



PRIVACY IMPACT ASSESSMENT (PIA)
for
iClicker

Table of Contents

Before you begin..... 2

PART ONE: PRIVACY REVIEW..... 2

Section 1: GENERAL INFORMATION 2

Section 2: COLLECTION, USE AND DISCLOSURE 9

Section 3: STORING PERSONAL INFORMATION..... 15

Section 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA..... 17

Section 5: ACCURACY, CORRECTION AND RETENTION..... 20

Section 6: ADDITIONAL RISKS 21

Section 7: PRIVACY SIGNATURE 23

PART 2: SECURITY REVIEW..... 25

Section 1: PHYISCAL AND TECHNICAL SECURITY 25

Section 2: ACCESS CONTROL..... 25

Section 3: RISK RESPONSE 26

Section 4: IT COMMENTS AND SIGNATURE 27

PART 3: ACCOUNTABILITY REVIEW 28

Before you begin

This form is used by SFU to determine if a new or a proposed substantial change to a 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). FIPPA 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 risk management and compliance tool to identify potential privacy issues and impacts, allowing correction and mitigation, thus avoiding costly redesign; privacy complaints or breaches; and harm to personal, professional and institutional reputation.

Before you begin this form, please contact the Privacy and Access Program, through the Archives and Records Management Department. See more information about the process here: <https://www.sfu.ca/archives/fippa/privacy-impact-assessments.html>.

PART ONE: PRIVACY REVIEW

Section 1: GENERAL INFORMATION

PIA file number: PIA 2023-062

Initiative title:	Privacy Impact Assessment: iClicker
SFU Department / Faculty:	N/A: Institutional
Branch or unit:	N/A: Institutional
Link to SFU initiative website:	Getting Started with iClickers - Canvas Support - Simon Fraser University (sfu.ca)
Link to vendor website:	iClicker: Student Response Systems & Classroom Engagement Tools
Link to vendor privacy policy:	Privacy Notice Macmillan Learning Student Store
Your name and title:	Kar On Lee, Learning Technology Specialist
Your work phone and email:	cal2@sfu.ca
Initiative Lead name and title:	N/A
Initiative Lead phone and email:	N/A
Privacy Rep name and title:	Ernest Soares, Privacy Legal Counsel
Privacy Rep phone and email:	Ernest_soares@sfu.ca

A. Related PIAs, if any:

- PIA 2023-063 - Top Hat

B. If this initiative involves an external service provider or vendor, has a contract between SFU and the vendor been signed?

- Yes
- This product involves the conclusion of two contracts.
 - (a) One between the SFU instructor and iClicker - MacMillan Learning ("iClicker") which is free; and
 - (b) a second contract between the SFU student and iClicker, which is paid for by the student. SFU is not a party to the second agreement.

C. Has SFU's "Privacy Protection Schedule" been agreed to by the vendor?

- No, but the vendor has committed to adhering to FIPPA as per their privacy policy.

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

This is a student response system which is used in teaching at SFU across all faculties in order to create student engagement and formative assessment in classrooms. It is particularly used in larger undergraduate courses. Typically, the usage is for the duration of the semester but the student is likely going to be involved with several courses that utilize this tool. It may or may not be used for summative or formative assessment as well.

iClicker is an in-classroom student response tool facilitated by software that enables lecturers to pose a question(s) to the students and enables students to respond via the app. Student responses can be made to be anonymous. Data collection may occur at account creation and at response stage depending on the question posed.

Phase 1 – Account creation

An account is required to use iClicker for both an instructor and a student. The first step is to go to www.iclicker.com and click on Create an Account. Choose either Student or Instructor option

Student Account Creation requires the following personal information:

- First name
- Last name
- SFU Email
- Student Number (optional)

The screenshot shows the 'Create Account' page for a student. At the top, there is a blue header with a back arrow and the text 'Create Account'. Below the header, a green message says 'Great! Now, tell us a bit about yourself.' The form contains several input fields: 'First Name', 'Last Name', 'Simon Fraser University-Burnaby Email', 'Confirm Email', 'Student Number' (with a '(Recommended)' note), and 'Password'. The password field has a strength indicator showing '8 characters', 'Lowercase Letter', 'Uppercase letter', and 'Number or special character'. Below the password field is a 'Confirm Password' field. At the bottom, there are two checkboxes: 'I agree to the Privacy Notice and Terms of Use' and 'I agree to the treatment of my personal information as set out below, including access and use of my personal information outside Canada.' A large block of text provides a detailed privacy notice. At the very bottom, there is a 'Create Account' button.

Figure 1: Student Account Creation

Instructor Account Creation requires the following personal information:

- Primary Institution
- Primary Discipline (optional)
- Primary Role

- First Name
- Last Name
- SFU Email

Primary Institution

Simon Fraser University-Burnaby X

Primary Discipline (Optional)

Select Discipline v

Primary Role

Select Role v

First Name

Last Name

Instructor Email

Password

8 characters

Uppercase letter

Lowercase letter

Number or special character

Confirm Password

Instructor Remote ID (Optional)

Can't find your iClicker remote ID?

☐ I agree to the [Privacy Notice](#) and [Terms of Use](#)

☐ I agree to the treatment of my personal information as set out below, including access and use of my personal information outside Canada.

iClicker and my educational institution will collect and use my personal information (including name, email address, student ID as applicable, iClicker course and session information, responses and answers, attendance, and scoring), for the purposes of providing the iClicker online student response system, including questions, scoring responses, recording attendance, and facilitating classroom interaction, in accordance with the Macmillan Learning Privacy Notice. I understand that my personal information from my use of iClicker will be stored on servers located within Canada, and consent to such data also being accessed and stored outside of Canada by iClicker and its authorized service providers for support services, software upgrades,

Figure 2: Instructor Account Creation Screen

Phase 2 – Utilisation in classroom

Instructors will create a PowerPoint slide with questions and then they will launch the iClicker app. The iClicker app is downloaded as a software by the instructor on to their computer or onto the podium computer. Once the instructor launches the app a floating toolbar appears where they can open or close a polling tool for students.

iClicker can be used as short formative assessment during the lecture. Questions are multiple choice type questions that gauge the student's understanding of the lecture to date and test their knowledge of the lecture. It can also be used to break up longer lectures to keep students informed or engaged with the course material/content.

Instructors can also sync student information with iClicker when populating their classes. This is performed through Roster and Grade Sync integration, this integration has been turned on by SFU. An instructor is prompted to log into their campus LMS portal and connect their iClicker course to one of their campus LMS courses. They can then sync the roster from the campus LMS to iClicker. This is entirely handled on the backend through the product integration and the instructor does not manually upload or download any of this.

Phase 3 – Retention of data

MacMillan's iClicker program does not "purge" data once a year it retains all user personal information for as long as the information is needed for the purposes set forth in our Privacy Notice (<https://store.macmillanlearning.com/us/privacy-notice>), including to fulfill the contract and for any additional period that may be required or permitted by law. With the exception of de-identified and/or anonymized data and after receipt of written request from the Institution, we shall ensure that all PII in Protected Data stored on Macmillan Learning systems is securely destroyed pursuant to the National Institute of Standards and Technology (NIST) SP 800-88 Guidelines for Media Sanitization.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

The entire usage and process of the iClicker program is covered by this PIA

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

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative.

Consider segmenting your response into the different categories of people who you will collect different types of information from (e.g. students, administrators, employees, alumni, etc.).

Please include where the information is coming from (directly from users, pulled from pre-existing SFU databases, etc.).

Students (Information is collect directly from the student/user

- Contact Information:
 - First Name,
 - Last Name
 - SFU email address,
 - Student Number
 - Location
 - IP Address

- Student Payment Screen
 - First Name
 - Last Name
 - Email
 - Billing Address – handled by third party vendors
 - Payment information – handled by third party vendors

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference. For example:

- names, home addresses, emails, and telephone numbers of the individual or of their guardians or family members;
- images of the individual;
- anyone else's opinions about an individual;
- an individual's personal views or opinions;
- identifying number (e.g., student number, employee number, health care number);
- age, sex, gender, marital status, race, national or ethnic origin;
- religious or political beliefs or associations;
- educational, medical, criminal, financial, employment history.

Type “yes” or “no” to indicate your response.

Yes

- **If yes**, are all of the personal information elements you are collecting necessary for your initiative?
 - Yes
- **If no**, how will SFU reduce the risk of unintentionally collecting personal information? After you Answer this question, submit this PIA to the Access and Privacy Program. **You do not need to complete the rest of the PIA template.**
 - [Answer]

Section 2: COLLECTION, USE AND DISCLOSURE

4. Collection, use and disclosure flow

Describe the information flow of your initiative in the below chart.

- **Collection:** Describe the steps in collecting personal information from individuals by SFU and/or the vendor (be sure to clarify which party is collecting the information).
- **Use:** How does SFU and/or the vendor use personal information (be sure to clarify which party is using the information)?
- **Disclosure:** When, if ever, would SFU and/or the vendor provide the personal information to an internal or external third party that does not normally have access to the personal information?

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority See the most common FIPPA authorities listed below this chart.	Other legal authority
Step 1: Student is advised they are required to purchase and use either a hardware or mobile version of the service by the instructor/course outline	N/A	N/A	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority <i>See the most common FIPPA authorities listed below this chart.</i>	Other legal authority
Step 2: Student must sign up for the service and is required to enter their name and email address or alias is desired. Instructor signs up for program. Vendor Collection	Collection	26(c)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority <i>See the most common FIPPA authorities listed below this chart.</i>	Other legal authority
Step 3: If the student elects for mobile service then they will need to purchase a subscription which includes payment information such as credit card information, address) Third Party Collection (payment services)	Collection	26(c)	
Step 4: Vendor may collect and use technical data such as IP Address, Device identifiers, web logs, website cookies	Collection Use	26(c) 32(a)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority <i>See the most common FIPPA authorities listed below this chart.</i>	Other legal authority
Step 5: Student uses the tool during class to answer questions as directed by the instructor and is collected into the system and can be shared with the class or instructional team	Use Disclosure The instructor takes the information and is either used for formative or summative assessment for the particular class. Responses may be viewed by the instructional team (Teacher and TA). Additionally, responses can be displayed to the class anonymously	32(a) 33(2)(d)	
Step 6: Retention of data by application	Vendor retains all user personal information for as long as the information is needed for the purposes set forth in our Privacy Notice (https://store.macmillanlearning.com/us/privacy-notice),	31	

Most Common FIPPA Authority References

For more options, see the full text of FIPPA ([link](#)).

Type	Description	Section
Collection	The collection of the information is expressly authorized under an Act	26(a) <i>*and list the enactment and section above</i>

Type	Description	Section
	The collected information relates directly to and is necessary for a program or activity of the University.	26(c)
	The collected information is necessary for the purposes of planning or evaluating a program or activity of the University.	26(e)
Use	Use of the information is for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.	32(a)
	The individual the information is about has consented to the use (<i>If using this authority, provide a copy of the consent language after your collection notice, below</i>)	32(b)
	Use of the information is for a purpose for which the information may be disclosed to the public body under FIPPA s. 33	32(c) <i>*also list which authority under s.33</i>
Disclosure	The individual the information is about has consented to the disclosure (<i>If using this authority, provide a copy of the consent language after your collection notice, below</i>).	33(2)(c)
	Disclosure of the information is for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose. (<i>If you select this authority, ensure the disclosure is described in the collection notice, below</i>).	33(2)(d)
	Disclosure of the information is in accordance with an enactment of British Columbia or of Canada that authorizes or requires the disclosure: <i>[insert detail]</i>	33(2)(e) <i>*and list the enactment and section</i>

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

5. Collection Notice and Consent

5.1 Collection Notice: *If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice (except in limited circumstances). If your vendor is collecting personal information on behalf of SFU, the vendor must also provide a collection notice.*

Review the template collection notice and update as applicable. Consider whether you will need more than one collection notice.

The below collection notice will be posted either in the course outline, on the course canvas, on a powerpoint during lecture.

iClicker collects personal information on behalf of SFU under the authority of the University Act (R.S.B.C. 1996, c. 468), and Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165).

The information is related directly to and needed by the

University to facilitate engagement and interaction between the instructor and students.

The information will be used by iClicker to facilitate engagement and interaction between the instructor and students in a face-to-face or virtual instructional space, score student responses, and record student attendance.

If you have any questions about the collection and use of this information please contact the Centre for Educational Excellence, 8888 University Drive, Burnaby, BC V5A 1S6, 778.782.7115.

The following Collection Notice is displayed on Instructor account creation:

iClicker and my educational institution will collect and use my personal information (including name, email address, student ID as applicable, iClicker course and session information, responses and answers, attendance, and scoring), for the purposes of providing the iClicker online student response system, including questions, scoring responses, recording attendance, and facilitating classroom interaction, in accordance with the Macmillan Learning Privacy Notice. I understand that my personal information from my use of iClicker will be stored on servers located within Canada, and consent to such data also being accessed and stored outside of Canada by iClicker and its authorized service providers for support services, software upgrades, and to create de-identified data sets. I understand that providing my consent is voluntary. If I do not consent to the access and storage of my personal information outside Canada as set out above, I have the option of registering under an alias by creating an alias and creating and opening an e-mail account under that alias with a third-party email service, as specified in the Macmillan Learning Privacy Policy under the Section Pseudonymous Registration. The consents above are effective as of the date I sign up for an iClicker account and will continue until I request that I close my account after completion of the applicable course.

The following Collection Notice is displayed on Student account creation:

iClicker and my educational institution will collect and use my personal information (including name, email address, student ID as applicable, iClicker course and session information, responses and answers, attendance, and scoring), for the purposes of providing the iClicker online student response system, including questions, scoring responses, recording attendance, and facilitating classroom interaction, in accordance with the Macmillan Learning Privacy Notice. I understand that my personal information from my use of iClicker will be stored on servers located within Canada, and consent to such data also being accessed and stored outside of Canada by iClicker and its authorized service providers for support services, software upgrades, and to create de-identified data sets. I understand that providing my consent is voluntary. If I do not consent to the access and storage of my personal information outside Canada as set out above, I have the option of registering under an alias by creating an alias and creating and opening an e-mail account under that alias with a third-party email service, as specified in the

Macmillan Learning Privacy Policy under the Section Pseudonymous Registration. The consents above are effective as of the date I sign up for an iClicker account and will continue until I request that I close my account after completion of the applicable course.

5.2 Consent: *If you are obtaining consent for the use or disclosure of personal information, add any consent language here.*

Consent must have the following elements:

- a) be in writing; and*
- b) be done in a manner that specifies:*
 - a. the personal information for which the individual is providing consent;*
 - b. the date on which the consent is effective and, if applicable, the date on which the consent expires;*
 - c. for “use” consent, the use of the personal information; and*
 - d. for “disclosure” consent:*
 - i. to whom the personal information may be disclosed;*
 - ii. if practicable, the jurisdiction to which the personal information may be disclosed; and*
 - iii. the purpose of the disclosure of the personal information.*

[Answer]

Section 3: STORING PERSONAL INFORMATION

6. Is any personal information stored outside of Canada?

No

- *If yes, where (e.g. which states or countries)?*
 -

7. Has the vendor agreed to notify SFU if it changes the country in which personal information is stored?

If the vendor has agreed to SFU’s Privacy Protection Schedule, then the answer is ‘yes’. If ‘no’, add this as a risk in section 6 “Additional Risks”.

Yes

8. Does your initiative involve sensitive personal information that will be stored outside of Canada?

“Sensitive” is not defined. What information is sensitive may depend on the context. Examples can include medical information, unique government issued identifiers (passport number, driver’s license, PHN, SIN), financial information, disciplinary or complaint history, ethnic and racial origins, an individual’s sexual orientation, religious or philosophical beliefs, etc. You may need help from the Access and Privacy Program to determine whether the personal information is “sensitive”.

No

- If yes, go to question 9.
- If no, then skip ahead to Section 5.

~~**9. Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public?**~~

~~Type “yes” or “no” to indicate your response. “No” is the most likely response.~~

~~NO (?)~~

- ~~• If yes, what enactment? Then skip Section 4 and go to Section 5.~~
- ~~• [Answer]~~
- ~~• If no, go to Section 4.~~

Section 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

WAIT! Complete Section 4 only if sensitive personal information will be stored outside of Canada. See question 8, above, for an explanation of what may be “sensitive”.

10. Storage details

Fill in the table below (add more rows if necessary)

Name of service provider (including subcontractors)	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

11. Does the contract you rely on include privacy-related terms?

[Answer]

- If yes, describe the contractual measures related to your initiative, or copy the terms in here.

☐ [Answer]
- Has SFU's Cloud Privacy Protection Schedule been appended to the contract?

☐ [Answer]

12. What controls are in place to prevent unauthorized access to sensitive personal information?

[Answer]

13. Provide details about how the vendor will track access to sensitive personal information (e.g. logging access to data).

[Answer]

14. ~~Describe the privacy risks for disclosure outside of Canada.~~

~~Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.~~

~~This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.~~

Privacy risk	Impact to individuals (low, medium, high)	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Examples of privacy risks	Examples of risk responses
Vendor has access to the sensitive personal information on an ongoing basis. This is known as standing access. Standing access increases the risk of an unauthorized disclosure of personal information.	Time limited access where access ends automatically after a set period of time.
Vendor is subject to laws that may compel them to disclose the public body's personal information to another entity without notifying the public body. In this case, the public body may not have an opportunity to contest the disclosure, which may be unauthorized under FIPPA. Assessing this risk should take into consideration the sensitivity of the information and likelihood of occurrence.	Contractual language
The vendor uses third party subcontractors that they do not agree to be accountable for related to privacy practices.	Contractual language
The jurisdiction in which sensitive personal information is stored does not respect the rule of law or has no privacy laws.	Contractual language (note there will likely be outstanding risks)

Examples of privacy risks	Examples of risk responses
Retention of personal information longer than is necessary, which increases the risk of unauthorized use, access, and disclosure.	Retention schedules, contractual language
Vendor refuses to agree to SFU's Privacy Protection Schedule.	Other contractual privacy language (does the vendor agree it is a service provider subject to FIPPA?)

15. Outcome of Section 4

The outcome of Section 4 will be a risk based decision made by the role designated accountable (see Part 3) on whether to proceed with the initiative, with consideration of the risks and risk responses, including consideration of the outstanding risks in question.

Is the outcome to proceed with the initiative?

[Answer]

Section 5: ACCURACY, CORRECTION AND RETENTION

16. How will SFU make sure that the personal information is accurate and complete?

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete. For example, information collected is provided directly by the individual for a known purpose, information used is not outdated, etc.

Students provide their own details to iClicker when they setup their accounts as per their own agreement with iClicker.

17. Requests for correction

FIPPA gives an individual the right to request correction of errors or omissions to their personal information. SFU's formal process to respond to these requests is here: [Requesting a Correction to Personal Information in University Records](#).

17.1 What process is in place to correct personal information?

SFU has a process in place to correct or annotate an individual's personal information upon request: <https://www.sfu.ca/archives/fippa/changes-corrections.html>

17.2 Sometimes it's not possible to correct the personal information. FIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response.

Yes

17.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year to one or more third parties, FIPPA requires you to notify the parties you disclosed to of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response.

Yes

18. Does your initiative use personal information to make decisions that directly affect an individual?

Yes

- If yes, go to question 19
- If no, skip ahead to Section 6

19. Do you have a records retention schedule in place related to personal information used to make a decision?

FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

Yes - Student grades - RRSDA1995-018

- ~~• If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.~~

○ **[Answer]**

Section 6: ADDITIONAL RISKS

20. Has the vendor expressed, either through contract, communications with you, or their privacy policy, their agreement to notify SFU of a privacy breach?

Under s.30.5 of FIPPA, an SFU employee or service provider to SFU “who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the [University Archivist and Coordinator of Information and Privacy]”.

Privacy breaches can be reported to SFU here:

<https://www.sfu.ca/archives/fippa/breaches-complaints/report-respond-to-a-breach.html>

Yes

21. Risk Response (non-security risks)

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

If you filled in the risk table at Q.14 for sensitive information stored outside of Canada, only include additional risks here.

Add new rows if necessary.

Possible (non-security) risk	Proportionate response / mitigation strategies	Mitigation strategy to be implemented (Y / N / Already done)	Deadline date for implementation

Examples of (non-security) privacy risks	Examples of risk responses / strategies
Vendor is subject to laws that may compel them to disclose the public body's personal information to another entity without notifying the public body (e.g. The USA's <i>Patriot Act</i>). In this case, the public body may not have an opportunity to contest the disclosure, which may be unauthorized under FIPPA.	Contractual language

Examples of (non-security) privacy risks	Examples of risk responses / strategies
The vendor uses third party subcontractors that they do not agree to be accountable for related to privacy practices.	Contractual language
The jurisdiction in which sensitive personal information is stored does not respect the rule of law or has no privacy laws.	Contractual language (note there will likely be outstanding risks)
Retention of personal information longer than is necessary, which increases the risk of unauthorized use, access, and disclosure.	Retention schedules, contractual language
Vendor refuses to agree to SFU's Privacy Protection Schedule.	Other contractual privacy language (does the vendor agree it is a service provider subject to FIPPA?)
Unauthorized use or disclosure by internal SFU staff members with authorized access.	SFU staff sign privacy and confidentiality agreements and are bound by FIPPA and SFU policy I10.11 SFU staff will be trained on privacy protection risks and solutions
Collection notices do not accurately reflect how personal information will be used. Care must be taken that personal information is used for the purpose for which it was obtained or compiled, or for a use consistent with that purpose.	Ensure any future new uses of personal information are first vetted against existing collection notices and amend as necessary.
Inaccurate (i.e., outdated) information is used to make a decision that directly and adversely affects an individual	RRSDAs; Develop mechanisms for ensuring personal information remains up to date and in-sync with related systems.

Section 7: PRIVACY SIGNATURE

This PIA was conducted by the Delegated Authority below, in accordance with the Minister of Citizens' Services Direction 2-21 and SFU Policy I 10.02 'Head of the Institution and Delegation of Authority under FIPPA'.

Under SFU's [Protection of Privacy Policy I 10.11](#), the Access and Privacy Program is responsible for advising on, reviewing, and recommending for approval Privacy Impact Assessments (s.6.1.2).

Role	Name & title	Signature	Date signed
Privacy program representative (Delegated Authority)	Ernest Soares Privacy Legal Counsel		

22. Is the Delegated Authority’s signature contingent upon review and signature by Information Security per Part 2?

If yes, provide PIA to Information Security to complete Part 2, below.

[Answer]

PART 2: SECURITY REVIEW

In this Part, you will share information about the privacy aspect of securing personal information with an SFU Information Security reviewer. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

Section 1: PHYISCAL AND TECHNICAL SECURITY

1. SFU’s Security Arrangements

Will the initiative involve a new system at SFU for storage or access to records, with unique physical or technical security measures to what already exists for SFU records?

Type “yes” or “no” to indicate your response.

[Answer]

- *If yes, describe where the records for your initiative are stored (e.g., on the University's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc. See Schedule A, below, for a list of security measures.*

○ [Answer]

2. Vendor’s Security Arrangements

If this initiative involves a vendor, what are their physical and technical security arrangements for protecting the personal information in their custody against such risks as unauthorized collection, use, disclosure, or storage?

[Answer]

Section 2: ACCESS CONTROL

3. Controlling and tracking access

Please check each strategy that describes how you or your vendor limits or restricts who can access personal information and how you keep track of who has accessed personal information in the past. Insert additional strategies if needed.

Strategy	Yes/No
We only allow employees in certain roles access to information	[Y/N]

Strategy		Yes/No
Employees that need standing or recurring access to personal information must be approved by executive lead		[Y/N]
We use audit logs to see who accesses a file and when		[Y/N]
Describe any additional controls:	[Answer]	

Section 3: RISK RESPONSE

4. Risk Response (Security Risks)

Describe any security risks that arise in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible security risks	Proportionate response / mitigation strategies
Risk 1: [Answer]	[Answer]
Risk 2:	
Risk 3:	
Risk 4:	

Examples of security risks	Examples of risk responses / strategies
Standing access: Vendor has access to the personal information on an ongoing basis, which increases the risk of an unauthorized disclosure of personal information.	Time limited access where access ends automatically after a set period of time.
System and data security breached by a hacker.	Security measures and policies
Individual's personal data is compromised while in transmission.	Security measures
Unauthorized access by SFU employees to the data.	Ensure access and permissions are set up to best practice recommendations. Implement standard off-boarding when employees' roles change or leave SFU.

Section 4: IT COMMENTS AND SIGNATURE

This section is to be filled in by the ITS reviewer.

- 5. Does this initiative have reasonable security arrangements?
 - [Yes / No]
- 6. Comments / Recommendations:
 -

Role	Name & title	Signature	Date signed
Information Security representative	Steve MacGregor, CIPT, PCI ISA Information Compliance Architect		

PART 3: ACCOUNTABILITY REVIEW

The Minister of Citizens' Services Direction 2-21, "[Privacy Impact Assessment Directions](#)" requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s.D8).

Accountability is maintained by the role or position, regardless of who fills the role.

The role ultimately responsible for deciding whether or not to implement the initiative referred to in this PIA is the role most likely to be appropriate for holding accountability.

Under SFU's [Protection of Privacy Policy I 10.11](#), administrators are responsible for:

- ensuring that the activities of their departments are in compliance with the privacy principles articulated in the Policy;*
- preparing Privacy Impact Assessments; and*
- abiding by the requirements of a completed Privacy Impact Assessment, including taking steps to correct or mitigate any privacy issues or foregoing the implementation of an initiative if the implementation is in violation of FIPPA or SFU policies.*

Holding accountability for the privacy risks of this initiative includes:

- reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;*
- making a risk-based decision on whether to proceed with the initiative, with consideration of the risks and risk responses, including consideration of the outstanding risks in question;*
- ensuring accountability is transferred to any individual who assumes this role;*
- if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the Access and Privacy Program is engaged, and if necessary, completing a PIA update; and*
- understanding what your privacy obligations are, and if not, following up with the Privacy and Access Program.*

Accountability includes affirming that this PIA accurately documents the data elements and information flow at the time of signing.

Role	Name & title	Signature	Date signed
Initiative lead			
Role designated accountable for the initiative			

Schedule A

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