing this PIA, it isn't clear how access is granted and/or monitored. This is mentioned within the Risk Mitigation Table.

If there is a third party or a service provider involved in the initiative, what access controls are/will be put in place? (to make sure the data/information we store with them is secure)

Meazure Learning has completed a SOC 2 Type 2 Report for the ProctorU Online Proctoring platform, where behavioural standards of personnel are outlined as follows:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an onboarding agreement form indicating they have been given access to the Meazure Learning Handbook and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employment agreement.

2. Disclosure of Personal Information:

Please respond to the following statements:	**YES**	**NO**	**N/A**
Will the personal information be disclosed internally to an employee, only when the information is necessary for the performance of the duties of that employee?	X		
Will the personal information be disclosed externally to a service provider, only when the information is necessary for the delivery of the contracted services?	X		

3. Storage of Personal Information:

Describe exactly where and how will the personal information be stored.

WHERE? *e.g., in Canada or outside Canada? Provide details.*	In United States (AWS cloud storage operated by ProctorU / Meazure Learning)
HOW/WHAT FORMAT? *e.g., electronic, and on-premise servers or data centres.*	Encrypted electronic files, accessible through secure ProctorU platform

D. ACCURACY, CORRECTION, RETENTION & DISPOSAL OF PERSONAL INFORMATION

1. Decisions Affecting Individuals (Section 28):

	YES	**NO**
As part of this initiative, an individual's personal information will be used to make a decision that directly affects the individual.	X	

Examples of using personal information to make decisions include but are not limited to:

- *Using a person's employment history to decide whether they can move forward in a job competition*
- *Using a student's exam results to pass them in a course*
- *Using a student's information to approve them for financial aid*

If "yes", please explain how and why that will be done:

Exam integrity decisions are made based on the collected data (e.g., academic misconduct).

If answered "yes" above, please respond to the following statement:

Public bodies are required to keep personal information for a minimum of one year after it is used to make a decision that affects the individual.
Please describe how/what steps will be taken to 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.

As per Section 31 of the FOIPPA Act, 31 "If an individual's personal information (a)is in the custody or under the control of a public body, and (b)is used by or on behalf of the public body to make a decision that directly affects the individual, the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information." Retention needs to meet FIPPA's one-year minimum for decisions affecting individuals, in case a student might want to appeal the decision that affected them. This is mentioned within the Risk Mitigation Table.

The ProctorU Platform only uses the data captured during test sessions to conduct online proctoring. As their Privacy Policy states: ProctorU does not use any test-taker's personal information for any purpose other than for facilitating the proctoring of online exams.

Once an exam session ends, the proctoring session data is stored in US-based encrypted servers (AES 256). The screen recordings and webcam audio/video are accessible to the institution or organization for a period determined by the institution or organization but are automatically deleted, per NIST 800-88 guidelines, after one year..

The information and recordings belong to the testing institution or organization and ProctorU acts as a service provider. ProctorU do not own the data, the University does. ProctorU doesn't sell or otherwise monetize any data from test-takers and never markets to test-takers nor allow any of their service providers to do so.

2. Accuracy of Personal Information (Section 28):
If an individual's personal information is used to make a decision that directly affects that individual, please explain the efforts that will be made to ensure that the personal information is accurate and complete (e.g., collecting the information directly from the individual, verifying the information with the individual prior to recording it, etc.).

Data is collected directly from the student. Students verify identity at start of session; accuracy is supported by video verification.

3. Correction of Personal Information (Section 29):
Please describe how an individual can update or correct their personal information. Describe the process, this could be processes where an individual can ask for system administrators to make changes on their behalf.

Students may request correction of personal information by contacting the Privacy Officer or Academic Integrity Office. ProctorU will update data upon validated requests. If corrections cannot be made, annotations will be added.

If it is not possible to update or correct the information (for physical, procedural, or other reasons) please explain how it will be annotated to reflect that the correction was requested but not made.

N/A

Where personal information is disclosed to third parties, how will the third parties be notified of the update, correction, or annotation?

ProctorU will update data upon validated requests. If corrections cannot be made, annotations will be added.

To be completed by the Privacy Officer:

s. 29	Right to request correction of personal information	**YES**	**NO**	**N/A**
	Are there procedures in place to enable an individual to request/review a copy of their own personal information?	X		
(1), (2)	Are there procedures in place to correct or annotate an individual's personal information if requested, including the source that was used to update the file?	X		
(3)	Is there a process in place to notify third parties where a correction is requested?	X		
	Do controls and procedures exist for the authority to add, change, or delete personal information?	X		
	Are reasonable efforts taken to ensure that personal information is accurate and complete if being used to make a decision that directly affects the individual?	X		

4. Records Retention (Section 31):

Personal information collected, used, and/or disclosed as part of this initiative must have an assigned retention period. Is there a defined retention period assigned? How long the records will be retained for?

ProctorU retains recordings and metadata for up to 1 year. CapU should retain the decision logs for at least 1 year, this is mentioned within the Risk Mitigation Table.

5. Disposal

How are the records containing personal information disposed of?
Who (title) is in charge of disposing them?

ProctorU disposes of data via secure deletion protocols. Oversight is ensured by ProctorU's Compliance Officer. However, It's not clear for how long Capilano University is storing test taker's data, or whether any of the 35 users can download it off the ProctorU dashboard, this risk is discussed within the Risk Mitigation Table below.

E. ACCESS, DISCLOSURE, STORAGE, RETENTION & DISPOSAL OF SENSITIVE PERSONAL INFORMATION OUTSIDE OF CANADA

Complete this section only if you are disclosing or storing sensitive personal information outside of Canada. Please contact the Privacy Officer for assistance.

To be completed by the Privacy Officer:

	YES	NO
Is it necessary to fill out section E. of this PIA?	X	

1. Is Sensitive Personal Information Disclosed Outside of Canada under FIPPA section 33(2)(f)?
FIPPA Section 33(2)(f) states that a public body may disclose personal information if the information is made available to the public under an enactment that authorizes or requires the information to be made public.

Disclosure is necessary for delivery of contracted services.

Please respond to the following statements:	YES	NO	N/A
Is access to sensitive personal information based on a need-to-know basis?	X		
If you're utilizing third party for storage/processing of sensitive personal information, do you have controls in place to monitor access?		X	
Is there an ongoing audit process that can track access (e.g., who accessed and/or updated sensitive personal information records and when)?		X	

2. Access to Sensitive Personal Information:
Identify who will have access to sensitive personal information as a result of this project (e.g., teams, roles, or individuals, including any third party service providers, contractors, etc.), what type of sensitive personal information will they be privy to, the purposes for which they will have access, and how information will be made available to them/user access assigned?

Who?	Type of PI?	Purpose(s)?	How?
ProctorU (Meazure Learning) staff	Video/audio recordings, facial image (biometric), government-issued ID, geolocation metadata	Identity verification, exam monitoring, academic integrity reviews	Through secure ProctorU platforms with encrypted transmission and role-based access
Capilano University instructors	flags, reports	academic integrity investigations, decision-making	Access through secure ProctorU dashboard with role-based permissions. However, there are no audit trails, which is also addressed within the Risk Mitigation Table.
Academic integrity staff	flags, reports	academic integrity investigations, decision-making	Access through secure ProctorU dashboard with role-based permissions. However, there are no audit trails, which is also addressed within the Risk Mitigation Table.

Provide details about how you will track and monitor access to sensitive personal information (e.g., audit trails or physical sign-in and sign-out of files)?

ProctorU holds a SOC2 Type II certification, reflecting a third-party audit of their internal controls about data security, storage, and management.

On ProctorU, proctors cannot access students’ computer files without their knowledge. Everything the proctors do will be shown on students’ screen and proctors cannot perform any "hidden" actions. This access is only granted with students’ explicit permission and after students clicked a button to confirm.

Proctors have the ability to view the screen and utilize the mouse and keyboard as if they were sitting next to the student. Once the exam starts, the proctor will monitor everything on the students’ computer screen but can no longer utilize students’ mouse and keyboard.

During the entire process, a chat box is running on students’ computer, and students can see what permissions the proctor currently has at any time. The entire chat session log is saved, including a permanent record of what actions the proctor took while accessing students’ computer.

In terms of access of files at Capilano University, there isn’t a process set out, at the moment, with established persons holding admin controls and monitoring access. (on risk mitigation schedule)

Is there a defined approval process in place for granting access? Is there a person (title) who will authorize and/or revoke access? How/how often will the approval authorities be reviewed to ensure they are current?

No, currently, there is not a defined approval process in place, this is recorded within the Risk Mitigation Table.

Identify who (title) has the authority to add, change or delete sensitive personal information. Is this power limited to a specific individual(s) or anyone with access can add, change, or delete personal information?

Role-based access restricts editing/deletion of personal information to authorized personnel only. However, currently, there is not a defined approval process in place, this is recorded within the Risk Mitigation Table.

What controls are in place to prevent unauthorized access to sensitive personal information (e.g., locked cabinets, key cards, passwords)?

Meazure Learning's infrastructure is built upon Amazon Web Services (AWS) for all application hosting and data storage. AWS operate in the United States and feature industry-leading digital and physical security. AES 256 bit encryption for data-at-rest and TLS 1.2 connections for data-in-transit.

At Capilano University, only authorized users can access ProctorU portal/dashboard. However, at the time of writing this PIA, it isn’t clear how access is granted and/or monitored. This is mentioned within the Risk Mitigation Table.

If there is a third party or a service provider involved in the initiative, what access controls are/will be put in place?

Meazure Learning has completed a SOC 2 Type 2 Report for the ProctorU Online Proctoring platform, where behavioural standards of personnel are outlined as follows:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an onboarding agreement form indicating they have been given access to the Meazure Learning Handbook and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employment agreement.

3. Disclosure of Sensitive Personal Information:

Please respond to the following statements:	**YES**	**NO**	**N/A**
Will the sensitive personal information be disclosed internally to an employee, only when the information is necessary for the performance of the duties of that employee?	X		
Will the information be disclosed externally to a service provider, only when the information is necessary for the delivery of the contracted services?	X		

4. Storage of Sensitive Personal Information:

Please respond to the following question:	**YES**	**NO**
Is the sensitive personal information stored by a Service Provider?	X	

If "yes", fill in the table below:

Name of the Service Provider:	Meazure Learning (ProctorU)
Name of cloud infrastructure and/or platform provider(s) (if applicable):	Amazon Web Services (AWS)
Where is the sensitive personal information stored (including backups):	United States (encrypted cloud storage and backups)

If "no", please provide the details of the disclosure:
Please include to whom is the sensitive personal information disclosed to, and where is it stored:

N/A

5. Records Retention (Section 31):
Personal information collected, used, and/or disclosed as part of this initiative must have an assigned retention period. Is there a defined retention period assigned? How long the records will be retained for?

ProctorU retains data (recordings, reports) for up to 1 year.

6. Disposal
How are the records containing personal information disposed of?
Who (title) is in charge of disposing them?

ProctorU disposes of data via secure deletion protocols. Oversight is ensured by ProctorU's Compliance Officer. However, It's not clear for how long Capilano University is storing test taker's data, or whether any of the 35 users can download it off the ProctorU dashboard, this risk is discussed within the Risk Mitigation Table below.

F. RISK MANAGEMENT & SECURITY OF PERSONAL INFORMATION

1. Protection of Personal Information (Section 30):
Describe the audit, compliance, and enforcement mechanisms in place to protect against the unauthorized collection, access, use, disclosure, or storage of personal information, in course of the initiative (including for contracted service providers).

ProctorU claims to maintain audit, compliance and enforcement processes. However, there aren't audit trails in place at Capilano University, in regard to this initiative, this is noted in the Risk Mitigation table.

2. Policies and Procedures:

Are there policies and procedures in place for the security of personal information during routine collection, use and disclosure of the information? How will these be communicated to necessary parties, including employees, contractors, and third party service providers?

ProctorU follows internal security policies aligned with SOC 2 compliance. Capilano University has its own policies and procedures regarding the collection and handling of personal information.

3. Training:

Please describe how the conditions detailed in this PIA will be communicated to necessary parties, including employees, contractors, and third party service providers? Will specific guidance or training be provided on how to handle personal information in a privacy protective manner? Where you rely on enterprise-led privacy awareness training alone, please indicate this.

Staff and faculty receive University-wide privacy awareness training. Students are informed of ProctorU's privacy practices and expectations before the proctoring sessions begin.

4. Privacy Incident Reporting:

Please describe how necessary parties, including employees, contractors, and third party service providers, will be made aware of the privacy incident notification process (as documented in the University's "Personal Information Incident Management Procedure").

Capilano Univeristy follows its "Personal Information Incident Management" Procedure.

There are no breach notifications or procedural language included within the contract. The contract includes provisions for Privacy Disclosure, Data Termination and Retention. However, ProctorU isn't contractually obligated to let Capilano University know if it experienced a breach. This risk is further discussed within the Risk Mitigation Table below.

5. Contract:

Has there been a contract drafted or signed? If so, please indicate below and provide a copy to the Privacy Officer.

CapU has a signed agreement with Meazure Learning (ProctorU).

6. Contractual Privacy Provisions:

If the contract has been drafted or signed, does it include privacy provisions?

The contract includes provisions for Privacy Disclosure, Data Termination and Retention. However, ProctorU isn't contractually obligated to let us know if there's a breach. This is mentioned within the Risk Mitigation Table.

7. Risk Reduction:

How will you (and the third party providers, if applicable) reduce the risk of unintentionally collecting personal information?

For example, if you are collecting opinions as part of a public engagement strategy, participants may offer personal information about themselves or others, even though you've instructed them not to. If you do inadvertently receive or collect personal information, what steps will you take to:

- *Destroy it*
- *Return it*
- *Transfer it to the correct recipient*

Students are instructed, by ProctorU, not to share unnecessary personal information during proctored sessions.

8. Digital Tools, Databases, or Information Systems:

A digital tool, database or information system may leave personal information exposed or otherwise vulnerable to security threats.

	YES	NO
Does your initiative involve digital tools, databases, or information systems?	X	

If "yes", please describe:

ProctorU platform, AWS cloud systems, and LMS integration tools are involved.

9. STRA (Security Threat and Risk Assessment):
Security assessments are used on information systems and other digital tools to assess and document security risks, risk ratings and planned risk responses.

	YES	NO
Will a separate security assessment be completed?	X	

If "yes", please describe the assessment to be undertaken, including who will complete the assessment and when it will be completed:

Ankan Garg and Michael Shi on the DTS team have completed the preliminary STRA, based on their review and analysis, they have identified a few **key action items** that need to be addressed to strengthen the security and governance of the ProctorU platform:

1. **SSO Integration**
   - We need to implement **Single Sign-On (SSO)** with Entra ID (Azure AD) to ensure secure authentication and centralized identity management. This will help enforce role-based access control (RBAC) and reduce the risk of unauthorized access.
2. **Quarterly Access Audit/reviews**
   - A **quarterly access review process** should be established to verify that only authorized users retain active accounts and permissions. This will help maintain compliance and support least privilege principles.
3. **Centralized Administration & Governance**
   - Currently, **any user can self-register as an instructor** and gain elevated privileges, including admin-level access. We need to implement centralized administrative controls, approval workflows, and monitoring to prevent privilege escalation and account sprawl.

What they have identified would be considered as High-Risk finding related to identity and access management if Capilano University continues to use this vendor due to abovementioned factors and the sensitive student PII (student photos, exam recording) being collected and retained for one year after exam. However, the DTS team has confirmed with the vendor that this risk can be remediated if Capilano University implements the abovementioned recommendations. In addition, we have confirmed with the Privacy team that the DTS team is fine with minimum one year of data retention for recordings/photos of students as it is mandatory on the vendor side to provide exam investigation service if any exams related concerns.

10. Physical Security Measures:
Please describe the physical security measures established to protect the personal information in all media forms from unauthorized access.

Describe all aspects of the physical environment where personal information is held (e.g., Server(s) location/security, key card access to offices, CCTV surveillance, shredding, locked cabinets, password encryption for computers/laptops, alarm systems, building protection, staff screening, onsite security personnel, etc.).
Capilano University: password encryption for computers/laptops, individual access to the ProctorU dashboard. However, as mentioned in the Risk Mitigation Table, currently, admin access can be granted to any user. ProctorU: AWS datacenters with restricted physical access
11. Technical Security Measures: *Please describe the technical security measures established to protect the personal information in transit, at rest, and while in use.* *Please list the specific technical security measures in place to protect personal information and provide as much detail as possible (e.g., Firewall/virus protection and monitoring, tokenization, web interface features, encryption, backup cycles, scan software, VPN protocols, password protection, audits, role-based access, etc.).*
• Data in transit: TLS encryption • Data at rest: AES-256 encryption • ProctorU admin access • Role-based access control • Firewall, anti-virus, VPN protocols • Regular audit logging and review (ProctorU) • System penetration testing (ProctorU)

To be completed by the Privacy Officer:		
	YES	**NO**
Is there reasonable technical security in place to protect against unauthorized access or disclosure?	X	
Is there reasonable physical security in place to protect against unauthorized access or disclosure?	X	
To be completed by the Privacy Officer:		
11. a) Data-linking Initiative:		
Please respond to the following statements:	**YES**	**NO**
Personal information from one database will be linked or combined with personal information from another database.		X
The purpose for the linkage is different from that for which the personal information in each database was originally obtained or compiled.		X
Data linking will occur between either (i) two or more public bodies or (ii) one or more public bodies and one or more agencies.		X

11. b) Based on the answers above, is this initiative a data-linking program under FIPPA (? *If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.*		
This initiative is not a data-linking program, under FIPPA.		
To be completed by the Privacy Officer:		
12. a) Common or Integrated Program or Activity:		
Please respond to the following statements:	**YES**	**NO**
This initiative involves a program or activity that provides a service (or services) to the public.		X
Those services will be provided through (i) a public body and at least one other public body or agency working collaboratively to provide that service or (ii) one public body working on behalf of one or more other public bodies or agencies.		X
There is a written agreement signed by the head of each public body and agency through which the services of the program or activity are provided.		X
12. b) Based on the answers above, is this initiative a common or integrated program or activity? *Under section FIPPA 69(5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.*		
No, this is not common or integrated program or initiative.		
To be completed by the Privacy Officer:		
13. a) Project with High Visibility/Public Interest, and/or Audio/Video Surveillance:		
Please respond to the following statements:	**YES**	**NO**
This initiative involves installation or use of audio recording equipment.		X
This initiative involves installation or use of video recording equipment.	X	
This initiative involves the use of new technology which might be perceived as being privacy intrusive. For example, the use of biometrics or facial recognition.		X
This initiative involves a program or activity that may generate high visibility or public interest.		X
13. b) Based on the answers above, does this initiative qualify as a project with high visibility/public interest, and/or does it include audio or video surveillance? *If so, the completed PIA should be sent to the OIPC for review and comment.*		
This initiative does not qualify as a project with high visibility/public interest. There is an element of video recording involved, however not for video surveillance.		

Risk Mitigation Table

14. Privacy Risks:

Use the table below to outline the risk associated with unauthorized collection, use, disclosure, or storage of personal information. Include a description of the potential impacts (consider both individuals and any broader impact if relevant) and then rate the likelihood and the level of risk (use a simple low, medium & high scale). For each privacy risk identified describe the current controls and those that will be put in place as part of the initiative. Controls may include contractual, technical, security, administrative and/or policy measures. Where the level of risk is still significant describe the additional controls that need to be implemented.

Area of Risk Exposure	Area of Privacy	Likelihood	Impact	Level of Privacy Risk	Mitigation Strategy / Actions	Responsibility for Mitigation Actions	Timeline for Mitigation Actions
There are no privacy incident/breach notifications or procedural language included within the contract. The contract includes provisions for Privacy Disclosure, Data Termination and Retention. However, ProctorU isn't contractually obligated to let Capilano University know if it experienced a breach.	BREACH / CONTRACT	High	High	High	Any breach within ProctorU should be reported to Capilano University and managed jointly. There should also be a stand-alone Privacy Schedule added onto the contract, if the University decides to continue use of services provided by ProctorU. However, it isn't clear who is responsible for maintaining the contract, which needs to be addressed.		
According to ProctorU, it disposes of data via secure deletion protocols, and oversight is ensured by ProctorU's Compliance Officer. However, It's not clear for how long Capilano University is storing test taker's data, or whether any of the 35 current users can download the data off the ProctorU dashboard.	DISPOSAL / STORAGE	High	High	High	To limit the possibilities of a privacy incident/breach, there should be better control of admin access, audit trails and limitations put in place, regarding downloading of data. Also, there should be a retention period of at least one year set in place, as mentioned below.		

Once an exam session ends, the proctoring session data is stored in US-based encrypted servers (AES 256). The screen recordings and webcam audio/video are accessible to the institution or organization for a period determined by the institution. It is unclear what has been determined as the retention period for Capilano University.	STORAGE	High	High	High	As per Section 31 of the FOIPPA Act, 31 “If an individual's personal information (a)is in the custody or under the control of a public body, and (b)is used by or on behalf of the public body to make a decision that directly affects the individual, the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.” So, we must store the information for one year, in case a student might want to appeal the decision that affected them.		
Access to personal information is through secure ProctorU dashboard with role-based permissions. However, there isn’t a process set out, at the moment, with established persons holding admin controls and monitoring access. Currently, admin access can be granted to any user. Also, there are no audit trails or ongoing audit process (e.g., who accessed and/or updated personal information records and when).	ACCESS	High	High	High	There should be a defined approval process in place for granting access, with a person (title) responsible for authorizing and/or revoking access. Also, role-based access restricts editing/deletion of personal information to authorized personnel only. In addition, approval authorities should be reviewed on a regular basis, to ensure they are current.		

Currently, it appears that Capilano University doesn’t have the collection notice in place, on the exam launch page and/or in course outlines for courses that use ProctorU.	NOTICE	Med	Med	Med	There should be following collection notice added: *"Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA), as the information relates directly to and is necessary for an operating program or activity of the University. Questions about the collection of this information may be directed to the Privacy Officer at privacy@capilanou.ca."*		

G. PERSONAL INFORMATION BANKS & INFORMATION SHARING AGREEMENTS

To be completed by the Privacy Officer:

1. Personal Information Bank (PIB)

PIB is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned only to that individual. A personal information bank can be a simple list of personal information. Personal information banks contain personal information that is:

- *Linked to an identifiable individual*
- *Organized and capable of being retrieved by a personal identifier*
- *Normally compiled for a single purpose*

	YES	NO
Will this initiative result in the creation of a personal information bank?		X

If "yes", fill in the table below:

Describe the type of information in the bank:	N/A
List any other ministries, agencies, public bodies, or organizations involved:	N/A
Record the Business contact title and phone number for person responsible for managing the PIB:	N/A

To be completed by the Privacy Officer:

2. Information Sharing Agreements (ISAs) & Systematic or Repetitious Disclosure/Exchanges

Public bodies enter Information Sharing Agreements (ISAs) when there is a regular and systematic exchange of personal information between public sector organizations or between a public sector organization and an external agency. ISAs document the terms and conditions of the exchange of personal information in compliance with the provisions of the Act and any other applicable legislation. ISAs help to ensure privacy protection where personal information is exchanged.

	YES	NO
Does this initiative involve an Information Sharing Agreement?		X
Is the ISA added as an appendix to this PIA?		X

To be completed by the Privacy Officer:		
	YES	**NO**
Does the initiative involve a regular and systematic exchange of personal information on a regular or ongoing basis between public bodies and/or external agency(ies)?	X	
If "yes", please explain. *For example: the initiative will involve systematic collection and disclosure of personal information, in order for the department to provide specific services to students.*		
To allow ProctorU to deliver secure remote proctoring services on behalf of CapU while ensuring compliance with applicable privacy legislation and institutional policies.		

INFORMATION SHARING AGREEMENT SUPPLEMENT

To be completed by the Privacy Officer:
Description of ISA:
Service Agreement between ProctorU and Capilano University
Name(s) of third parties involved:
ProctorU
Business contact title and phone number for person responsible for maintaining the ISA:
Not available at the moment, and this is mentioned within the Risk Mitigation Table above.
ISA start date:
February 27, 2017
ISA end date:
The Agreement is effective as of the Effective Date and may be cancelled at any time and for any reason by either party with thirty (30) calendar days written notice to the other party.

H. SIGNATURES

Project Manager Signature:	
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.	
Title:	**Director, Teaching and Learning**
Name:	**Brit Paris**
Date:	**October 29, 2025**
Signature:	

Privacy Officer Comments & Signature:	
Comments:	Based on the identified risks within this PIA,it has been decided by the ETLE Committee to stop any further use of ProctorU by the University.
Name:	**Jacquetta Goy**
Date:	**29 October 2025**
Signature:	

Additional Signatures (if required):	
Title:	
Name:	
Date:	
Signature:	

I. APPENDICES

	YES	NO
Will this PIA include appendices?		X

If "yes", please list them, and combine them with the PDF of this PIA.
For example: excerpt from a contract/privacy schedule, third party provider policies, blank questionnaire/examples of PI being collected during the course of the initiative.

The following documents were reviewed as part of completion of this PIA:
Meazure Learning SOC 2 Type 2 Report
The Service Agreement with Capilano University
ProctorU Technical Security Overview