Privacy Impact Assessment

PIA# 24-0015

INSTRUCTIONS/INFORMATION:

Why do I need to do a PIA?
Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA.

Do I have to answer all the questions?
Sections marked as "required" must have an answer. Specify *N/A (not applicable)* if appropriate. Other sections not marked mandatory should STILL be answered if the information is known. You will be contacted to answer any questions that are deemed relevant to this assessment so it's best to be complete.

What if my initiative does not include personal information?
You still need to complete some parts of the PIA to ensure compliance with regulation. Under question "4. Elements of Information or Data", specify "*no personal information collected*". Sections that are marked as "*required*" still need to be answered.

What if I have questions?
If you have any questions about FOIPPA generally, you may contact the "*Privacy and Access Officer*" (privacy@tru.ca). For questions specific to this PIA, contact the "*Information Security Director*" (jcuzzola@tru.ca).

Initiative Preamble (Required)

Initiative/ Project/ Program Name:	Studiosity (pilot/research)		
Name of TRU Department/Branch:	Bob Gaglardi School of Business and Economics		
PIA Drafter (you):	Heidi Milovick (Executive Director, Administration and Student Services, TRU Gaglardi		
Your Email:	hmilovick@tru.ca	Phone:	250-318-0542
Service/Vendor:	Chris Helsby, Vice President and General Manager - Canada		
Vendor Email:	chelsby@studiosity.com	Phone:	416-267-5568

Have you consulted IT Department for this Initiative/Project/Program?
_Yes _____
(*If no, it is recommended to consult IT Department first to resolve any potential IT-related issues.*)

Part 1 – General

1. **Description of the Initiative (required)**
   To deliver on-demand academic support to improve attainment and retention for TRU Gaglardi graduate students studying on campus and online. By providing students with a scalable 24/7, 365 days a year support service, students will create a closer affiliation with their programme and the University, and increase their confidence levels when preparing for assignments and examinations.

   Pilot / Programme: To provide access to Studiosity Writing Feedback and Connect Live services for students within the TRU Gaglardi graduate programs. The aforementioned students will have access to the services for the duration of the term identified. As a result of using Writing Feedback and Connect Live, Studiosity partners measure a range of improvements to student retention and experience (summarized in this research matrix), with up to 60 percent of service engagement taking place at evenings, weekends, and holiday periods.

2. **Scope of this PIA (required)**
   To assess the data security of Studiosity by examining their technical safeguards and policies. To determine which PII fields are being used by Studiosity, for what intent, their legitimacy of use for the purpose intended, and whether technical/policy safeguards are adequate for their (PII) protection.

2-1. Is this in a regular interval, e.g., yearly, or biennially? (required)

This is a pilot program. Initial pilot is for four months.

3. **Related Privacy Impact Assessments**
   One created back in 2022 by Donald Poirier for Open Learning (PIA#23-004). Studiosity has added the use of AI since this time.

4. **Elements of Information or Data (required)**

Where is data stored? *In the Amazon Web Services cloud. Studiosity uses their local server in Sydney, Australia.*

When/how is data encrypted? *Data is encrypted while in transit and at rest, using standard protocols.*

What student data is required and for how long? *Student first name, last name, and email address at minimum are required. Student data is stored for 15 months from the last point of use and then removed/deleted. Data is stored for this period of time so students may retrieve their*

feedback and interactions from Studiosity for future reference. At any time, students can request to have their data removed.

Studiosity+ information regarding our generative AI (GenAI) tool (applies to Writing Feedback Plus):

a. Our GenAI ecosystem has been developed using Studiosity's unique and academically rigorous approach to providing academic writing feedback, proven via multiple research studies and over 23 million feedback data points. Undertaken in partnership with education institutions, this metadataset of feedback was created with thousands of human Subject Specialists, all graduates of the Top 10% of universities worldwide, applying their feedback on real student tasks.
b. All personal identifiable information (PII) is redacted from students' work before submission to the GenAI which **does not use** students' work for training, ONLY inference. Student work is not retained within the LLMs.
c. Writing Feedback+ is a 'closed system' meaning that training of the GenAI only occurs via our Quality Assurance team, never student inputs - which are used for 'inference' only. The approach to feedback is identical to that taken in the past and is based upon our existing education and academic integrity policies. Given its closed nature, data does not go anywhere else.
d. Continual training is based on feedback given, not on the student's content. This is because Writing Feedback+ is feedback, not corrections, suggestions, or answers that are dependent on content or curricula.
e. Our unique Humans in the Loop system – including our Quality Assurance team, Academic Services Team, Student Experience, Senior Leadership, Academic Advisory Board, Higher Education advisers, Global Student Advisory Group – provides governance, oversight, and due diligence around service delivery and development. Our principles in this regard were built on emerging policy from education departments as well as direct consultation with leadership amongst our university partners - we are setting a best practice for AI in learning technology as a benchmark for others.

Documentation

1. HECVAT302.xlsx
2. Privacy Policy - Canada: https://studiosity.com/connect/policy_agreements/6/privacy
3. Data Security and Protection Policy 1.1.0.pdf
4. Data Breach Policy and Procedure 1.1.0.pdf
5. BusinessContinuityOverview-1.0.0-RELEASE-49af708b.pdf
6. SoftwareChangeManagementProcesses-1.0.8-RELEASE-49af708b.p…
7. Studiosity Platform Overview - Architecture Diagram.png
8. GDPR Processors.pdf

Services:

1. Get writing and referencing feedback. (in person and via AI feedback)
2. Online study help from Subject Matter Expert.
3. Flagging of potentially emotionally at risk and academically at-risk students, and passed to the appropriate TRU contact, to decide on follow-up based on institutional policies. This academic and well-being flagging service helps to identify students requiring additional support and escalates them directly back into your university's support ecosystem.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

5-1. Is a service provider(s) involved? If so, where is the provider located (e.g. Canada, U.S., or other country)? (required)
In the Amazon Web Services cloud. Studiosity uses their local server in Sydney, Australia.

6. Common or Integrated Program or Activity (required)
If you answer yes to all three questions, please contact the *Privacy and Access Officer*

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

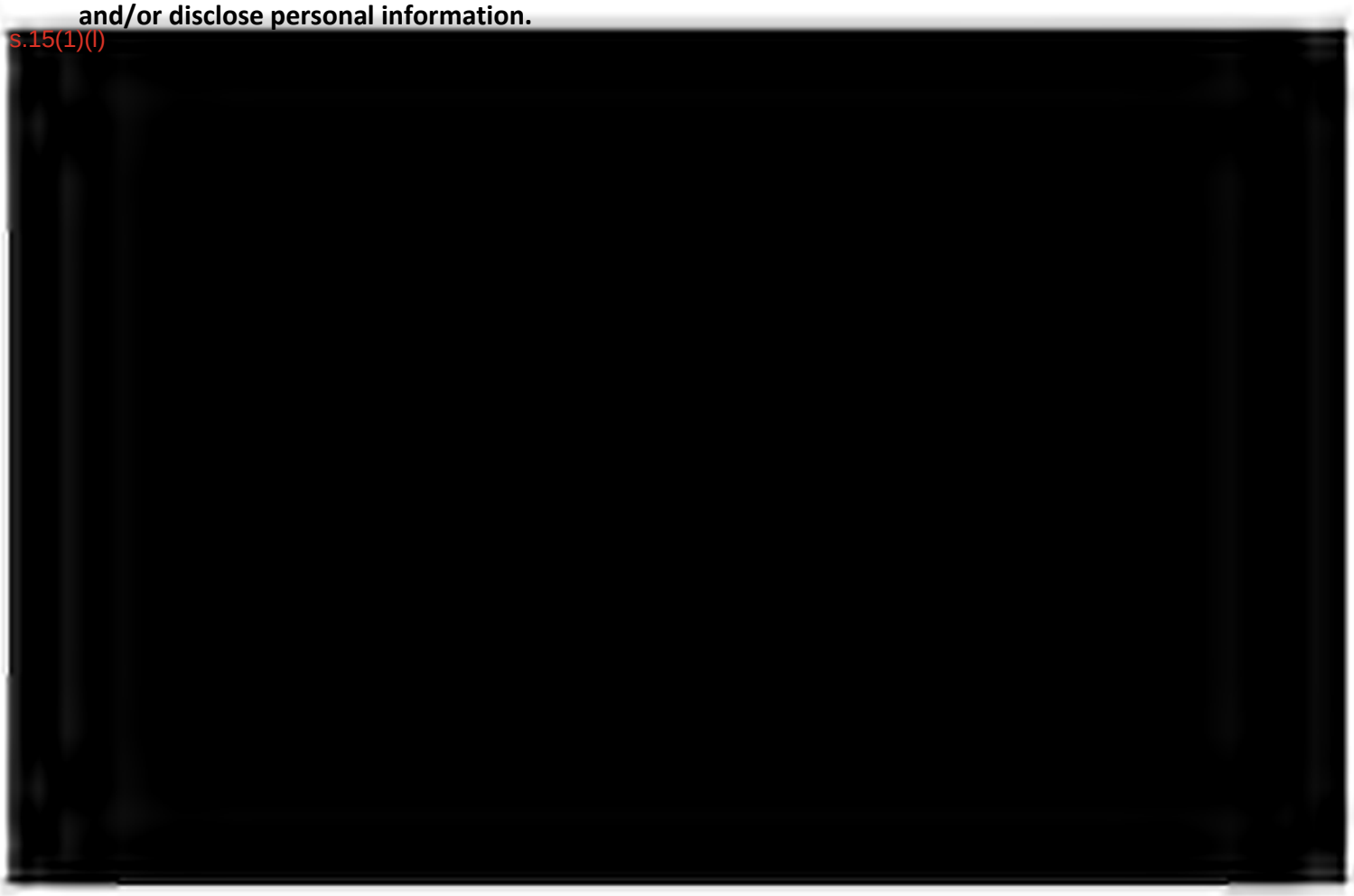
7. Data-linking Initiative* (required)

If you answer yes to all three questions, please contact *Privacy and Access Officer*

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under FOIPPA.	
1. Personal information from one database is linked or combined with personal information from another database;	yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no

8. Provide a diagram, flowchart, and/or table that shows how your initiative will collect, use, and/or disclose personal information.

s.15(1)(l)



Personal Information Flow Table.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	Student registers with Studiosity.	Collection & Consent	26 (c)(d)
2	Student logs into Studiosity portal authenticated by TRU's single sign in (SSO).	Consent & Use	32(a)(b)
3	Student is presented with a dashboard, and selects a service which connects them with a subject-matter-expert.	Consent & Use	32(a)(b)
4	Students at academic risk are identified by Studiosity and are brought to the attention of TRU Open Learning for intervention.	Disclosure & Use	32a, 33(2)(d)

9. Risk Mitigation Table (required)

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please identify the likelihood (rare, unlikely, possible, likely, almost certain) and the degree of impact (insignificant, minor, moderate, major, catastrophic).

Risk Mitigation Table				
Risk	**Mitigation Strategy**	**Likelihood**	**Impact**	**Exposure**
1	s.13 [redacted]			
2				
3				

s.13

→ Exposure rating of *high* or *critical* is of concern. Please contact Director, Information Security to discuss possible solutions.

s.13

Risk Exposure Matrix

Risk Exposure Matrix		IMPACT				
		Insignificant	Minor	Moderate	Major	Catastrophic
	Almost Certain	Low	Medium	High	Critical	Critical
	Likely	Low	Medium	High	Critical	Critical
	Possible	Insignificant	Low	Medium	High	High
	Unlikely	Insignificant	Low	Low	Medium	Medium
	Rare	Insignificant	Insignificant	Insignificant	Low	Low

10. Collection Notice

If your initiative collects personal information directly from any individuals, you must ensure that all individuals involved are told the following:

1. The purpose for which the information is being collected
2. The legal authority for collecting it, and
3. The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

Please contact *Privacy and Access Officer* for assistance on this.

Standard Collection Notice Statement

This should be presented to participants at or before the time of collection (participation in survey):

"Thompson Rivers University (TRU) collects, uses, discloses and retains personal information in compliance with the BC Freedom of Information and Protection of Privacy Act (FIPPA). Your personal is being collected by TRU for the purpose of delivering support through Studiosity, a 3rd party service provider who provides online study help through its platform of subject matter experts (SMEs), as authorized by s.26(c) of FIPPA.

For further information about how your personal information is being collected, please contact: Heidi Milovick, TRU, hmilovick@tru.ca."

Section 26(c) applies where the information relates directly to and is necessary for a program or activity of the public body (TRU). If you do not think this section applies, contact prviacy@tru.ca for assistance.

Part 3 – Security of Personal Information

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

- **Revocation of Access**: Upon the conclusion of employment, an employee's access to physical premises must be revoked.
- **SOC 2 Type 2 Compliance**: hosted on AWS platform.

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

Data is encrypted while in transit and at rest, using standard protocols. Please see attached Data Security and Protection Policy 1.1.0.pdf

From the policies provided:
The technical security measures related to the initiative include the following:

a. **Password Management**: Employees are required to use a password manager (Dashlane). Passwords must adhere to complexity and length requirements, must not be reused, and must be unique to each service.
b. **Secure Coding**: Developers must be familiar with OWASP guidelines and peer review proposed changes for security implications. The Common Weakness Enumeration (CWE) "Top 25" is referenced during code reviews.
c. **Secure Data Destruction**: This includes deleting encryption keys and securely erasing disks for workstations and mobile devices. Cloud storage data destruction follows policies by AWS, Google Workspace, Google Cloud, and Microsoft Azure.
d. **Encryption**:
    - **Transport**: TLS 1.2 and above must be used. SSL is prohibited.
    - **User Device Disk Encryption**: All devices used for fulfilling roles must use Full Disk Encryption (FDE).
    - **Server Disk Encryption**: All EC2 instances must use EBS volume encryption for data in transit and at rest.
e. **Anti-Virus and Malware Protection**: Required for workstations (Windows Defender for Windows, XProtect and Gatekeeper for macOS, ClamAV and Rootkit Hunter for Linux) and servers (ClamAV, unhide).
f. **Vulnerability Scanning**: Regular network vulnerability scans are performed quarterly by an Approved Scanning Vendor (ASV) and monthly by internal qualified resources. Identified vulnerabilities are remediated based on their severity.
g. **Change Control and Risk Assessments**: Employees must adhere to change control policies, including performing data security risk assessments for proposed changes, identifying assets, and determining risks.
h. **Secure Workstation and Mobile Device Policies**: Workstations and mobile devices must use supported operating systems, have automatic updates enabled, and be configured with personal firewalls and screen locking functionality.
i. **Permitted Cloud Storage**: Only specified platforms (Amazon S3, Google Team Drive, Google Cloud Storage, Microsoft Azure Blob Storage) are permitted for file storage.
j. **Notification of Security Breaches**: Employees must report any information security breach to the CTO or CEO immediately.

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

The security policies used in this initiative are detailed in the "Data Security and Protection Policy" document. Key policies include:

a. **Compliance Policies**:
    - **PCI DSS**: Adherence to PCI DSS SAQ A-EP 3.2 obligations.
    - **Applicable Legislation**: Compliance with GDPR, Data Protection Act 2018, Australian Privacy Act 1988, and the Personal Information Protection and Electronic Documents Act of Canada.

- **Cyber Essentials**: Compliance with the Cyber Essentials Framework.

b. **Standard Operating Environment**:
   - Requirements for server environments, workstations, mobile devices, and web browsers, including encryption and firewall configurations.

c. **Bring Your Own Device (BYOD)**:
   - Policies governing the use of personal devices, ensuring they meet company standards for security and encryption.

d. **Encryption**:
   - **General Encryption**: Policies on data encryption at rest and in transit, requiring TLS 1.2 and above.
   - **Disk Encryption**: Full Disk Encryption (FDE) for internal and external devices.

e. **Screen Locking**:
   - Policies for using screen locking on all devices with corporate data, including display lock on idle timeout.

f. **Permitted Cloud Storage**:
   - Approved platforms for file storage such as Amazon S3, Google Team Drive, Google Cloud Storage, and Microsoft Azure Blob Storage.

g. **Anti-Virus and Malware Protection**:
   - Requirements for anti-virus and malware protection on workstations and servers.

h. **Security and Software Patching**:
   - Policies for maintaining up-to-date software and applying security patches within specified timeframes.

i. **Vulnerability Scanning**:
   - Regular network vulnerability scans and remediation of detected vulnerabilities based on severity.

j. **Notification of Security Breaches**:
   - Procedures for reporting and responding to information security breaches.

k. **Password Management**:
   - Policies for creating, managing, and securing passwords, including the use of a password manager.

l. **Secure Coding**:
   - Requirements for secure coding practices and peer review of code changes.

m. **Secure Data Destruction**:
   - Procedures for securely erasing data on workstations, mobile devices, and cloud storage.

n. **Change Control**:
   - Policies for managing and assessing risks associated with changes to systems and processes.

o. **Staff Employment Lifecycle**:
   - Policies for onboarding and offboarding employees, including revocation of access to premises and digital infrastructure.

p. **User Accounts**:
   - Management and auditing of user accounts and access permissions.

q. **Data Classification and Handling**:
   - Classification of data into levels (PUBLIC, INTERNAL, CONFIDENTIAL, RESTRICTED) and corresponding handling procedures. t

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

The initiative uses several access controls and mechanisms to limit or restrict unauthorized changes (such as additions or deletions) to personal information:

a. **Limited Access and Processing**: Access to personal data is restricted to employees who require it for the stated purpose for which it was collected.

b. **User Accounts**:
   - User access accounts must be deactivated if not used within 90 days and automatically locked in the event of excessive authentication failures.
   - Access to resources is granted only as needed for the employee's role, and additional access must be revoked as soon as it is no longer required.
   - Auditing of user accounts and access must be conducted regularly.

c. **Change Control Policies**:
   - Employees must adhere to established change control policies and conduct Data Security Risk Assessments for proposed changes.
   - Changes involving personal data must be documented, reviewed for security and data protection, and approved by the Data Privacy Officer or Chief Technology Officer. A Data Protection Impact Assessment (DPIA) must be conducted if necessary.

d. **Data Classification and Handling Policy**:
   - Data is classified into levels (PUBLIC, INTERNAL, CONFIDENTIAL, RESTRICTED) to ensure appropriate handling, transfer, dissemination, and destruction.

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

Logging and monitoring are constantly looking for error conditions and unauthorised access attempts.

In addition to the aforementioned, Studiosity tracks who has access to personal information using several policies and procedures:

a. **User Accounts**:
   - User access accounts are tracked using immutable audit or activity logging.
   - Regular auditing of user accounts and access is conducted at monthly intervals, whenever an employee's role changes substantially, and whenever an employee leaves the organization.

b. **Data Management and Archiving**:
   - Access to archived data is logged to ensure that historical access can be audited.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's personal information updated or corrected? If it is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated.

A privacy document was included in the submission. *In addition, individual's personal information can be updated or corrected as follows:*

a. ***Documentation and Review**: Any changes involving personal data must be clearly documented, including the impact on the collection, storage, and processing of personal data. The security and data protection qualities of any Data Processors involved in the changes must be carefully reviewed. Required:*

- *Clearly document what changes are being made and their impact on the collection, storage, and processing of personal data.*
- *Carefully review the security and data protection qualities of any Data Processors involved in the changes.*
- *Conduct a matrix-based risk analysis.*
- *Seek a review by the Data Privacy Officer or Chief Technology Officer.*
- *Conduct a Data Protection Impact Assessment (DPIA) if necessary.*
- *If the information is not updated or corrected, it will be annotated by documenting the proposed changes, the review process, and the reasons for not implementing the changes.*

b. ***Approval and Assessment**: Changes must be reviewed by the Data Privacy Officer or Chief Technology Officer, and a Data Protection Impact Assessment (DPIA) must be conducted if necessary.*

If the information is not updated or corrected due to physical, procedural, or other reasons, it must be annotated to reflect the necessary changes and ensure that any issues with data accuracy are addressed through proper documentation and review processes.

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

No

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate, complete and up-to-date.
For example: check to see that the information was obtained from a reputable source such as another government agency.

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

If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please contact Manager, Information Services.

During the research study we will retain the detailed student information, plus data gathered from the research study, and retain in an identified format for no longer than 12 months. *The aggregated, deidentified (anonymized) data will be retained in perpetuity*.

Part 5 – Further Information

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

For example: your initiative involves a regular exchange of personal information (both collection and disclosure) with other government(s) and/or other agencies in order to provide services to your clients.

N/A

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact Legal Services.	N/A

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

During the research study we will retain the detailed student information, plus data gathered from the research study, and retain in an identified format for no longer than 12 months. The aggregated, deidentified (anonymized) data will be retained in perpetuity.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA, please contact *Privacy and Access Officer*.	N/A

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

A personal information bank means 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 to an individual.

N/A

Part 6 – Canada's Anti-Spam Legislation (CASL) Compliance

23. Please confirm if you plan on emailing, texting, or instant messaging as part of your project. (required)

Studiosity may use your personal information for marketing their Services to all User types to show how their Services can help.

24. If you answered yes to question 23, please explain the purpose(s) of the messages you intend to send. Be sure to note any messages involving promotional activities, including links to the TRU public website or other Internet site(s). The purpose(s) you provide will help us identify whether the overall communication is a commercial electronic message (CEM[1])?

Studiosity may use your personal information for marketing their Services to all User types to show how their Services can help. To facilitate, process and respond to the educational or study queries of Students, Student Mentors and Subject Specialists. To facilitate online chats between Students and Student Mentors and Subject Specialists. To facilitate Subject Specialist training. To seek feedback in relation to partner satisfaction; and to consider any concerns or complaints made against.

25. If your communication message does fall under CEM rules, you must comply with the unsubscribe mechanism and identification requirements under CASL. Please confirm your method of unsubscribe mechanism that must be processed within 10 business days and how you will meet the identification requirements?

N/A

26. If you do meet the definition of CEM, please confirm that you have a records retention schedule that will ensure that consent communications, both paper and electronic, are stored appropriately and retained for three years after the last communication?

N/A

Part 7 – Common Vulnerabilities and Exposures (CVE) Assessment

(This section to be completed by the **Information Security Office**). If your initiative involves the transmission of personal data between TRU and the vendor, or from the vendor to 3rd parties, then TRU may ask for the name of the software used to determine if there are applicable CVEs.

There are no CVEs on record.

[1] If your initiative or program sends commercial electronic messages (CEMs), such as emails promoting a product or service, you must comply with CASL's requirements to: (1) obtain consent, (2) provide identification information, and (3) include an unsubscribe mechanism in each message. Please note that an electronic message that contains a request for express consent is also considered to be a CEM under CASL.

Part 8a – Information Security Director Comments

s.13 [redacted]

John Cuzzola | s.22 [redacted] | 2024-07-24

Information Security Director | Date

Part 8b – Privacy Officer Comments

Privacy and Access Officer | Signature | Date

Part 9 – Program Area Signatures

Program/Department Manager	Signature	Date
John Cuzzola	s.22 [redacted]	2024-07-24
Information Security Director	Signature	Date
Senior Manager, Program Area/Division	Signature	Date
General Manager	Signature	Date
General Manager	Signature	Date

A Final Copy of this PIA (with all signatures) shall be kept on record by the program area responsible for this project. The signed original record will be retained by the FOI and Privacy Office. ***If you have any questions about FOIPPA generally, you may contact the "Privacy and Access Officer" (privacy@tru.ca). For questions specific to this PIA, contact the "Information Security Director" (jcuzzola@tru.ca).***