

Privacy Impact Assessment

PIA # and Name- 24-04 Symplicity

Legislative Requirement

Under Section 69 (5.3) of FIPPA UNBC is required to conduct a privacy impact assessment (PIA) and must do so in accordance with the directions of the Minister responsible for the Act.

A PIA needs to be conducted

- For a new initiative for which no PIA has previously been conducted.
- Before implementing significant change to an existing initiative, including but not limited to a change in the location in which sensitive personal information is stored.
- At the discretion of the person(s) with delegated authority under section 66 of the Act

1. Accountability

1.1 Identify Department, Branch, or Program Area involved in the initiative

Career Centre

1.2 Identify UNBC role responsible for the Initiative

Work Integrated Learning Projects Coordinator

1.3 Describe the Governance Model – who is accountable for the program or system.

Manager, Student Experience & Planning

1.4 Timeline for the initiative

Anticipated start date for the initiative,

6/3/24

Is this a one-time event?

Yes

No

2. Overview

2.1 Describe the New Program or Service or the Change.

Symplicity - Career Services Manager (CSM) is a SaaS database platform for consolidating, organizing and disseminating data on identified data points.

2.2 Describe the Purposes, Goals and Objectives.

The purpose of a CSM is to revolutionize and revitalize the UNBC Career Centre's processes and addresses longstanding challenges. By utilizing this software it will attack a critical deficiency with manual processes that are both labor-intensive and inefficient. The absence of dedicated software for tracking students through Co-op placements, experiential experience, and employer interactions hinders the ability to effectively support student career aspirations and cultivate meaningful employee relationships, resulting in a reputational lag, impacting UNBC's standing in its ability to offer career readiness supports and co-op opportunities. The 4 main goals of this platform and processes are to:

- 1) modernize career services
- 2) enhance co-op program growth
- 3) improve employer relations
- 4) boost reputation

2.3 List any Relevant PIAs

2.4 List any relevant contracts or software purchases.

Be sure to follow [UNBC guidelines](#) regarding purchasing policies.

2.5 List all interested parties impacted / Involved

(i.e. who are you collecting information from, UNBC roles accessing/using information, 3rd parties with whom you will share information)

Interested Party	Role in the initiative
Students	Inputting data for application, having data tracked through Co-op workflow, data held for.
Career centre team	Manage data, system, processes, and permission levels.
Vendor	Owner of software and any updates.
Reg office	Manage data that is sent to symplicity.
Employers (external)	Post job and co-op opportunities, receive basic information from students and relationship with career centre team.
Faculty	Can interact with both job boards, view some student data, and view employers.

3. Collection of Personal Information

3.1 List the data elements or personal information involved in your initiative.

Data Element name, email, id#, grade	Rationale for collection	Method of Collection	FIPPA Authorization
student name, email, student number, program, international/domestic, status, graduate/undergraduate	identification, contact, and identification of eligibility for program.	Direct Indirect NA	26(c)
GPA /cGPA	necessary for eligibility verification	Direct Indirect NA	26(c)
student documents (resume, cover letter, offer letters for placements)	support of students & application to jobs	Direct Indirect NA	26(c)
Notes on Students & interactions with them	necessary for operation and recording	Direct Indirect NA	26(c)
		Direct Indirect NA	TBD
		Direct Indirect NA	TBD
		Direct Indirect NA	TBD

3.2 Describe how personal information is to be collected.

If you already have a collection notice, attach it as an appendix.

indirect will be through banner.

direct will be submitted by the student, employer, or collected through forms, submitted by the student or employer.

4. Use of Personal Information

4.1 List all users of PI and Describe how personal information is to be used.

User (UNBC Roles e.g Governance officer)	How the info is used	FIPPA Authorization
Career Centre Coordinators	power user - access to all information within system	32(a)
Faculty	Will use information provided to assist students and connect with employers.	32(a)
Student ambassadors	Employed students will assist students and connect with employers.	32(a)
		TBD

4.2 Describe the record management of Personal information involved in the initiative.

Does the initiative involve using personal information to make a decision about an individual?	Does the initiative have a retention schedule regarding personal information used to make decisions?
<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<p>If the initiative involves using personal information to make a decision about an individual, but does not have a record retention schedule, 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.</p>	
<p>Data tied directly to banner. but a data retention process is able to be implemented, to be determined during implementation.</p>	

5. Research/ Health System Use of Personal Information

5.1 Will data collected through this initiative be used for research or health system use?

Yes

No

If "Yes" answer the following questions, if "No" please proceed to the next section.

5.2 Explain and provide details of data state (aggregate, de-identified, anonymized etc.)

Empty text box for response to question 5.2.

5.3 If data will it be disclosed as part of Health System Use, provide details on the method of disclosure, as well as where and how personal information will be stored by 3rd party.

Empty text box for response to question 5.3.

5.4 If data will it be disclosed as part of Research/ Open Data, provide details on the method of disclosure, as well as where and how personal information will be stored by 3rd party.

Empty text box for response to question 5.4.

6. Storage of Personal Information

6.1 Does the initiative involve digital tools, databases, or information systems?

Yes

No

If yes, contact [UNBC Information Security](#) to determine whether the initiative requires a security and threat risk assessment.

6.2 As part of this initiative, will Personal information be store outside of Canada?

Yes

No

6.3 Describe how information will be stored during this initiative (i.e., cloud storage, SaaS, etc).

Symplicity provides SaaS applications hosted by major cloud service providers. Symplicity utilizes Amazon Web Services, Microsoft Azure, and Oracle Clouds for our hosting and storage needs.



7. Disclosure of Personal Information

7.1 Does the initiative involve disclosing information to 3rd parties (i.e. non-unbc employees?)

Yes

No

If "Yes" answer the following questions, if "No" please proceed to the next section.

7.2 Provide details on the disclosure, including to whom, purpose, method of disclosure, and how personal information will be stored by 3rd party.

CEWIL and ACEWIL- Aggregate data for reporting purposes
Employers - access to our network, information pertaining to posting jobs, and release of resumes and cover letters through our system, as part of students applying for positions.

7.3 If disclosing information to anyone outside of Canada, Provide details regarding to whom purpose, method of disclosure, and how personal information will be stored by 3rd party.

n/a unless co-op employer outside of Canada, then same process as 7.2

8. Accuracy and Correction of Personal Information

8.1 How will you make sure that the personal information collected is accurate and complete?

base data collected directly from Banner. Student data will be submitted by students, and may be validated against information pulled from banner.

8.2 Do you have a process in place to correct personal information?

Yes

No

8.3 If yes, please describe your process below?

super users (career centre staff) will be able to go in and directly update data.

8.4 Describe the process of how you will make a note on the record, if you're not able to correct the record itself.

to be determined. - super users able to manage nearly all data. Exception may be data pulled from banner which may be immutable.

8.5 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, how will you ensure that you conduct these notifications when necessary?

if the information would impact reporting, and within the reporting time frame, generate a new report and submit. Otherwise, the unit will coordinate with Privacy to determine next steps.

9. Personal Information Bank

A personal information bank is a collection of personal information that is organized or searchable by the name of the individual or an identifying number, symbol, or other identifier. A personal information bank can be a simple list of personal information.

Personal information banks contain personal information that is:

- linked to an identifiable individual
- organized and capable of being retrieved by a personal identifier
- normally compiled for a single purpose

9.1 Will your initiative result in a personal information bank?

Yes

No

If "Yes", answer the following questions, if "No" please proceed to the next section.

9.2 Describe the business purpose for the information bank (i.e., account management of clients/ students).

account management of students, aggregate data of reporting and accreditation purposes.

9.3 If aggregate reports are generated from the information bank, explain how Personal Information will be de-identified or anonymized.

identifying reports will remove personal information

9.4 Describe the category of users and the information to which the user will have access

Category of Users (i.e., system admin, clerk, etc.)

Information accessed (i.e. contact info, grades, fee etc.)

System admin	all
faculty	basic student information, some uploaded documents, job board, employer information. Will only have access to information about students in their program or students that they teach.
student ambassador	basic student information, some uploaded documents, job board. Will only have access to students that they have been assigned to work with.

9.5 Identify the UNBC role(s) responsible for managing user accounts and audit user access.

Co-op Coordinator, Work Integrated Learning Projects coordinator, Career Readiness Coordinator

9.6 Describe the process for auditing user access.

How detailed is the data (e.g., date stamps, time stamps, IP address, etc.)? Does the audit log include the purpose of an access?

[Redacted content]

9.7 Is there a separation of responsibility between those who supervise administration of the system, or security of the system, and those who verify the audit logs

Yes

No

9.8 Are the audit logs immutable?

Yes

No

9.9 Is the system responsive or passive?

Is it possible to put a monitor on particular individuals? Will access produce an immediate response/notification or a log entry for review?

9.10 How will those found to abuse access privileges be sanctioned ?

administrative action to be taken.

10. Common or Integrated Program or Activity

In FOIPPA, “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 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

10.1 Does this initiative involve a program or activity that provides a service(s) through at least one other public body or agency working collaboratively to provide that service?

Yes

No

10.2 Does this initiative involve a program or activity that provides a service(s) through UNBC that is working on behalf of one or more other public bodies or agencies?

Yes

No

10.3 The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the Regulations? (Privacy Officer will answer).

Yes

No

If this PIA addresses a common or integrated program, UNBC must submit this PIA to the Office of the Information and Privacy Commissioner and be subject to their examination, advice, and timelines.

11. Privacy and Security Safeguards

11.1 Describe administrative safeguards(i.e. policy documents, procedures, or training).

11.2 Describe physical safeguards(i.e. locked, filing cabinets, locked doors, or restricted areas).

11.3 Describe the controls in place to prevent unauthorized access to personal information(i.e. role-based access to software, access logs).

11.4 Describe technical safeguards(i.e. firewalls, encryption, or intrusion prevention systems).

12. Privacy Risk Identification and Mitigation

Identify any privacy risks and the corresponding mitigation strategies that will be implemented. Try to include at least one risk related to each step in the information cycle (collection, use, storage, disclosure, and retention). Refer to the [risk classification table](#) to assist with likelihood and impact rating. **If you are disclosing or storing data outside of Canada you will need to identify additional risks related to storage/disclosure outside of Canada.**

12.1 Risk Description	Likelihood	Impact	Risk level	Mitigation Strategy Describe how above safeguards could be used to mitigate the risk

13. Collection Notice

All collection notices must include the:

- Purpose for the collection
- Legal authority for the collection
- Contact information for an employee of UNBC who can answer the individual's questions about the collection.

The employee responsible for responding to data collection questions should be able to explain why the personal information is being collected and how it will be used, retained, and disclosed.

The contact method should suit the collection method. For example, if you collect personal information through an online form, you could include an email contact.

13.1 Privacy notice

Be sure to include all 3 required parts of the notice

Your personal information will be collected for accessing career centre resources. If you have any questions about the collection of this personal information, please contact hirestudents@unbc.ca. This information is being collected by the UNBC Career Centre under FOIPPA Section 26

13.2 Location of Privacy Notice

If the notice is to be posted on the website please include url of webpage.

TBD - likely on front page after logging in, or consent page for use of tool.

14. Signing and Approval

Individual leading the Program/Project: Rachelle Munchinsky

Position: Manager, Student Experience & Planning

I confirm the information management practices in this initiative have been documented as accurately as I am aware. I commit to communicating appropriate information management practices to all individuals participating in this initiative. I commit to following the documented practices on this PIA, or arranging a PIA amendment if I am aware information management practices in this initiative change.

Signature: 

Date: May 3, 2024

Director/Dean Overseeing the Program/Project: Director, Student Success

I am accountable for overseeing my staff involved in this initiative to ensure they adhere to information management practices presented in this PIA. I will arrange for the project lead named above to contact the Privacy Officer to arrange a PIA amendment if required.

Signature: 

Date: 04/06/2024

Vice-President authorizing the Program/Project: VP Academic & Provost

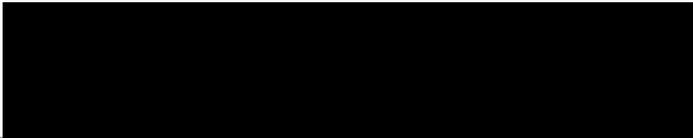
I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that complies with policies and procedures of the University of Northern British Columbia.

Signature: 

Date: May 8, 2024

Privacy Officer reviewing the Program/Project: Christopher Ross

I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that comply with British Columbia's Freedom of Information and Protection of Privacy Act.

Signature: 

Date: May 8, 2024

15. Reference Tools

“personal information” means recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, telephone number, fingerprints or blood type of the individual,
- (e) the personal opinions or views of the individual except where they relate to another individual,
- (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- (h) the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Privacy Impact Risk assessment:

		Impact Severity of outcome of identified risk occurs				
		Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
Probability Likelihood that identified risk will occur	almost certain 5	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
	Likely 4	Medium 4	Medium 8	High 12	Very High 16	Extreme 20
	Moderate 3	Low 3	Medium 6	Medium 9	High 12	Very High 15
	Unlikely 2	Very low 2	Low 4	Medium 6	Medium 8	High 10
	Rare 1	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Risk Rating	*Risk Levels	Description	Actions Required
1-4	Minimal	Unlikely that associated risk would result in harm to privacy	Review of safeguards to be done at PIA review date
5-9	Moderate	Unlikely that associated risk would result in significant harm to privacy	annually review existing safeguards required
10-16	Elevated	Likely that associated risk would result in harm to the privacy	Routine monitoring of data processing or additional safeguards required
17-25	Unacceptable	Associated Risk would likely cause significant and immediate harm to the privacy	Must not proceed as existing safeguards and controls are insufficient

[Return to Risk Matrix](#)