



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

PRIVACY IMPACT ASSESSMENT
for
Examity

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

Office of primary responsibility	Associate Vice-President, Learning and Teaching	Approved date	Sep. 28, 2020
PIA #	2020-012	OIPC notified date	
Type of PIA	☐ Department ☒ Corporate ☐ Update	OIPC response date	
Type of PIA review	☐ Policy ☒ System ☐ Project		
(Check all that apply)	☐ Program ☐ Activity		
Other applicable PIA provisions	☐ Common or integrated program ☐ Data-linking initiative		
(Check all that apply)	☐ Information sharing agreement		

2. General Information

2.1. Unit and Program Area

Identify the Department and Program submitting this PIA

Department:	Associate Vice-President, Learning and Teaching
Program:	Examiity

2.2. Contact

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

Name of PIA Drafter:	Stephen MacGregor		
Position Title:	Information Compliance Architect, IT Services		
Phone:	22319		smacgreg@sfu.ca
Name of Program Manager:			
Position Title:			
Phone:			

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

With the move to remote instruction in March 2020 due to COVID-19, and the need for some courses to include online exams, concerns about academic dishonesty have been raised. The University takes academic misconduct seriously, and acknowledges the need to address this

issue proactively and rigorously, in accordance with SFU's Student Academic Integrity Policy (S10.01). Our students should feel confident in the integrity of their grades and the value of their degrees. Because of the physical distancing restrictions imposed by the ongoing COVID-19 pandemic, in-person proctoring is not feasible. Accordingly, while we are learning and taking exams remotely during this pandemic, SFU needs to temporarily adopt diverse methods to improve how we invigilate online exams, and Examity is one such tool. In the interest of continuously improving the services that SFU offers, online exam proctoring may continue after the COVID-19 physical distancing restrictions have eased. However, the current decision is to use Examity for the duration of remote instruction. Therefore, we will be relying on M180 (Ministerial Order) as authority for instructors currently located outside of Canada to access Examity.

Examity can record student identity via webcam, and then relies on video and audio recording using the webcam and microphone on the student's computer. The program also captures screenshots and/or keyboard activity during the session as required. Instructors control administrative settings. The video is not accessible to Examity staff but only to instructors and other staff (registrar, department chair) at SFU. Based on activities flagged by the software, instructors would decide whether an academic integrity breach may have occurred and whether to file an academic integrity report. SFU does not plan to use Examity's human ID verification or human anomaly review services, ensuring that video captured would only be accessible to SFU staff.

Students must have video and audio capture capabilities on their computer and they must use a compatible web browser with the Examity add-on.

2.3.2. Student Information

Collection: student name, email, phone number, image of SFU ID Card, and "typing cadence" are required to create a profile and access the service. Phone numbers are gathered as part of a student's Examity profile so that they can be contacted directly in case of a disconnection. Course information is required to pair the student with available exams. This information is made available to Examity through an encrypted LTI session token that is handed to Examity from Canvas during the session handover process. SFU ID Card image and typing cadence are captured at exam time and compared to profile data. Image (video) and behaviour is captured during the exam.

Access: video recordings of students taking exams, including sounds, will be available to SFU staff after the exam is complete, including the course instructor and TAs, department chairs or designates and the Registrar (in the case that an academic dishonesty report is filed). It should be noted the SFU staff will not be viewing students "live" but only when activity is flagged. Some students registered with the Centre for Accessible Learning will have their video reviewed by CAL staff rather than by their course instructor.

Use: To monitor behaviour during online exams in a way that is equivalent to live proctoring for in-person exams, in accordance with SFU's Academic Integrity policy.

Disclosure: The files will be disclosed to SFU staff who have access. A file may also be disclosed to the Academic Integrity Coordinator, if necessary for the performance of the job duties of that position. A file may also be disclosed to the student the personal information is about, if it is necessary under S10.05.

Retention: By default, PII is kept by Examity for the duration of the contract. However, Examity has indicated that they are willing to incorporate a custom schedule for purging PII. Proctored recordings are kept in an accessible state (to authorized SFU staff) for thirty days. Recordings

are then archived for an additional thirty days. Recordings that are “red-flagged” are kept for a year.

2.3.3. Instructor (Employee) Information

Collection: Employee name and email are required to enrol and access the service. This information is made available to Examity through an encrypted LTI session token that is handed to Examity from Canvas during the session handover process.

Access: Staff members will have access to their own information in Examity. Students will have access to course instructor name.

Use: Examity uses this information to determine user access control, which specifies which courses to manage, including reviewing student exams, and the ability to create new content.

Disclosure: Information will be disclosed to SFU staff who have access. Information may also be disclosed to the Academic Integrity Coordinator, if necessary, for the performance of the job duties of that position. Information may also be disclosed to the student involved in the proctored exam, if it is necessary under S10.05.

Retention: By default, PII is kept by Examity for the duration of the contract, which is renewed on an annual basis and will be in effect until SFU no longer uses the service. However, Examity has indicated that they are willing to incorporate a custom schedule for purging PII. Proctored recordings are kept in an accessible state (to authorized SFU staff) for thirty days. Recordings are then archived for an additional thirty days. Recordings that are “red-flagged” are kept for a year.

2.4. Scope of this PIA

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

- 1. This PIA covers:
 - 1. Privacy and security of the Examity tool and service
 - 2. Data shared between Canvas and Examity
 - 3. Data collection and recording of proctored sessions
 - 4. Disclosure, retention, and disposition of proctored session recordings.
- 2. This PIA does not cover:
 - 1. Privacy and security of Canvas Learning Management System
 - 2. Supported browser compatibility with Examity
 - 3. Security issues with student computers

2.5. Related PIAs

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

Not applicable

2.6. 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.

2.6.1. Student Data Elements

Attribute	Access	Purpose
First name	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying exam taker.
Last name	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying exam taker.
Given name	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying exam taker.
Email	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying exam taker.
Phone Number	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Used by Examity to contact and support the student in the event of a disconnection during a proctored exam
Exam recording	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Proctor exam by reviewing recording of student taking the exam.
SFU Computing ID	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying exam taker.
Role	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying user role in Examity.
Program of study	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Determine exam access.
Department	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Determine exam access.
Faculty	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Determine exam access.
User Image (profile image stored in Canvas)	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying exam taker.

Image of SFU ID Card	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying exam taker.
Typing Cadence	Examity software	Identifying exam taker.

2.6.2. Employee Data Elements

Attribute	Access	Purpose
First name	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying employee.
Last name	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying employee.
Given name	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying employee.
Email	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying employee.
SFU Computing ID	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying employee.
Role	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Identifying user role in Examity.
Program of study	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Determine access to content.
Department	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Determine access to content.
Faculty	Authorized SFU staff (course instructor and TAs, department chairs or designates and the Registrar)	Determine access to content.

2.7. 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.

Examity is a cloud-based solution, hosted in a Canadian data centre owned and managed by Rogers Communications and service providers contracted by Rogers Communications. Access to Examity is done through the Internet, and international access by students is expected. Access to Examity by SFU staff will generally be from within Canada; however, some staff access

may happen outside of Canada. SFU relies on Ministerial Order M180, which permits personal information to be stored outside of Canada, without consent, provided the third-party application is reasonably secure and the University makes all reasonable efforts to remove personal information from the third party application as soon as is operationally reasonable.

Examity help desk staff (and proctoring agents) are located in India. Examity help desk and support staff may access SFU data during support cases in order to provide assistance. Access by Examity staff is explicitly granted by authorized SFU IT staff on a temporary case-by-case basis. As the helpdesk is providing troubleshooting services, FIPPA s. 33(1.1)(1)(p) is authority for this temporary, time-limited access.

2.8. Data-linking Initiative

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.	
1. Personal information from one database is linked or combined with personal information from another database	☒ Yes ☐ No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled	☒ Yes ☐ 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	☐ Yes ☒ No
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.	

2.9. Common or Integrated Program or Activity

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.	
1. This initiative involves a program or activity that provides a service (or services)	☒ Yes ☐ No
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	☐ Yes ☒ No

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 Regulation and read section 12)	☐ Yes ☒ No
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.	

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

Personal Information Flow Table			
	Description/Purpose of Activity	Privacy Rule	Legal Authority
1.	Student, signed into Canvas, clicks a link to access Examity from within a specific course.	Collection	FIPPA 26(c)
2.	Examity collects PI from LTI token during login, including name, email and academic information (course and program). Examity attempts to match the login info with an existing profile. If a student profile does not already exist in Examity, the student is prompted to create one: entering name, phone number, email address, an image of the student SFU ID Card, and a "typing cadence" is also recorded. No information is passed back into Canvas.	Collection	FIPPA 26(c)
3.	Student selects an available date for a scheduled proctored exam.	Use	FIPPA 32(a), 34(a)
4.	On the scheduled date, student enters Examity and starts Proctored exam. The student must correctly match the saved profile information, including typing cadence previously recorded.	Use	FIPPA 32(a), 34(a)
5.	Student takes exam, using webcam and speaker to record surroundings.	Collection, Use	FIPPA 26(c), 32(a), 34(a)
6.	The Examity software analyses exam data, including video, for indicators of suspicious activity.	Use	FIPPA 32(a), 34(a)

7.	Suspicious exam videos are flagged by SFU staff for further assessment/escalation and investigation.	Use	FIPPA 32(a), 34(a)
8.	Academic dishonesty decisions are made by the authoritative officer based on exam video assessment and further investigation.	Use, Disclosure	FIPPA 32(a), 34(a), 33.2(a), M085.2(a)

S.15(1)(l)

Sample LTI Token Data



3.1.2. Employee Data Flow

Personal Information Flow Table			
	Description/Purpose of Activity	Privacy Rule	Legal Authority
1.	Employee, signed into Canvas, clicks a link to access Examity.	Collection	FIPPA 26(c)
2.	Examity collects PI from LTI token and creates profile if one does not exist.	Collection	FIPPA 26(c)
3.	Employee uses Examity based on access control defined by the LTI token and settings in Examity.	Use	FIPPA 32(a), 34(a)

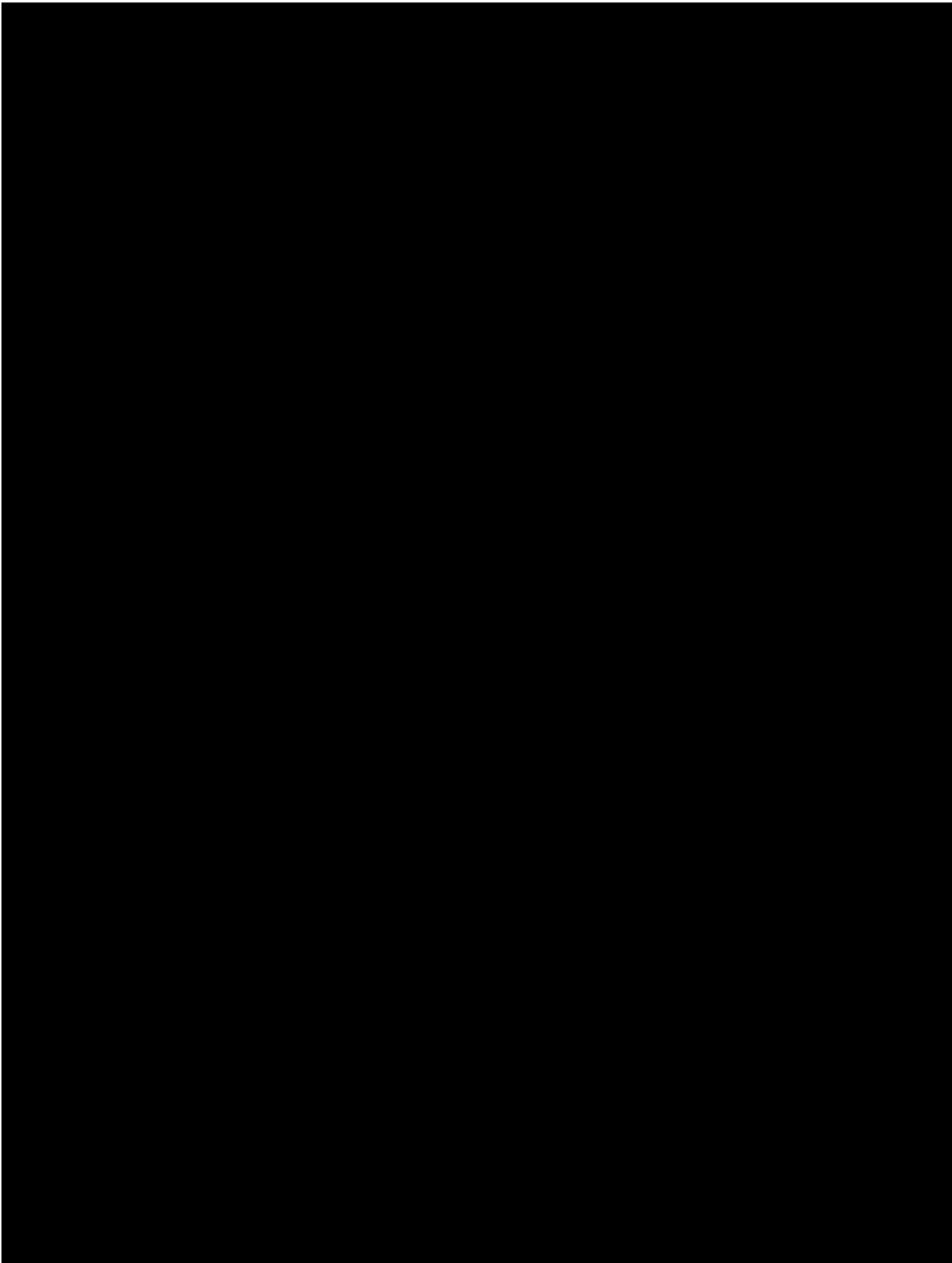
3.1. Risk Mitigation Table

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.

3.1.1. Risks to Student Data

RISK	MITIGATION STRATEGY	LIKELIHOOD	IMPACT



3.1.2. Risks to Instructor and Administrator (Employee) Data

RISK	MITIGATION STRATEGY	LIKELIHOOD	IMPACT

3.2. 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](#).

3.2.1. Student Collection Notice

SFU will provide a standard privacy notification we require instructors to use if they employ Examity for auto-proctoring. Instructors have been told to include the collection notice with each exam.

The collection notice will read:

The information you provide to SFU via Examity is collected under the authority of the University Act and the Freedom of Information and Protection of Privacy Act. It is related directly to and needed by the University to administer SFU Policy S10.01 Student Academic Integrity Policy. The information will be used to verify your identity and proctor your exam. It may be used in an academic dishonesty proceeding. If you have any questions about the collection and use of your information, please contact your instructor.

The AVPLT and CEE will develop FAQs for both instructors and students about Examity including the responsibilities of instructors regarding collection notices. The FAQ for students is as follows:

THE SFU EXAMITY PILOT: FAQ FOR STUDENTS

My instructor says I need to take a proctored online exam. Do I?

Your syllabus will indicate if this is a requirement of the course.

What technology do I need to write an auto-proctored exam?

Students will need a computer or laptop, webcam, microphone, a web browser with the Examity extension, and a reliable internet connection. As almost all instruction is remote this fall, it's reasonable to expect that you will have most of these; if you do not, you should inform your instructor right away who will find an alternative way to proctor your exam.

Can I take my exam on my mobile phone or tablet?

No.

What is Examity?

Examity software acts similarly to an invigilator during an in-person exam. The software records students through video, audio, and/or screen activity while you write. You will not be able to access other applications, websites, or browser tabs during the exam, unless specifically permitted by your instructor who enables the security settings. It is automated, meaning no one is actually watching you while you take the exam.

What is auto-proctoring?

Auto-proctoring is the software version of an invigilator in face-to-face exams. Examity acts as an invigilator would by observing students during an exam and flagging potential issues for review by your instructor or TA, to ensure academic integrity.

Is my personal information protected?

Yes. Examity encrypts the data and it can only be accessed by authorized SFU personnel, like your instructor. The recording and your exam will be destroyed following SFU retention policies that apply to all course material.

Does Examity have access to information stored on my computer?

No. Examity is an extension in your web browser. The software monitors screen activity, keyboard activity, and sounds, to ensure you aren't opening up several browser tabs or performing other suspicious behaviour while taking your text. Examity does not have access to your computer's files or any other personal information, and you should uninstall and remove it once your exams are complete.

What if I have technical issues or my computer crashes while I'm taking an exam?

We have negotiated that you can take a practice exam to ensure Examity works with your computer system. You should check everything is functional prior to your first auto-invigilated exam; instructors have been encouraged to set a practice exam for you. During the exam, technical support is available for you 24/7/365 directly through Examity. If you need assistance during an exam, there is a Live Chat box in the Examity window as well as phone support at 1-855-EXAMITY (1-855-392-6489). Email support is also available at support@examity.com, though of course email response will be less immediate than Live Chat or phone support. Generally, we'd suggest using the Live Chat feature as the first option for support.

In the case of intermittent network disconnections due to things like weak WiFi, the session will not be disrupted. If you lose network connection for more than 60 seconds during the exam, Examity will place a block over the exam screen to protect the content so you have a chance to reconnect. Do not disable the proctoring software or close the browser, as this ends the session! You will be able to rejoin the exam as long as the test session is still active. If the session ends, contact Examity to reset the session; whether you can re-attempt will depend on the settings your instructor has chosen. Those settings should be communicated to you. For other technical issues, you should inform your instructor as soon as possible after the exam and describe the problem.

3.2.2. Instructor and Administrator (Employee) Collection Notice

Not applicable.

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

Examity has implemented the following physical security measures:

[Redacted text block]

4.2. Technical Security Measures

[Redacted text block]

Endpoint Protection

[Redacted]

[Redacted]

[Redacted]

[Redacted]

4.3. Security Policies, Procedures and Standards

[Redacted]

4.4. Tracking Access / Access Controls

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

[Redacted]

[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.

N/A

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](#).

Students are responsible for ensuring the accuracy of their personal information when they take an auto-proctored exam.

If a student wishes to correct or update their personal information, the University will follow SFU’s formal procedure for Requesting a Correction to Personal Information in University Records.

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.

Examity will flag anomalies or potential anomalies in behaviour during a proctored session, and instructors and TAs should review the recordings to assess whether the anomalies may indicate academic dishonesty. Instructor assessments of the anomalies will contribute to their actions (such as filing an academic dishonesty report) which can impact student’s grades and academic standing in the University.

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.

Records used in an academic dishonesty case should be retained in accordance with RRSDA 2006-003 Student Discipline Records (retain for current year case closed + one additional year). Recordings that are not used as evidence in an academic dishonesty case can be destroyed

within 30 days. Apply RRSDA 1999-061, Transitory Records
<http://www.sfu.ca/archives2/dur/rrsdasGeneral.html>
At a minimum these retention instructions will be included in the FAQ associated with the rollout of Examity.

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.

Not applicable.

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](#).

Not applicable

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:
Examity proctored exam recordings

Location:
University department responsible for the exam

Types of personal information:
Identity verification, recorded images, educational history

Purpose for which personal information obtained/compiled and disclosed:

To support SFU policy I10.01 Student Academic Integrity Policy. The information will be used to proctor exams, and may be used in investigations of academic dishonesty

Individuals using personal information or to whom it is disclosed:

Authorized employees of the University. These are course instructors, TAs or TMs, department chairs (or designates), the Registrar, and the Academic Integrity Coordinator

Individuals included in PIB:

Students

Legal authorities for the collection of personal information:

The *Freedom of Information and Protection of Privacy Act* (RSBC, 1996, c. 165) and the *University Act* (RSBC, 1996, c. 468)

RRSDA number:

RRSDA 2006-003 Student Discipline Records and RRSDA 1999-061 Transitory Records.

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.

The Information and Privacy Officer, Bill Trott, reviewed and considered:

- 1. Examity Services Agreement; 2. Rogers Communications Canada, Inc. Type II System and Organization Controls Report (SOC 2)
- 3. Emails and edits of the draft PIA from Stephen MacGregor and Elizabeth Elle

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.

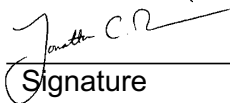
Recommended conditions are:

- 1. Any contemplated changes to or use of this software that differs from the description provided in this PIA (e.g., in the collection, use, disclosure or storage of personal information) must be reviewed by the Archives for compliance with FIPPA. AVPLT must consult with the Archives and Records Management Department prior to implementing any proposed changes.
- 2. If the option to renew for a period January 1, 2021 – April 30, 2021 is exercised, a consent process needs to be established for the out of Canada access by instructors and Examity help desk staff.
- 3. As SFU is relying on FIPPA s. 33.1(1)(p) for authority for the help desk located outside of Canada to access personal information.

- 4. When the customized schedule for the purging of personal information is complete, it should be attached to this PIA.
- 5. Departments using Examity should develop on-boarding and off-boarding procedures to ensure only authorized staff can access Examity.
- 6. Departments should apply RRSDAs 1999-061 and 2006-003 to the invigilation records stored in Examity.
- 7. The AVPLT should establish guidelines for instructors on use of Examity, including the need for collection notices, on reviewing of recordings, and on retention periods for Examity files.
- 8. The AVPLT should add to the student FAQs guidance that the student should ensure no personal information appears in their surroundings.
- 9. As SFU is relying on Ministerial Order M180 to authorize access by SFU staff (including instructors and TAs) based outside of Canada, AVPLT and IT Services must make reasonable efforts to remove personal information from the application as soon as operationally reasonable after December 31, 2020.

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.

<u>Jon Driver</u> Vice-President, Academic	 Signature	<u>September 28, 2020</u> Date
<u>Elizabeth Elle</u> Vice Provost & Associate Vice-President, Learning and Teaching	 Signature	 Date
<u>Stephen MacGregor</u>	 Signature	<u>September 23, 2020</u> Date
<u>Information Compliance Architect, IT Services</u>	 Signature	 Date
<u>Paul Hebbard</u> Coordinator of Information and Privacy	 Signature	<u>September 23, 2020</u> Date

Schedule A

Definition of terms	
Access	Disclosure of personal information by the provision of access to personal information.
Anonymize	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.
Authorized access	Occurs when a person has access to personal information in the custody or control of the University that is authorized by the Act.
Consistent purpose	A use of personal information is consistent with the purpose for which the information was obtained or compiled if the use: 1. has a reasonable and direct connection to that purpose, and 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.
Contact information	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.
Data linking	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: 1. the purpose for which the information in each database was originally obtained or compiled, and 2. every purpose that is consistent with each purpose referred to in paragraph (a).
Disclose	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.
Employee	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).

Individual identifier	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

Collection	Section 26	Purpose for which personal information may be collected
		1. Prescribes the only situations in which SFU is permitted to collect personal information 2. Collect only the minimum personal information related directly to and necessary for the particular purpose
	Section 27	How personal information is to be collected
		3. Prescribes that SFU must collect personal information directly from the individual the information is about except in very limited and specified circumstances 4. Prescribes when a collection notice is required and not required to be given to individuals
	Section 27.1	When personal information is not collected
		5. Describes the situation when personal information is received by SFU but not collected
Accuracy	Section 28	Accuracy of personal information
		1. Prescribes that SFU must make every reasonable effort to ensure that the personal information it uses is accurate and complete 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
Correction	Section 29	Right to request correction of personal information
		1. Prescribes how SFU must handle a request made by an individual to correct her or his information 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

Protection	Section 30	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
		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
	Section 30.1	Storage and access must be in Canada
		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
Retention	Section 31	Retention of personal information
		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

Use and Disclosure of Personal Information

Use	Section 32	Use of personal information
		1. Prescribes the only situations in which SFU may use the personal information it collects 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)
Disclosure	Section 33	SFU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3
		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

- Section 33.1 Disclosure inside or outside Canada
 - 2. Prescribes the only situations in which SFU may disclose personal information inside or outside Canada

- 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

Types of security measures	
Physical	1. SFU data centre and backup data centre are both located on SFU campuses in Canada 2. Locked doors 3. Key card and electronic access control devices 4. Securely stored computing equipment 5. Receptionist supervision 6. Physical barrier to the public 7. Staff only access 8. Alarm systems 9. After hours security patrol checks
Technical	1. Firewalls 2. Encrypted network transmission 3. Tiered network infrastructure 4. Identity assurance provided by SFU's main Systems of Record 5. Role-based user access assigned on a need-to-know basis 6. Log-on user ID and password (single sign-on) provided by SFU's Central Authentication Service (CAS) 7. Timed out computer sessions
Security Policy, Procedure and Standards	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 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) 3. SFU's IDAM infrastructure is benchmarked against the InCommon assurance program (http://incommn.org), 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 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

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