



OFFICE OF THE VICE-PRESIDENT, LEGAL AFFAIRS  
Archives and Records Management Department

## PRIVACY IMPACT ASSESSMENT

for

### Instructure Canvas LMS for SFU Beedie School of Business

#### 1. Purpose of the Privacy Impact Assessment (PIA)

This form is used by SFU to determine if a current or proposed policy, system, project, program or activity meets or will meet the protection of privacy requirements under Part 3 of the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA). The Act makes it a legal requirement that SFU conduct a PIA in accordance with the directions of the minister responsible for the Act. The PIA is a compliance and risk management tool to identify potential privacy issues and impacts, allowing correction and mitigation, thus avoiding costly system, program, service, or process redesign; privacy complaints or breaches; and harm to personal, professional and institutional reputation.

See Schedule A for definition of terms.

*Archives and Records Management Department use only*

<b>Office of primary responsibility</b>	Beedie School of Business	<b>Approved date</b>
<b>PIA #</b>	2022-001	<b>OIPC notified date</b>
<b>Type of PIA</b>	<input checked="" type="checkbox"/> Department <input type="checkbox"/> Corporate <input type="checkbox"/> Update	<b>OIPC response date</b>
<b>Type of PIA review</b> (Check all that apply)	<input type="checkbox"/> Policy <input checked="" type="checkbox"/> System <input type="checkbox"/> Program <input type="checkbox"/> Activity	<input type="checkbox"/> Project
<b>Other applicable PIA provisions</b> (Check all that apply)	<input type="checkbox"/> Common or integrated program <input type="checkbox"/> Information sharing agreement	<input type="checkbox"/> Data-linking initiative

## 2. General Information

### 2.1 Unit and Program Area

Identify the Department and Program submitting this PIA

Department:	Beedie School of Business
Program:	SFU Beedie Executive Education

### 2.2 Contact

Identify the individuals best positioned to speak to the contents of this PIA

Name of PIA Drafter:	Saskia Morgan		
Position Title:	Project Manager, Digital Transformation		
Phone:	778.782.9357	E-Mail:	smorgan@sfu.ca
Name of Program Manager:	Jennifer Beale		
Position Title:	Executive Director, Executive Education		
Phone:	778.782.7587	E-Mail:	jennifer_beale@sfu.ca

### 2.3 Description of the Current or Proposed Policy, System, Project or Program

Provide as background a general description of the initiative and the context in which it functions. This could include the purpose of the initiative and its benefits, what larger process it is part of, how it functions, how it integrates with or consolidates other information systems, how it aggregates and stores together information that was previously maintained separately, how it converges different record keeping systems, the parties involved, how it will automate or otherwise change the existing business workflow, etc. Describe in the sections immediately following the background (if applicable) specific details with respect to the individual actors involved in the business process, focusing on how their personal information will be collected, accessed, used, disclosed and retained.

Include copies of documentation (if it exists) that describe the business requirements, functional analysis, conceptual overview, etc. that helps explain the initiative.

#### 2.3.1 Background

As an initiative under *Canada's Digital Technology SuperCluster*, SFU's Beedie School of Business received a grant to support furthering work in Executive Education, specifically this grant supports the Digital Innovation and Leadership Initiative (DIAL). Under the SuperCluster program, one of the goals is to increase corporate engagement with educational institutions to encourage collaboration in solving social and industry problems. To achieve this goal, one requirement of the grant

recipients is to directly engage with sponsoring businesses. Instructure, the developer of the Canvas Learning Management System is one of these participating businesses.

SFU has an existing relationship with Instructure and Canvas: we have been running the Canvas LMS since 2012, under the community open-source model, running our own instance in the SFU data centre. Canvas was chosen by a community selection process. It was run on-premise in order to address privacy requirements under BC FIPPA when Instructure's data centres were solely run in the United States at a time when it was not possible for SFU to use Canvas in a way that was compliant with that legislation.

In recent years, Instructure has broadened their support for the data privacy needs of the international community including running instances of Canvas in a Canadian data centre. The related changes can provide a basis of risk mitigation in response to BC FIPPA requirements, and other BC institutions including UBC have adopted the cloud-hosted version of Canvas with the Canadian facilities now in place.

In this document where "Canvas" is referenced, we refer to the instance of Canvas hosted by Instructure in the cloud in their Canadian data centre; references to the on-premise, open-source instance of Canvas currently being used for courses at SFU will be referred to as "SFU Canvas."

The intent of this PIA is to support the SFU Beedie School of Business' engagement with the Digital SuperCluster initiative by adopting the cloud instance of Canvas in order to leverage additional capabilities available in the Instructure-hosted, commercial instance of Canvas. While SFU Canvas is nearly identical in most aspects to the cloud-based Canvas, there are features only available in cloud-hosted Canvas that would be beneficial to this program:

- Shareable Content Object Reference Model (SCORM) - a set of technical standards for eLearning development. SCORM support for content integration will allow re-usable content delivery modules to be constructed, creating significant technical and operational efficiencies related to course content production; (source: <https://scorm.com/>)
- Content Delivery Networks (CDN) - a geographically distributed group of servers that work together to provide fast delivery of Internet content. CDN can improve site responsiveness for students working far from the SFU data centres in the Lower Mainland. (Source: <https://www.cloudflare.com/en-ca/learning/cdn/what-is-a-cdn/>)

The audience for this initial use case is non-credit students of SFU-Beedie's Executive Education program, as well as Executive Education's participation in the BC digital SuperCluster program. Non-credit students are manually enrolled specifically into their program of participation, their enrolment data is not integrated with SIMS or other SFU systems, and these students do not normally participate in other undergraduate or graduate programs at SFU.

### 2.3.1.1 Student Information

**Collection:** Students submit their information via webform including name, email, and desired program of enrollment. SFU Beedie staff use this information to manually enroll students in Canvas using their provided name and email address. Once enrolled, students may log-in to canvas and submit their own data including optional biographical details in a profile summary statement, opinions in published comments, posts, and assignments, and coursework including assignments and quizzes. Canvas logs student engagement activity including date and time of access. Please see below for details on use of engagement activity.

**Access:**

The data may be accessed by authorized members of SFU Faculty, staff and students enrolled in related courses. Access is scoped to appropriate levels for a given role in the system (e.g., a student needs to be able to identify other course participants in order to

engage in discussion or group work; an instructor must be able to see the entire class list for meaningful interaction and administrative needs such as grading). User access is controlled by role assignment permissions within the application.

**Instructor access:** Instructors will have access to the following, only for courses to which they are assigned “instructor” access: Student names, emails, student submission date and time stamps, student’s submitted assignments (including submission date/time for confirming due date requirements are met), student’s published discussion posts, questions, and public comments, (students must publish their posts to make them visible to instructors), student engagement activity.

**Student access:** Students may access the following only for courses they have been enrolled in: Classmate names, view/reply access to classmates’ published discussion posts, questions or comments (students must choose to publish their posts to make them visible to classmates).

**Staff Administrator access:** SFU-Beedie staff administrators will have access to the following for courses they administrate student names and emails for the purposes of enrollment in courses and communication about course related matters, instructor name and email for assigning instructors access to courses and providing communication and support, aggregate student engagement details for the purposes of assessing effectiveness of course design and materials.

**About student engagement activity:** Basic student engagement activity is logged by URL and time of access, and that information is visible to the course instructor and institutional Canvas account administrators with appropriate roles in the student’s courses. Time of log-in is required for time-sensitive assignment submissions. Aggregate engagement data (e.g., total student hours spent logged into course, number of modules viewed, etc.) may also be considered when designing or improving course structure and content by instructional designers and instructors.

Logs of activities, IP addresses and other information necessary for security, audit logging, and similar operational activities of the service by Instructure are visible to their staff under Instructure’s Data Classification, Handling and Encryption Policy. Customer data and identity information is classified as Confidential under this policy, encrypted at rest, and shared only with appropriate and authorized personnel when necessary.

**Use:**

Participation in course activities including accessing and responding to discussion items, receiving, submitting assignments and quizzes, and retrieving course content. Identity information is used to control access to resources appropriate to the role that a student has in a course.

**Disclosure:**

1. SFU Enterprise and SFU Beedie IT and Administrative staff who are responsible for administering the Canvas presence for these programs at the course level and configuring the Canvas application overall
2. Instructors can see submitted content from the student as well as personal information related to enrollment and participation in the course (Name information, email address, page view counts and URLs of course content for those courses)

that the instructor and the student are enrolled in; instructors can only view information for students enrolled in their own courses)

3. Students can see the names of classmates enrolled in the same course and the publicly posted discussions, questions, and/or personal statements published by those students.

**Retention:**

1. Course data is retained on the server after the course is completed unless deleted by a course administrator. SFU course content that is used to evaluate a student is required to be kept for one year following the final exam of a course in order to support grade appeal processes. See RRSDA 1995-018, Examination Papers and Course Assignments.
2. Student information is required while the student is in a program that requires access to Canvas and will be maintained in the Canvas' user database until deleted/removed by administrative staff or deprovisioning processes.

### 2.3.1.2 Instructor (Employee) Information

**Collection:** Instructors contracted or hired to teach a course in Canvas will be added by SFU Beedie staff administrators using their name and email. Once enrolled in their course(s) of instruction, instructors may choose to add additional details including a biographical/professional profile summary, learning module content in the form of written content, slides, presentations, videos or illustrations, discussion posts, comments, and feedback for students.

**Access:**

The data may be accessed by authorized members of SFU Faculty, staff and students enrolled in related courses. Access is scoped to appropriate levels for a given role in the system (e.g., a student needs to be able to identify other course participants in order to engage in discussion or group work; an instructor must be able to see the entire class list for meaningful interaction and administrative needs such as grading).

User access is controlled by role assignment within the application.

**Instructor access:** Instructors will have access to the following, only for courses to which they are assigned "instructor" access: Co-instructor(s) name and email address, published discussion or answer/question posts, announcements, published and draft course content (learning module content, assignments, quizzes, etc).

**Student access:** Students may access the following only for courses they have been enrolled in: Instructor name, instructor email, published discussion posts, announcements, or question/answer posts, learning module content published by instructors (not PI).

**Staff Administrator access:** SFU-Beedie staff administrators will have access to the following for courses they administrate student names and emails for the purposes of enrollment in courses and communication about course related matters, instructor name and email for assigning instructors access to courses and providing communication and support, draft and published learning module content (not PI) for providing technology support.

Activities such as using course module are logged by URL and time and that information is visible to the course instructor and institutional Canvas account administrators with appropriate roles in the student's courses.

Logs of activities, IP addresses and other information necessary for security, audit logging, and similar operational activities of the service by Instructure are visible to their staff under Instructure's Data Classification, Handling and Encryption Policy. Customer data and identity information is classified as Confidential under this policy, encrypted at rest, and shared only with appropriate and authorized personal when necessary.

**Use:**

Identity information is used to control access to resources appropriate to the role that an instructor has in a course and to make it possible for students to identify and communicate with the instructor as needed by the course. The instructor's role information in Canvas also indicates to support staff within SFU IT and at Instructure what requests may be made by the user.

**Disclosure:**

1. SFU Enterprise and SFU Beedie IT and Administrative staff who are responsible for administering the Canvas presence for these programmes at the course level and configuring the Canvas application overall.
2. Students enrolled in a course led by the instructor for purposes of communication in course related activities.

**Retention:**

1. Instructor data is kept with the course until the course or data is deleted as well as in Canvas' account database until deleted by an administrator of the Canvas account. Personal student data will be deleted after one year per SFU retention policies. Learning materials produced by the instructor will be retained until the instructor deletes them or the archived course is deleted.

### 2.1.1. Administrator / Supervisor (Employee) Information

**Collection:** SFU Beedie staff assigned to administrate courses may be enrolled in canvas using their name and email. Canvas may log time and date of last access which may be used to manage versioning of page layouts and course content production supported by the staff member.

**Access:**

The data may be accessed by authorized members of SFU staff with administrative access and support staff employed by Instructure (the personnel are often located outside of Canada even though the data is hosted in a Canadian data centre).

User access is controlled by role assignment within the application.

Activities such as using course module or performing configuration changes are logged by URL and time and that information is visible to the course instructor and institutional Canvas account administrators with appropriate roles in the student's courses.

Logs of activities, IP addresses and other information necessary for security, audit logging, and similar operational activities of the service by Instructure are visible to their

staff under Instructure's Data Classification, Handling and Encryption Policy. Customer data and identity information is classified as Confidential under this policy, encrypted at rest, and shared only with appropriate and authorized personal when necessary.

**Use:**

Identity information is used to control access to resources appropriate to the role that an administrator has in the system. Canvas has an extensive permission system to allow primary system administrators to create and maintain additional roles with access restricted to specific administrative tasks. Roles pre-exist for common activities such as Course designer, sub-account administrator, rubrik-manager, etc.

**Disclosure:**

Name, email address, and activity times may be exposed in the context of tools where that information is normally provided as part of the interaction (e.g., if an administrator chooses to interact with another user via the discussion/chat interface). Named administrators will be identifiable by role generally by other administrators in the institutional account and to support resources at Instructure who require that information in order to provide service in response to support requests.

**Retention:**

Administrator personal information is required to remain in the system as long as the administrator has a role in the system and will not automatically expire. User accounts for administrators would only be disposed of when the administrator no longer retains a role in the Canvas system.

## 2.2. Scope of this PIA

Explain exactly what the PIA covers and conversely what it does not.

This PIA covers:

1. The use of Instructure Canvas by the SFU Beedie School of Business for use with The *Digital Transformation Management Program* and required as part of the conditions of funding from the Digital Technology Supercluster

This PIA does not cover:

1. Further use of Canvas for courses beyond this or general institutional usage
2. Use of tools that are possible to integrate with the Canvas environment that may use data centres beyond those run by Instructure in the AWS Canada Zone. At this time no system integrations are planned. Any future integrations will require separate assessments for privacy and security compliance.

## 2.3. Related PIAs

Identify PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative.

SFU Canvas PIA for on-premise installation (PIA 2013-003).

## 2.4. Elements of Information or Data

List the types of personal information involved in the initiative (if applicable). This could include the individual's name, age, address, work/home email, work/home phone number, educational history, employment history, work status, health information, financial information, photos, comments, or opinions about third parties. See Schedule A for a partial list of types of personal information.

### 2.4.1. Student Data Elements

1. Last Name
2. First Name
3. Optional: Students may elect to provide a preferred alternative name
4. Email address (user provided email address of participating student)
5. Date and time stamp of logins and course activities (e.g. Date/time stamped assignment submissions, discussion posts, quiz submissions)
6. IP address
7. Canvas course enrollment information
8. Optional: students may choose to post a brief biographical profile statement visible to classmates, instructors, and staff administrators
9. User submitted course content such as documents for assignments or contributions to online discussions

### 2.4.2. Instructor (employee) data elements

1. Last Name
2. First Name
3. Optional: Students may elect to provide a preferred alternative name
4. Email address (user provided email address of participating student)
5. Date and time stamp of logins and course activities (e.g. Date/time stamped assignment submissions, discussion posts, quiz submissions)
6. IP address
7. Canvas course enrollment information
8. Optional: students may choose to post a brief biographical profile statement visible to classmates, instructors, and staff administrators
9. User submitted course content such as learning module content, documents for assignments, feedback on student assignments, or contributions to online discussions

### 2.4.3. Administrator (Employee) Data Elements

1. Last Name
2. First Name
3. Email address (SFU email address of participating employee)
4. Date and time of logins and logs of activities
5. IP address

### 2.5. Storage or Access outside Canada

Provide a brief description of whether the personal information can be accessed from outside Canada. For example, by a service provider that is repairing a system, or if the information is being stored outside Canada, for example, in the "cloud". If the data is stored within Canada and accessible only within Canada, please indicate this and describe with whom and where it is stored.

All data for Instructure’s hosting resides in Amazon AWS servers within Canada. However, support for instructors and students will be provided by Canvas support in other regions including the United States. Instructure has agreed to the terms of the Privacy Protection Schedule with the exception of two items:

- Section 15: In order to provide support, Instructure staff located in regions outside of Canada need to access the Canvas course data, including personal information of student and instructor participants. The support staff also use Salesforce as their ticketing and CRM system, which stores both customer contact data and student information related to the ticket. This disclosure is necessary in order to provide the services and may be covered by Section 21(b)(i).
- Section 26: Instructure’s standard for providing information about unauthorized disclosure of information is 48 hours.

### 2.6. Data-linking Initiative

<p>In FIPPA, "data linking" and a "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you must comply with requirements under the Act for a data-linking initiative.</p>	
<p>1. Personal information from one database is linked or combined with personal information from another database</p>	<input checked="" type="checkbox"/> <b>Yes</b> <input type="checkbox"/> <b>No</b>
<p>2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled</p>	<input type="checkbox"/> <b>Yes</b> <input checked="" type="checkbox"/> <b>No</b>
<p>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</p>	<input type="checkbox"/> <b>Yes</b> <input checked="" type="checkbox"/> <b>No</b>
<p>If you answered "yes" to all three questions, please contact the Information and Privacy Coordinator or Officer to discuss the requirements of a data-linking initiative.</p>	

**2.7. Common or Integrated Program or Activity**

<p>In FIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 questions, you must comply with requirements under the Act for common or integrated programs and activities.</p>	
<p>1. This initiative involves a program or activity that provides a service (or services)</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>2. Those services are provided through: 1) a public body and at least one other public body or agency working collaboratively to provide that service; or 2) one public body working on behalf of one or more other public bodies or agencies</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>3. The common or integrated program or activity is confirmed by a written agreement that meets the requirements set out in section 12 of the FIPPA Regulation (link to the <a href="#">Regulation</a> and read section 12)</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>If you answered “yes” to all three questions, please contact the Information and Privacy Coordinator or Officer to discuss the requirements of a common or integrated program or activity.</p>	

**3. Collection, Use and Disclosure of Personal Information**

**3.1. Personal Information Flow Diagram / Table**

Complete the table(s) below (if applicable). Include a personal data flow diagram (if one exists) as well as completing the table(s). See Schedule B for a list of the privacy rules. Use the hyperlink to the Act in Schedule B to identify the specific rule and cite the appropriate section number in the “Legal Authority” column.

**3.1.1. Student Data Flow**

<b>Personal Information Flow Table</b>			
	<b>Description/Purpose of Activity</b>	<b>Privacy Rule</b>	<b>Legal Authority</b>
1.	Account data for student users (Name, external email address, SFU affiliation) is entered by program administrators for the purposes of populating courses with students	Collection, Use	26 (a) and (c) 32
2.	System or service data is stored on Amazon Web Services managed by Instructure inside Canada	Storage Disclosure	33.2
3.	Student-generated content including assignments, course-related documents, or discussion participation stored in Amazon Web Services Canadian data centre	Disclosure	33.2
4.	SFU Program Administrators adds student to enrolled courses for the appropriate stage of the student’s progress. Classmate names, and self-	Collection Disclosure	26 (a) and (c) 33.2

	published discussion posts, comments, and personal statements are visible to other students in the same course(s)		
5.	Student or instructor searches for and selects students within their course(s) in order to communicate or participate in assignments and discussions	Use Disclosure	32 33(2)
6.	Students may follow help link within the application to request assistance with the operation of the Canvas application. Support staff outside of Canada may need to look at course and student data in order to resolve issues or provide solutions	Disclosure outside of Canada	33.1 33.1

**3.1.2. Instructor Data Flow**

Personal Information Flow Table			
	Description/Purpose of Activity	Privacy Rule	Legal Authority
1.	Account data for instructor users (Name, external email address or SFU email address, SFU affiliation) is entered by program administrators for the purposes of creating a user profile for the instructor and assigning them role of "instructor".	Collection	26 (a) and (c)
2.	System or service data is stored on Amazon Web Services managed by Instructure inside Canadian data centres	Storage Disclosure	33(2)
3.	Instructor-generated content including assignments, course-related documents, or discussion participation is used as student learning resources (instructor's research, lecture material and feedback on student questions) stored in Amazon Web Services Canadian data centre	Storage Disclosure Use	33(2) 32
4.	Instructor may follow help link within the application to request assistance with the operation of the Canvas application. Support staff outside of Canada may need to look at course and student data in order to resolve issues or provide solutions	Disclosure outside of Canada	33.1

**3.1.3. Administrator / Supervisor (Employee) Information**

Personal Information Flow Table			
	Description/Purpose of Activity	Privacy Rule	Legal Authority
1.	Instructure administrators may monitor sessions, at SFU's request, to install, implement, maintain, repair, troubleshoot or upgrade the system.	Disclosure outside of Canada	33.1

### 3.2. Risk Mitigation Table

Complete the table(s) below. Describe the risk and the mitigation strategy. Use the terms "High", "Medium" or "Low" to rate the "Likelihood" and "Impact" of each risk. In cases where the risks are substantially different for the individuals whose personal information is in SFU's custody or under its control, complete a table for each group. In cases where the risks are substantially similar or the same, complete only one table.

#### 3.2.1. Risks to Student Data

The following table outlines a complete list of the anticipated risks this system may present to student data and any mitigations strategies in place.

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Non-compliance with FIPPA privacy notification requirement.	<ul style="list-style-type: none"> <li>Collection notices will be presented to students</li> </ul>	Low	Low
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
3.	Vendor does not comply with BC's FIPPA	<ul style="list-style-type: none"> <li>Vendor has agreed to sign SFU's standard Cloud PPS</li> </ul>	Low	High

#### 3.2.2. Risks to Instructor and Administrator (Employee) Data

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Same as above			

### 3.3. Collection Notice

In order to allow individuals the ability to exercise their information rights with knowledge of how their information will be used, they must be notified at or prior to the time of collection. Section 27(2) of the Act requires that the individual from whom personal information is collected be told: a) the purpose for collecting it, b) the legal authority for collecting it, and c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Describe below how and when notice will be given to individuals. Include the specific collection notice(s) that will be used. Link to SFU's [collection notice templates](#).

**3.3.1. Student Collection Notice**

The personal information obtained through Canvas, SFU Beedie's learning management system, and external learning tools, is collected under the general authority of the University Act (R.S.B.C. 1996, c. 468) and the Freedom of Information and Protection of Privacy Act (R.S.B.C. 1996, c. 165). It is related directly to and needed by the University to operate its academic programs and provide instruction. The information will be used for teaching, learning, assessing student academic performance and assigning grades. Aggregate student engagement data (e.g., total hours spent logged into courses, number of modules viewed, etc.) may be used to inform course design and planning. If students have any questions about the collection and use of this information please contact Saskia Morgan, Project Manager, Digital Transformation at 778-782-9357.

Students are not permitted to integrate external learning tools within their Canvas courses.

**4. Security of Personal Information**

Describe below the specific measures that will be used to protect the personal information from unauthorized collection, access, use, disclosure, retention and disposal. See Schedule C for a list of common types of security measures.

**4.1. Physical Security Measures**

[Redacted]

**4.2. Technical Security Measures**

[Redacted]

**4.3. Security Policies, Procedures and Standards**

SFU collects personal information under the general authority of the University Act (R.S.B.C. 1996, c. 468) and other applicable administrative policies approved by the University's Board of Governors; other provincial or federal legislation or regulation; and, binding legal contracts such as collective agreements.

Link to University Act:

[http://www.bclaws.ca/EPLibraries/bclaws\\_new/document/ID/freeside/00\\_96468\\_01](http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_96468_01)

All personal information provided for the University's administrative and operational purposes and any other information placed into a student, alumnus, employee personal record will be collected, protected, used, disclosed, and retained in compliance with British Columbia's Freedom of Information and Protection of Privacy Act (R.S.B.C. 1996, c. 165).

Link to Freedom of Information and Protection of Privacy Act:

[https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165\\_00](https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00)

Usage of Canvas Cloud by SFU staff, faculty, and students is governed by the SFU Fair Use of Information and Communication policy (GP 24)

<https://www.sfu.ca/policies/gazette/general/gp24.html>

Link to SFU Fair Use of Information and Communication policy:

<https://www.sfu.ca/policies/gazette/general/gp24.html>

**4.4. Tracking Access / Access Controls**

Describe the controls used to track access by authorized users of the personal information.

[Redacted content]

[Redacted]

[Redacted]

[Redacted]

**4.5. Information Classification Standard**

(Note: this standard is under development – please leave this section blank). Using Information Technology Services' standard for classifying the sensitivity, access restrictions and minimum-security requirements for information, identify the specific classification level that applies to this initiative.

Data stored, processed and/or transmitted by this system has been classified as Regulated Data, according to SFU Data Classification Standards.

The Regulated Data classification level applies specifically because the data involved contains personally identifiable information (see 2.6) which requires compliance with external regulations (FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT).

SFU Regulated Data standards need to be applied to this system. Exceptions and compensating controls should be noted below this section.

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

█ [Redacted]

█ [Redacted]

█ [Redacted]

Exceptions and compensating controls:

█ [Redacted]

## 5. Accuracy, Correction and Retention of Personal Information

### 5.1. Updating and Correcting Personal Information

Describe here (if applicable) the procedure to allow individuals to routinely update or correct their personal information using regular channels (e.g., a student uses the SIS to update a home address or telephone number, an employee uses the HAP system to update emergency contact information, etc.).

In the absence of a routine process, this requirement would default to SFU's formal procedure [Requesting a Correction to Personal Information in University Records](#).

1. Student information will be entered and maintained by program staff as this category of students have identities external to SFU systems; requests for changes would be directed to Program Administrators
2. Employee and administrator information will initially be manually entered by Enterprise IT staff or Beedie Local IT staff.

### 5.2. Decisions That Directly Affect an Individual

Describe here (if applicable) how the information will be used to make decisions that directly affect an individual.

Documents, discussion posts, quizzes, and other student-user submitted materials may be used for the assessment and grading of course performance as it relates to the posted marking rubrics and/or grading, and performance evaluation criteria specific to the course.

Date stamped assignment and post submissions may be used to assess late assignment penalties or participation marks.

### 5.3. Records Retention and Disposal

Cite the approved SFU Records Retention and Disposal Authority (RRSDA) that apply to the records series generated through this initiative. Link to SFU's [Directory of University Records](#) to determine if an approved RRSDA exists for these records.

If no approved RRSDA exists, describe how the records will be kept in the meantime. Note that if an individual's personal information is used by or on behalf of SFU to make a decision that directly affects the individual, SFU must retain the personal information for at least one year after being used. This is to ensure that the affected individual has a reasonable opportunity to obtain access to that personal information.

Student-provided content and data will be retained and disposed of in accordance with governing RRSDAs for the handling of course-related data within the SFU Beedie School of Business. In the event that conflicting opinions about applicable RRSDAs arise, the SFU Archives will provide guidance about proper record disposition.

## 6. Further Information

### 6.1. Systematic Disclosures of Personal Information

Describe here (if applicable) any usual disclosures inside the University between the office with primary responsibility for the personal information and other SFU departments and programs. Also describe any usual disclosures outside the University between SFU and another public or private body (e.g., provincial, territorial or federal government ministry, department or agency; university or college; transit authority; law enforcement agency).

If SFU and one or more other parties have signed an Information Sharing Agreement, include a copy with this completed PIA. An Information Sharing Agreement sets terms and conditions on the collection, use, disclosure and protection of personal information by the parties to the agreement.

None known.

### 6.2. Access for Research or Statistical Purposes

Describe here (if applicable) any usual disclosures of the personal information made by your department for a research purpose, including statistical research, and how you comply with [section 35 of the Act](#).

None known.

### 6.3. Personal Information Directory (PID) and Personal Information Banks (PIB)

The Personal Information Directory (PID) contains descriptions of the Personal Information Banks (PIBs) created and maintained by Simon Fraser University. A 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 to an individual. PIB entries are added to the Directory as PIB records series are identified and scheduled.

Cite the PIB that apply to the records series generated through this initiative. Link to SFU's [Directory of University Records](#) and search the Personal Information Directory to determine if a PIB description exists for these records.

If no PIB description exists, create one below using the outline described in the [Personal Information Directory](#).

**Title:** SFU Beedie School of Business Salesforce: Executive Education

**Location:** Beedie School of Business, Simon Fraser University

**Types of personal information:** Students, alumni, and business contacts of SFU Beedie School of Business, Executive Education department including name, email, address, date of birth, employment information (if/when provided).

**Purpose for which personal information obtained / compiled and used / disclosed:** Information is obtained by voluntary disclosure by contacts, and is used to manage accurate, up to date contact details and basic communication records for business and non-credit student contacts.

**Individuals using personal information or to whom it is disclosed:** SFU Beedie Executive Education staff use personal information to manage applications and confirm enrollment lists for non-credit students, to coordinate contact and communication preferences of constituents, and to coordinate contact management among staff.

**Individuals included in the PIB:** Executive Education students, business contacts, executive education program alumni.

**Legal authorities for the collection of personal information:** The University Act [RSBC 1996] c .468 and the Freedom of Information and Protection of Privacy Act [RSBC 1996] c. 165

**RRSDA number(s):**

## 7. Coordinator of Information and Privacy Comments

### 7.1. Information or Materials Reviewed

The Coordinator will describe here any additional resources and authorities consulted when reviewing and commenting on the completed PIA.

I reviewed and considered:

1. PIA 2013-003, Canvas LMS
2. Feedback from Mike Stanger, Associate Director of Learning and Community Systems, IT Services
3. Feedback from Saskia Morgan, Project Manager, Digital Transformation, Beedie School of Business

### 7.2. Conditions of Approval

The Coordinator will describe here any recommended conditions to be considered by the University officer with delegated decision-making authority under the Act, who approves the completed PIA.

Recommended conditions are:

1. [REDACTED]

S.15(1)(l)

S.15(1)(l)

[Redacted]

[Redacted]

[Redacted]

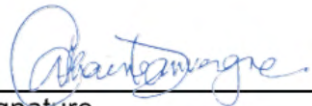

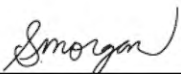
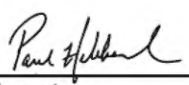
[Redacted]

[Redacted]

[Redacted]

### 8. Approval and Signatures

The undersigned confirm that they have taken reasonable steps to confirm that the contents of this PIA are accurate and complete.

Catherine Dauvergne VP Academic and Provost	 Signature	March 11, 2022 Date
Jennifer Beale Executive Director, Executive Education	 Signature	Date
Saskia Morgan Project Manager, Executive Education	 Signature	Date
Paul Hebbard Coordinator of Information and Privacy	 Signature	January 28, 2022 Date

### Schedule A

#### Definition of terms

<b>Access</b>	Disclosure of personal information by the provision of access to personal information.
<b>Anonymize</b>	Present the results of a process in such a way that individuals whose personal information is contained in the records cannot be identified, and no linkages can be made between any personal information found in the records and personal information that is publicly available from other sources.
<b>Authorized access</b>	Occurs when a person has access to personal information in the custody or control of the University that is authorized by the Act.
<b>Consistent purpose</b>	A use of personal information is consistent with the purpose for which the information was obtained or compiled if the use: <ol style="list-style-type: none"> <li>1. has a reasonable and direct connection to that purpose, and</li> <li>2. is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.</li> </ol>
<b>Contact information</b>	Information that enables an individual at a place of business to be contacted; includes name, position title, business telephone number, business address, business email or business fax number of the individual.
<b>Data linking</b>	The linking or combining of personal information in one source with personal information in one or more other sources if the purpose of the linking or combining is different from: <ol style="list-style-type: none"> <li>1. the purpose for which the information in each database was originally obtained or compiled, and</li> <li>2. every purpose that is consistent with each purpose referred to in paragraph (a).</li> </ol>
<b>Disclose</b>	Reveal, show, expose, provide copies of, sell, give or tell.  SFU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3 of the Act.
<b>Employee</b>	A person employed for wages or salary by the University. In relation to SFU, includes: (a) a volunteer and (b) a service provider (see also the definitions for each of the latter terms).
<b>Individual identifier</b>	Information that would enable a third party to deduce the identity of the person concerned; examples include a person's name, Social Insurance Number, student number, employee number, address, date of birth (usually used in combination with other identifiers).

**Instructor** Individuals responsible for the teaching of credit and non-credit courses including professors, associate professors, assistant professors, professors emeritus, adjunct professors, visiting faculty, practitioner faculty, post-retirement appointees, lecturers, instructors, teaching assistants, tutors and markers, faculty associates, in-service associates, associate members and program coordinators.

**Personal information** Recorded information about an identifiable individual, other than business contact information, including but not limited to:

1. names, home addresses and telephone numbers;
2. age;
3. sex;
4. marital or family status;
5. identifying number;
6. race, national or ethnic origin;
7. colour;
8. religious or political beliefs or associations;
9. educational history;
10. medical history;
11. disabilities;
12. blood type;
13. employment history;
14. financial history;
15. criminal history;
16. images;
17. anyone else's opinions about an individual;
18. an individual's personal views or opinions; and,
19. name, address and phone number of parent, guardian, spouse or next of kin.

**Record** Includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

**Service provider** A person retained under contract to perform services for SFU or a person with whom an employee automatically enters into an agreement by virtue of using their product or service and in so doing accepts the service provider's terms of use.

**Unauthorized collection, use, disclosure and disposal** Occurs when a person who has access, whether authorized or unauthorized, to personal information in the custody or control of the University, collects, uses, discloses and disposes of that information and it is not authorized by the Act.

**Use** Employ information to accomplish a specific purpose.

**Volunteer** A person who provides a service to the University without being paid.

### Schedule B

[FIPPA table of contents](#)

#### Collection, Accuracy, Correction, Protection and Retention of Personal Information

<b>Collection</b>	Section 26	Purpose for which personal information may be collected <ol style="list-style-type: none"> <li>1. Prescribes the only situations in which SFU is permitted to collect personal information</li> <li>2. Collect only the minimum personal information related directly to and necessary for the particular purpose</li> </ol>
	Section 27	How personal information is to be collected <ol style="list-style-type: none"> <li>3. Prescribes that SFU must collect personal information directly from the individual the information is about except in very limited and specified circumstances</li> <li>4. Prescribes when a collection notice is required and not required to be given to individuals</li> </ol>
	Section 27.1	When personal information is not collected <ol style="list-style-type: none"> <li>5. Describes the situation when personal information is received by SFU but not collected</li> </ol>
<b>Accuracy</b>	Section 28	Accuracy of personal information <ol style="list-style-type: none"> <li>1. Prescribes that SFU must make every reasonable effort to ensure that the personal information it uses is accurate and complete</li> <li>2. Information collected by the University is often used to make a decision that directly affects the individual. Ensure this information is accurate because using out-dated information may result in serious consequences for the individual and the University</li> </ol>
<b>Correction</b>	Section 29	Right to request correction of personal information <ol style="list-style-type: none"> <li>1. Prescribes how SFU must handle a request made by an individual to correct her or his information</li> <li>2. Where factual errors in personal information are identified, the University is responsible for making the appropriate corrections upon request. If the incorrect information was made available to a third party, the University is responsible for providing the corrected information to that third party</li> </ol>

<b>Protection</b>	Section 30	<p>Prescribes that SFU must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal</p> <ol style="list-style-type: none"> <li>1. The media on which information is stored (paper or digital) must be considered when deciding what reasonable physical, technical and procedural security measures are necessary to adequately protect the personal information</li> </ol>
	Section 30.1	<p>Storage and access must be in Canada</p> <ol style="list-style-type: none"> <li>2. Prescribes that SFU must ensure that personal information in its custody or under its control is stored and accessed only in Canada except in very limited and specified circumstances</li> </ol>
<b>Retention</b>	Section 31	<p>Retention of personal information</p> <ol style="list-style-type: none"> <li>1. Prescribes that SFU must ensure that 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</li> </ol>

**Use and Disclosure of Personal Information**

<b>Use</b>	Section 32	<p>Use of personal information</p> <ol style="list-style-type: none"> <li>1. Prescribes the only situations in which SFU may use the personal information it collects</li> <li>2. Consider the difference between “use” (within the University office that collected) and “disclosure” (making information available to anyone else inside or outside the University)</li> </ol>
<b>Disclosure</b>	Section 33	<p>SFU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3</p> <ol style="list-style-type: none"> <li>1. Describes the situations in which personal information may be released to another person. The circumstances under which personal information may be disclosed are prescribed in very specific and limited terms, therefore, it is important to confirm that one has legal authority to disclose personal information before doing so</li> </ol>
	Section 33.1	<p>Disclosure inside or outside Canada</p> <ol style="list-style-type: none"> <li>2. Prescribes the only situations in which SFU may disclose personal information inside or outside Canada</li> </ol>

- Section 33.2 Disclosure inside Canada only
  - 3. Prescribes the situations in which SFU may disclose personal information inside Canada only
  
- Section 33.3 Disclosure of personal information in records available to public without request
  - 4. Prescribes the situation when SFU may disclose to the public a record that is within a category of records established under section 71(1)
  
- Section 35 Disclosure for research or statistical purpose
  - 5. Prescribes the situation when SFU may disclose personal information in its custody or under its control for a research purpose, including statistical research

### Schedule C

<b>Types of security measures</b>	
<b>Physical</b>	<ol style="list-style-type: none"> <li>1. SFU data centre and backup data centre are both located on SFU campuses in Canada</li> <li>2. Locked doors</li> <li>3. Key card and electronic access control devices</li> <li>4. Securely stored computing equipment</li> <li>5. Receptionist supervision</li> <li>6. Physical barrier to the public</li> <li>7. Staff only access</li> <li>8. Alarm systems</li> <li>9. After hours security patrol checks</li> </ol>
<b>Technical</b>	<ol style="list-style-type: none"> <li>1. Firewalls</li> <li>2. Encrypted network transmission</li> <li>3. Tiered network infrastructure</li> <li>4. Identity assurance provided by SFU's main Systems of Record</li> <li>5. Role-based user access assigned on a need-to-know basis</li> <li>6. Log-on user ID and password (single sign-on) provided by SFU's Central Authentication Service (CAS)</li> <li>7. Timed out computer sessions</li> </ol>
<b>Security Policy, Procedure and Standards</b>	<ol style="list-style-type: none"> <li>1. University Policies e.g., GP-24 Fair Use of Information Systems, I 10.04 Access to Information and Protection of Privacy, I 10.05 Collection of Personal Information, I 10.09 Retention and Disposal of Student Exams or Assignments, and I 10.10 Confidentiality Policy</li> <li>2. Designation and authentication of authorized users is managed through SFU's Identity and Access Management (IDAM) infrastructure, which is registered with the Canadian Access Federation (CAF)</li> <li>3. SFU's IDAM infrastructure is benchmarked against the InCommon assurance program (<a href="http://incommn.org">http://incommn.org</a>), which certifies campuses, non-profits and research organizations to determine the accuracy of a user's electronic identity and help mitigate risk for the service provider. While InCommon certification is not available outside the US, the assurance program serves as a benchmark for international standards and best practices</li> <li>4. SFU's Privacy Protection Schedule is included as part of a signed agreement with a service provider of digital storage when purchased through Procurement, which includes provisions relating to data ownership, use, disclosure, security, retention and confidential/permanent deletion</li> <li>5. SFU has signed an Information Sharing Agreement with the public body describing the terms and conditions of their data-linking initiative or common or integrated program or activity</li> <li>6. Authorized users of the IT system are made aware of protection of privacy rights and responsibilities by means of notices when logging onto the system;</li> </ol>

	<p>education by through the SFU website, workshops and advisory service; and/or signing SFU's Privacy and Confidentiality Agreement</p> <p>7. Personal information is retained and disposed of according to an existing Records Retention Schedule and Disposal Authority approved by the University Archivist</p>
<b>Tracking Access / Access Controls</b>	<p>1. IDAM infrastructure assures identity</p> <p>2. Role-based access management infrastructure authorizes access</p> <p>3. Auditable log files</p>