Privacy Impact Assessment

24-0013

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:	**Modern Campus (Lifelong Learning Extended Education)**		
Name of TRU Department/Branch:	Deputy Registrar Student Records / Enrolment Services		
PIA Drafter (you):	Heidi Lawson		
Your Email:	hlawson@tru.ca	Phone:	**1-250-852-6436**
Service/Vendor:	**Modern Campus**		
Vendor Email:	Kevin Gish, Solution Engineer <kgish@moderncampus.com>	Phone:	**(416)480-0500**

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)

Please provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc. We will be assessing the impacts of this initiative so please include details which help us understand its size/scale and reach.

Modern Campus provides the industry-leading Lifelong Learning Extended Education (interchangeably with Extended Education) platform - a student lifecycle management cloud based solution that greatly improves student registration through an Amazon-like experience, streamlines business processes, assists with marketing communications, and optimizes the growth potential of programs for career and professional training, adult enrichment, contracted training, and other non-credit educational opportunities.

Lifelong Learning Extended Education includes key features specifically designed to support: 1. The needs of a unified, multi-program effort such as Thompson Rivers University 2. A way for Thompson Rivers University to effectively manage career-credit, workforce, and non-credit training offerings that may run on a different schedule and/or function differently from traditional credit-bearing offerings; and 3. A means for the college to facilitate, operate, and grow corporate partnerships, other 3rd party relationships, camps, conferences, and licensure/certification programs.

The system facilitates the registration and payment process, helps staff manage back-end operations such as automated waitlists, tuition profiles, and course scheduling, and provides consumable data through reports and dashboards so that key performance indicators can be analyzed and acted upon. Students can find courses that suit their schedules and styles of learning (e.g. face to face or online). Specifically, the system must:

• support the full range of student services that open learning provides such as information on Tuition and fees, education advising, orientation, final exam, and student forms.

• Support student registration either via online or email, mail, or fax.

• Support a standardized student enrollment and registration business process that is built on the principle of a student is a student regardless of program.

• Allow students from anywhere to register for any of the courses offered by OL that support their individualized educational needs.

• Support the current business process of material shipment through integration to Materials and Supply Chain system or in the event of elimination of the practice, an alternative medium that allows student to access their materials online.

• Support the current faculty payment process or allow the system to reengineer faculty payment functionality and the business practices within TRU with a more standardized faculty payment process like salaried payment structure.

• The system must be able to integrate with TRU ERP Banner System and any other impacted system that OL registration process currently connects without any loss of data or information throughout the student's OL life cycle.

• On demand reports, BI, or dashboard for OL, Enrollment Services, Finance, and other impacted stakeholder groups that service OL programs, students, and faculties.

2. Scope of this PIA (required)

This section should explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

To determine if the PII data elements in question #4 are adequately protected and the collection, use, and disclosure of such data is in compliance with legislation (FOIPPA).

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

Annual service contract. Current term: 5 years

3. Related Privacy Impact Assessments

Please identify any approved PIAs which cover any parts of the initiative or any previously approved PIAs for this initiative.

No Previous PIA

4. Elements of Information or Data (required)

Please list the elements of information or data involved in the initiative. This could include name, date of birth, home address, personal email, phone number, employment history, health information, financial information, photos, personal opinions, comments/open-ended questions on a survey, or information specific to your area, e.g., stumpage totals, visitor centre stats, etc.

Lifelong Learning Extended Education maintains the following information:

• *Curriculum information: courses, sections, certificates, fees, course calendar, etc.*

• *Student profile, communications and documents*

• *Enrollment data*

• *Financial data*

• *Ad-hoc Saleable items*

- *Instructor contract and biographical data*
- *Marketing data*
- *Information and calendar for school facilities*
- *Reporting information*
- *Dashboard information (with the optional Destiny Dashboards module)*
- *Integration information (which can also include connector data with the optional SalesForce Integration Option)*
- *Badging (micro credentialing) information (via the optional Lifelong Learning Extended Education Badging module)*
- *Corporate contract data (with the optional Corporate Engagement Manager module)*
- *Conference data (with the optional Conferences module)*
- *Data on international and specialty programs (with the optional International and Specialty Programs Manager module)*
- *Multi-language display information (with the optional Language Packs module)*
- *Permissions, access information, limits and restrictions*

The profile includes student name and demographic information, student categories, access information (user name, password and access attempts), multiple mailing addresses, multiple phone or fax numbers, multiple email addresses, enrolled certificates, applications, administrative and marketing contact methods, associated groups, manager and employer information, membership information, association and professional accreditations, student communities, educational background, email newsletter subscriptions, learning goals, interests, enrollment timeframe, international student information, emergency contact information, youth participant information, hold details and comments.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

Can your information be accessed from outside Canada (i.e. on the TRU website), or is your information being stored outside Canada (i.e. in the "cloud", or on a non-Canadian social media site)?

5-1. Is a service provider(s) involved? If so, where is the provider located (e.g. Canada, U.S., or other country)? (required)

The Lifelong Learning Extended Education software and all the data is in the cloud, on Amazon Web Services (AWS). The location of the AWS servers is in the Amazon Canada region with datacenter located in Montreal region. Data is sent from the Lifelong Learning Extended Education servers on AWS to specific integration points through secure channels (TLS). These include Payment Gateways, as well as any external systems required for integration by Thompson Rivers University. No data leaves the Amazon Web Services (AWS) servers or Canada.

6. Common or Integrated Program or Activity (required)

If you answer yes, 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, 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 (see examples below) (required).
Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. If the authority comes from other legislation, please identify the applicable act(s) or regulation(s), including specific section references. Please contact Manager, FOI and Privacy for assistance on this.

Below is a table showing how the initiative collects, uses, and discloses personal information:

Stage	Actions	Description
Collection **s. 26(c)(d)**	Web Forms	Personal information is collected through online forms filled out by users.
	Applications	Information is gathered from applications submitted by individuals.
	In-Person	Data is collected directly from individuals during face-to-face interactions.
Storage **s. 30**	Database	Information is stored in a secure database with restricted access.
	Secure Servers	Data is kept on secure servers with appropriate security measures.

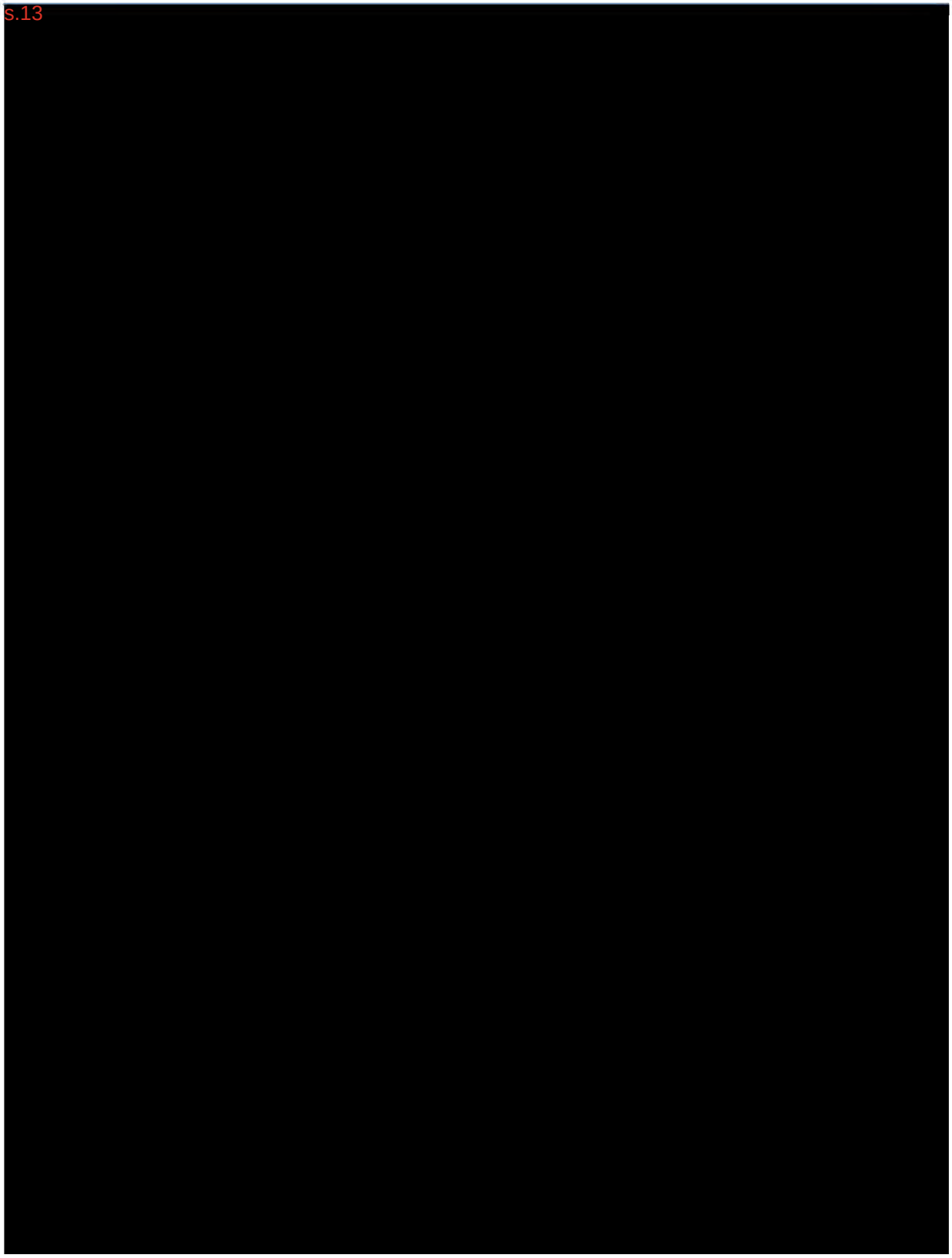
Stage	Actions	Description
	Encrypted Backups	Regular backups of data are encrypted for additional security.
Access & Use **s. 32(a)(b)**	Authorized Staff	Only authorized personnel can access personal information.
s. 32(a)(b)	User Profiles	Personal information is used to create and manage user profiles.
s. 32(a)(b)	Audit Logs	All access and changes to data are logged for audit purposes.
Disclosure **s. 33(2)**	Legal Compliance	Information may be disclosed to comply with legal requirements.
s. 33(2)(c)(d)	User Consent	Personal data is shared with third parties only with explicit user consent.
s. 33(2)(d)	Third-Party Services	Information may be shared with third-party services for processing, under strict agreements.

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) of this risk happening and the degree of impact it would have on individuals if it occurred (insignificant, minor, moderate, major, catastrophic). You may contact the *Information Security Director* for assistance.

Risk	Mitigation Strategy	Likelihood	Impact	Exposure
s.13	[redacted]			

s.13



s.13 [redacted]

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

s.13 [redacted]

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.

Insert Your Collection Notice Statement Here

Any personal information is collected by the Thompson Rivers University under Section 26 (c) of the *Freedom of Information and Protection of Privacy Act* and will be used to support student Open Learning (OL) registration including material shipping and tuition processing. Should you have questions about the collection of this information, please contact:

Heidi Lawson
Deputy Registrar Student Records / Enrolment Services
Thompson Rivers University
Phone: 1-250-852-6436
hlawson@tru.ca

END-OF-NOTICE <<<

Please see comments below:

"How Personal Information is to be collected" Section (platform specific options)

Thompson Rivers University can draft policies that are in accordance with the FOIPPA Act, and the individuals cannot register unless they accept the Terms and Conditions.

Lifelong Learning Extended Education maintains a "Privacy Policies" section as part of the student profile. In this section, detailed privacy policies can be drafted and presented to learners, and learners must acknowledge them by providing their initials before continuing.

Also, there is a separate Policy Confirmation area that is presented in every transaction, such as when a learner is purchasing courses and non-course saleable items. In this area, learners must fill in a checkbox stating that they acknowledge and agree with the policies. The language for this checkbox is configurable.

Additionally, Receipt Notes can be defined on each course section, which allows for section-specific policies which are displayed on the receipt.

Course and course-section specific forms that must be acknowledged before completing registration can be achieved with the configurable questionnaire and application functionality and enforced by enrollment restrictions.

A separate area to define and display Privacy Policies is also available.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).
For example: locked cabinets, securely stored laptops, or key card access to the building.

The physical security measures specified within the files are:

a. ***Access Control**:*

- *Access to Modern Campus offices is controlled by passkeys tagged to individual users. Loss of a passkey must be reported immediately to the COO or Chief Security Officer to ensure it is cancelled.*
- *Access to Modern Campus offices after hours is managed through controlled elevator and/or building access.*
- *Access to Modern Campus server rooms is controlled and limited to authorized individuals approved by the COO or Chief Security Officer.*
- *A physical barrier fully encloses the physical space preventing unauthorized physical contact*

b. ***AWS Infrastructure**:*

- *Modern Campus staff do not have access to AWS infrastructure, which is managed by AWS physical security policies.*

c. ***Data Centers**:*

- *Data centers are geographically diverse for disaster recovery purposes, with redundant power and cooling systems. They are staffed 24/7 and have multiple network provider entrances.*

d. ***Environmental Protection**:*

- *Media used for long-term retention of business data and archival purposes is stored in secure, environmentally protected areas.*

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

For example: use of firewalls, document encryption, or user access profiles assigned on a need-to-know basis.

The technical security measures specified within the files include:

a. ***Access Control**:*

- *Enforcement of authentication and authorization policies is automated through group policies. Each employee is added to the appropriate authorization groups during the initial new-hire provisioning process. Employees are required to notify the COO or Chief Security Officer if they believe that their access or authorization to Modern Campus resources is incorrect. Access to all computing resources is controlled through Login ID's and passwords. The structure and strength of these credentials is established using company group policies and cannot be overridden by the employee. Frequency of forced change of these credentials as well as lockout rules are set through group policy. User access is terminated immediately upon employee dismissal.*

b. ***Backup**:*

- *Backups are run regularly under different levels:*
  - *i. Shadow copies of corporate data on the main file systems occurs every 6 hours.*
  - *ii. Incremental backups of all corporate data on main file systems public and private directories occur daily.*
  - *iii. Multiple backup sets are used to ensure redundant backup copies for integrity purposes.*
  - *iv. Backups of infrequently used files occurs on a monthly basis.*
  - *v. Integrity checks occurs monthly (full and incremental restore test).*
  - *vi. All backup datasets are password protected and encrypted.*

c. ***Disaster Recovery**:*

- *Offsite independent full backups with business documents and source code. In the event of a on-premises disaster:*
  - *i. Executive call process to critical employees.*
  - *ii. Executive call process to customers as required.*

iii. *Provisioning of off-the-shelf hardware in 'on-demand' office facilities available in Toronto.*

iv. *Provisioning of suitable internet backbone in 'on-demand' office facilities available in Toronto.*

v. *Redirection of company phone/mail/other communications as required.*

vi. *Establishment of Firewall/VPN services on provisioned hardware.*

vii. *Restoration of main file system contents and source code to provisioned servers.*

viii. *Creation of required business process documentation for management of projects and staff during recovery period including remote access (work from home) and on premises for business continuity.*

d. ***Encryption**:*

- *Modern Campus employs encryption for sensitive information (protected health information, student identifiable, personnel information, intellectual property, etc.) for external or Internet transmissions with keys of at least 128 bits in length for symmetric encryption and 1024 bits or greater in length for asymmetric encryption.*

e. ***Anti-Virus and Patch Management**:*

- *Anti-virus is required for all computer equipment. All company desktop/laptops used in daily operation must be configured with anti-virus software with automatic detection file updates and scheduled scans.*
- *Employees are required to have all required security patches. This is managed through Windows automatic update.*

f. ***Password Security**:*

- *Passwords are never stored in clear text and must meet strength requirements, expire periodically, and have a minimum of 8 characters. System level and user level passwords are changed regularly based on group policies. User accounts are locked after unsuccessful login attempts are exceeded.*

g. ***Incident Response**:*

- *A documented Incident Response Plan which includes an Incident Response Team (IRT) composed of senior members of the DevOps, Customer Support, and R&D teams.*

h. ***SOC-2 Compliance**:*

- *Modern Campus products have the following certifications: PCI-DSS Service Provider L2 V3.2 and SOC-2 compliance.*

i. ***System Monitoring and Logging**:*

- *Modern Campus has implemented system event logging on all servers, and records 'who, what, and when'. Logs are routinely reviewed for failed logins, failed access attempts, dormant accounts, possible intrusion attempts, and unusual or anomalous activity.*

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

Please describe any specific policies and procedures and provide contact details for someone who could answer questions on this matter. If you are relying on a third-party's policies, please include links or documentation for our review, if available.

Modern Campus has several security policies in place:

a. ***Information Security Policy**:*

- *The Information Security Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Modern Campus without proper authorization.*

b. ***Access Control**:*

- *All access to Modern Campus offices is controlled by passkey tagged to an individual user. Any loss of passkey must be reported immediately to the COO or Chief Security Officer to ensure that the passkey is cancelled.*

c. ***Acceptable Use Policy**:*

- *Rules to protect the employee, customer and Modern Campus. Inappropriate use exposes Modern Campus to risks, including virus attacks, compromise of network systems, services and legal issues.*

d. ***Incident Response Plan**:*

- *Modern Campus has a documented Incident Response Plan to provide guidelines on the appropriate actions to carry out when a security exposure has been identified. This includes the formation of an Incident Response Team (IRT) composed of senior members of the DevOps, Customer Support, and R&D teams.*

e. ***Security Awareness and Training**:*

- *All staff are required to receive annual security awareness training.*

f. ***Compliance****:*

- *PCI-DSS Service Provider L2 V3.2 and SOC-2 compliance.*
- Complies with all appropriate government and industry security standards including FERPA, **FIPPA**, GDPR, CCPA, and PCI-DSS.

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)
For example: role-based access.

Modern Campus implements the following access controls and restrictions to limit unauthorized changes to personal information:

a. ***Permissions Framework****:*

- *A framework of over 1000 individual permissions assigned to roles. TRU can restrict access to curriculum, financial, enrollment, and other data, and related reports based on the departmental access that each user has been granted.*

b. ***Authentication and Authorization****:*

- *Policy enforcement is automated through group policies. Access controlled through Login ID's and passwords. Credential strength is by group policies. Frequency of forced change and lockout rules set through group policy. User access is terminated immediately upon employee dismissal.*

c. ***Least Privilege Principle****:*

Internal access to personal records is restricted to those having an authorized, business-related need-to-know. Release of personal information to outside sources without your written approval is forbidden, unless legally required.

d. ***Client Data Management****:*

- *Controls in place for distribution and management of data. Client PII information not stored on equipment leaving the company premises. TRU data will not be provided to any third party without explicit permission from TRU and Modern Campus CISO.*

15. Please describe how you track who has access to the personal information. (required)
For example: audit trails or physical sign-in and sign-out of files.

Modern Campus tracks access to personal information through various mechanisms and policies:

a. ***Audit Trails and Monitoring****:*

- *Audit tables provide a record of addition, update, and deletion with timestamp and user who performed the action.*
- *Supervisory staff users can detect unauthorized attempts using the Access History Report to identify all successful and failed login attempts.*

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.

For example: users have access to update their own information or notes will be made on a case file.

An individual's personal information is updated or corrected in the following ways:

a. ***Self-Editing by Students**:*

- *Students have access to populate and modify their own profiles in the password-protected Student View, while staff have a more comprehensive view than students. Changes and additions are tracked by the system at the user level, whether done by staff or by the students themselves.*

b. ***Staff Assistance for Non-Editable Fields**:*

- *For fields that are not directly modifiable by students, the students may submit a request for information modification; an authorized TRU staff member can make the modification.*

c. ***Annotations for Non-Updated Information**:*

- *Individuals may submit documentation to TRU to correct inaccuracies or provide written comments in disagreement with any material contained in their record.*

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

Yes, see Part 1, question 1 – "*purpose of the initiative*"

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.

Modern Campus ensures that personal information is accurate, complete, and up-to-date through the following measures:

a. ***User Access and Self-Editing**:*

- *Students have access to populate and modify their own profiles in the password-protected Student View, while authorized TRU staff can make changes on behalf of any student(see Part 4, question #16). Changes are tracked whether done by staff or by the students themselves.*

b. ***Data Integration**:*

- *Lifelong Learning Extended Education can integrate with the CRM allowing for single source of truth.*

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.

Modern Campus' retention policy and procedures are detailed as follows:

a. ***Retention Policy**:*

- *The Act requires Thompson Rivers University to retain personal information for at least one year after being used. Lifelong Learning Extended Education marks data as inactive if it is not in use. Inactive information does not appear in searches, nor does it appear within the current and active listings.*

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.	

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

For example: your initiative involves disclosing information to PhD students so that they can conduct research.

N/A.

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*.	

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.

Yes – see Part 1, question #4 for information collected.

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)

Yes

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])?

Messages may be sent to facilitate corporate sponsorships, provide information on conferences and available certification programs. Confirmation of registration and payments, waitlist information, and course scheduling, etc. See Part 1, question #1. Messaging is non-commercial.

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?

Does not fall under CEM.

[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.

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.

(Info. Sec): Not Applicable. No CVEs found.

Part 8a – Information Security Director Comments

s.13 [redacted]

John Cuzzola	s.22 [redacted]	2024-07-19
Information Security Director	Signature	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]	2024-07-19
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).***