Privacy Impact Assessment for Non-Ministry Public Bodies

Table of Contents

Before you start 1
PART 1: GENERAL INFORMATION 1
PART 2: COLLECTION, USE AND DISCLOSURE 4
PART 3: STORING PERSONAL INFORMATION 5
PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 6
PART 5: SECURITY OF PERSONAL INFORMATION 9
PART 6: ACCURACY, CORRECTION AND RETENTION 11
PART 7: AGREEMENTS AND INFORMATION BANKS 13
PART 8: ADDITIONAL RISKS 14
PART 9: SIGNATURES 15

Use this privacy impact assessment (PIA) template if you work for or a service provider to a non-ministry public body in B.C. and are starting a new initiative or significantly changing an existing initiative.

Before you start

- If you are in a non-ministry public body, you may use this template to document a PIA. This template leads you through a complete PIA but you are welcome to use another template or method for documenting your PIA
- An initiative is an enactment, system, project, program or activity
- Find information on the PIA review process and question-by-question guidance.
- If you have any questions, email Privacy.Helpline@gov.bc.ca or phone 250 356-1851

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Electude
Organization:	Vancouver Island University
Branch or unit:	Automotive

Your name and title:	Jacqueline Kirkham
Your work phone:	250.753.3245 Local:2916
Your email:	Jacqueline.Kirkham@viu.ca
Initiative Lead name and title:	Daryl Pushor, Instructor, Automotive Service Technician
Initiative Lead phone:	250.740.6658 Local: 6658
Initiative Lead email:	Daryl.Pushor@viu.ca
Privacy Officer:	William Boyte, General Counsel and University Secretary
Privacy Officer phone:	250.740.6564 Local: 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:
D2L Brightspace PIA - BCNET

1. What is the initiative?

Electude is an online learning platform designed to help students in trades and technical programs learn and retain information through gamification and highly interactive activities. VIU's Automotive program first adopted Electude to assist students in 2020 when trades learning needed to rapidly shift to online. In the initial roll out of the tool, students had to sign up to Electude and create their own accounts in order to access the interactive learning activities. In 2023, Automotive and CIEL are working with Electude to set up an LTI (learning technology interoperability) Integration which will help streamline the process of accessing these learning materials for students and allow instructors to more seamlessly integrate Electude materials and activities into their curriculum.

2. What is the scope of the PIA?

This PIA covers the Electude platform and the connection between Electude and VIULearn (VIU's Brightspace by D2L Learning Management System). For more information on how VIULearn collects, uses and protects user's data, see the D2L Brightspace PIA.

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

- First and last name of students and employees using the integration
- Email address for all students and employees who access the platform
- This will be the VIULearn email address (for students this email is VIU D2L followed by a randomized string of numbers, for employees this is their VIU username)
- Learning results:
    - collected from the student by using the service: responses, progress, scores and time spent
    - grades, certificates and feedback added by the teacher
- Organization: group membership, assigned learning content and license information
- Log file information IP address, request time, browser type and version, referrer URL.

3.1 Did you list personal information in question 3?

Yes

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

Instructors in Electude can disable the collection of some personal information such as phone number, and address/location information on the Electude site. The department has chosen to allow instructors to enter their phone number if they choose to do so, students do not currently have the option to enter phone number or address/location data in VIU's Electude courses.

The integration setup gives us the ability to limit the amount and type of data sent from the LMS to Electude. We will set up the integration to send the least amount of data possible for the integration to function. In order to allow instructors and students to use the integration fully this will require first name, last name, and email address to be sent from VIULearn to Electude. This information will be visible to the student themselves and to the instructor(s) of the course.

Within VIULearn, the Electude integration will be released only to specific courses. Any course not specifically connected to the LTI Integration will not be able to add Electude Integration Links to their course. This ensures that no one outside of the instructors who are using this tool with their students can accidentally point their students towards Electude.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

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**
Student Account Creation Student accesses an Electude activity or link inside a VIULearn course for the first time. The user must click **I Agree** to accept Electude's Terms of Service and Privacy and Cookie Statement. Once the student click I Accept an account will be created in the Electude LMS. To create the account, Electude collected the student's first name, last name, and email address. When students enter their voucher code (proof of purchase of the course materials) Electude also collects their course membership information.	Collection	26(c)	
Student Activity Completion When students complete activities in Electude, their activity progress, responses, scores and time spent are recorded in Electude and visible to the course instructor(s). Grade information may also be transmitted to VIULearn's Grades tool depending on the settings chosen by the instructor.	Collection and Disclosure	26(c) 33(2)	
All Users Access Log Any time a user accesses the Electude platform	Collection	26(c)	

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
their IP address, browser type and version, request time, and referrer URL are collected			
Instructor Assessment In order to carry out assessment and feedback within Electude, Instructors can access all data collected about student activities and attach feedback which is shared with the individual user and stored on Electude's servers for up to 1 year.	Use Retention	32(a) 31	

6. Collection Notice

Students are first informed about Electude in their list of required materials. The following language will be added to this list to disclose the collection of personal information by this third party service.

"When you use Electude, your personal information, consisting of your full name and VIULearn email address will be collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA). This information will be used for the purpose of creating your account and sharing your activity with your instructor and in order for you to complete required coursework. If you have any questions about the collection or use of your personal information when using Electude, please direct them to fipp@viu.ca. Additionally, you may speak with your instructor."

In addition, instructors talk about Electude with students on the first day of class and can further explain how users' data will be used and protected by VIU during those face to face discussions.

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?

If a user reaches out for technical support from Electude, information they include in their support request including their name and email address will be processed and stored outside of Canada.

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)?

N/A

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

VIU's Electude account information is stored in Canada. Electude uses the following sub processors to process and store data for their service.

SUB PROCESSOR	REGISTERED OFFICE	TYPE OF PROCESSING	COUNTRY OF PROCESSING
[redacted]	[redacted]	[redacted]	Canada
[redacted]	[redacted]	[redacted]	United States
[redacted]	[redacted]	[redacted]	Netherlands
[redacted]	[redacted]	[redacted]	Depends on user location

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

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

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

No

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

The following measures are in place at Electude to prevent unauthorized access to data.

Physical security and continuity

- Personal Data are only processed in a closed, physically secure environment with protection against threats from outside.
- Personal Data are only processed on equipment where measures have been taken to physically secure the equipment and ensure continuity of service.
- A backup is periodically made for the benefit of the continuity of service. This backup is treated confidentially and kept in a closed environment.
- The locations where data are processed are periodically tested, maintained and periodically assessed for safety risks.
- Electude has business continuity plans in which redundant locations are included.
- Personal Data are only stored in [redacted].

s. 15(1)(l)

Network, server and application security and maintenance

- [redacted]
- [redacted]
- [redacted]
- [redacted] s. 15(1)(l)
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Organization

- Electude has a security officer to identify risks with regard to the processing of Personal Data, raise security awareness, monitor resources and take measures to ensure compliance with the information security policy.
- Information security incidents are documented and are used for optimization of the information security policy.
- Electude has set up a process for communication about information security incidents.

Employees

- Employees have signed non-disclosure agreement agreements and an information security policy is established.
- Electude stimulates awareness, education and training of information security.
- Employees do not have access to more Personal Data than is strictly necessary for their position.

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

Strategy	
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:	Electude shall maintain a record of all categories of processing activities carried out on behalf of VIU, containing: 1. the name and contact details of the person at VIU on behalf of which Electude is acting, and, where applicable, of the VIU's or Electude's representative, and the data protection officer; 2. the categories of processing of personal data carried out on behalf of VIU; 3. where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in case it is necessary, the documentation of suitable safeguards; 4. where possible, a general description of the technical and organizational security measures. Electude continuously monitors the service and has taken the measures described to prevent and detect unauthorized or unlawful access to the Personal Data. [redacted] s. 15(1)(l) Incidents are analyzed to determine if the incident constitutes a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (hereinafter 'Personal Data Breach').

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?

The information sent to Electude from VIULearn is directly imported into VIULearn from the Student Record System. By passing information originating from official VIU systems, we ensure that student information is consistent across platforms and students only need to make corrections in one place if there is a change, or they find an error. If an error is found in Electude data and cannot be corrected by updating official records, students also have the ability to edit their name and email in the Electude platform.

22. 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.

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?

N/A – all personal information within Electude can be edited including user activity records.

Students can request corrections to their Student Record which will then pass automatically into VIULearn on the next update (updates happen every 12 hours). Within Electude, it is possible to give students the ability to change their first and last name, and the email address that any internal messages will be sent to. However, the preferred workflow if a student finds incorrect user information would be to fix it in the source (SRS) first, and allow the change to cascade down.

If an instructor or student finds an error in results reporting or other errors related to the activities/assignments on the platform, they can submit a request to Electude directly to have scores or results corrected.

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.

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

No.

- Personal data are stored until an authorized instructor deletes the data from the service or VIU sends a written request to Electude to have this data deleted.
- Student responses to e-learning activities are automatically deleted after 1 year.
- All personal data will be deleted after the end of the provision of service. After deletion of any personal data, backups are maintained for up to 2 months.
- Log files are automatically deleted after 1 year.
- A student who transfers to another institution that also uses Electude can request to have their Electude data transferred to a new instance's account and that would delete the data from VIU's Electude account.
- On termination of VIU's account with Electude, all data would be deleted. Deleted data is permanently destroyed 60 days after deletion.

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?

No.

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

Possible risk	Response
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: Unauthorized individuals could access the personal information in the system and use or disclose it for personal purposes (within Electude)	Electude implements measures to prevent their data processing systems from being used by unauthorized persons. The Electude uses access authorizations for employees and third parties such as agents, distributors and other sub processors. Persons are only able to access the data within the scope of their position. Employees have signed non-disclosure agreement agreements and an information security policy is established.
Risk 3: Electude security breach	Electude has measures in place to reduce the risk of a breach (outlines in section 19). In the event of a breach, VIU will be notified without undue via e-mail. The notification shall at least: • describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; • communicate the name and contact details of the contact point where more information can be obtained;

Possible risk	Response
	• describe the likely consequences of the personal data breach; • describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
Risk 4: Personal information data is compromised during transition.	Data is only transmitted in encrypted form.

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			

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			