UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment Form

PIA # and Name- 2305

1 General Information

1. Name of Department, Branch and Program Area

Office of the President

2. Name of Program or Service Representative

Renewal of Strategic Plan 2024 - 2029
Arleta Lucarelli, Executive Director, Strategy and Staff

3. When will the initiative take place? 4/3/23

4. Is this a one-time event?

✔ Yes ☐ No

5. Do you have an end date planned?

✔ Yes ☐ No

6. Describe the New Program or Service or the Change.

Strategic Planning process is underway. Our third party, Prime Strategy, will be using a product called Padlet to vet the draft Strategic Framwork. The vetting will be available to students, faculty, staff and community which includes alumni and public.

7. Describe the Purposes, Goals and Objectives.

A Privacy Imapct Assessment was already completed for the the Strategic Plan Renewal. This is an additional tool that's being added in order to check / vet if what we are hearing through consultations and survey is reflected in the draft framework. We want to share this draft framework first week of April and allow for comments.

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

Office of the President
President - Dr. Geoff Payne
Executive Director, Strategy and Staff - Arleta Lucarelli

9. List any Relevant PIAs

PIA 22-50 was completed when the Strategic Plan Renewal was launched in November 2022.

10. List of All Stakeholders Impacted / Involved (i.e. who are you collecting information from, UNBC roles using PI, 3rd parties with whom you will share information)

Stakeholder	Role in the initiative
Students, staff, faculty, community by invitation	opportunity to provide comments to vet the draft framework

11. List any relevant contracts or software purchases. Be sure to follow UNBC guidelines regarding purchasing policies.

Prime Strategy

2 Collection and Use of Personal Information

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

Data Element name, email, id#, grade	Rationale for collection, use or disclosure	Method of Collection or Disclosure	FIPPA Section (completed by Privacy)
opinions	quality improvement - purpose is to collect comments back on the draft framework	**Direct** Indirect	26(e)
		Direct **Indirect**	TBD
		Direct **Indirect**	TBD
		Direct **Indirect**	TBD
		Direct **Indirect**	TBD
		Direct **Indirect**	TBD
		Direct **Indirect**	TBD

13. Describe how personal information is to be collected

Padlet is a software that allows for participants who receive the link to post comments. Prime Strategy will display the the draft strategic framework and will invite participants to comment on the draft. All comments will be posted anonymously. Names will not be linked to comments. Participants will have 1 week to provide comments. After close, access to the page will be closed and the page will be deleted.

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

15. Please 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
Prime Strategy (Consultant)	To improve the draft framework

16. Do you use personal information in your initiative to make a decision about an individual?

☐ Yes ☑ No

17. If yes, do you have a retention schedule in place related to personal information used to make decisions?

☐ Yes ☑ No

18. If yes, please your approved information schedule as an appendix.

19. If you answered 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.

The comments will be collected for up to 1 year and then destroyed as part of the previous PIA on this process (to be consitent).

3 Storage of Personal Information

20. Is any personal information stored outside of Canada?

☑ Yes ☐ No

21. Describe how PI information will be stored

For example, are you using a cloud storage (OneDrive), or Software as a Service (SaaS).

Padlet information is stored on US servers. Participants will have 1 week to provide comments. After close, access to the page will be closed and the page will be deleted. All data will be store with Prime Strategy. With the Prime Strategy contract it was agreed that any data collected through this process will be retained for 1 year only.

22. Does your initiative involve digital tools, databases information systems?

☑ Yes ☐ No

If yes, please discuss with UNBC Information Security whether you also require a security and threat risk assessment

4 Research / Health System Use

23. Do you anticipate that data collected by this program / system will be used for research or health system use?

☐ Yes ☑ No

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

24. Please explain and provide details of data state (aggregate, de-identified, anonymized etc.)

25. Will it be disclosed as part of Health System Use?

Provide details on the disclosure, including where and how personal information will be stored.

26. Will it be disclosed as part of Research / Open Data?

Provide details on the disclosure, including where and how personal information will be stored.

5 Disclosure

27. Will you be 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.

28. To whom will you be disclosing personal information?Provide details on the disclosure, including where and how personal information will be stored.

Prime Strategy and Strategic Project Team will be use the information. As noted above the comments provided will be seen to all participants at the time of posting.

29. If personal information will be disclosed to anyone outside of Canada, provide details on the disclosure,including where and how personal information will be stored.

No

6 Accuracy and Correction

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

No decisions are made about individuals, No process necessary for accuracy.

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

☐ Yes ☑ No

32. If yes, please describe your process below?

NA

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

NA

34. If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third-party recipient of the request for correction. How will you ensure that you conduct these notifications when necessary?

NA

7 Personal Information Banks

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

35. 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.

36. Describe the business purpose for the information bank (i.e., account management of clients, student record management)

37. If aggregate reports are generated, explain how Personal Information will be de identified or anonymized and by whom?

38. Describe the category of users and the information to which they will have access

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

39. Who is responsible for oversight of user access?

40. Who reads the audit logs, and how long are they kept?

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

42. Are the audit logs immutable?

☐ Yes ☐ No

43. 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 (e.g., does the auditor in the organization have a role, or is it the security department?)

☐ Yes ☐ No

44. Is the system responsive or passive? For instance, is it possible to put a monitor on particular individuals (e.g., in a hospital setting, if a celebrity is admitted as a patient, etc.)? Will access produce an immediate response and not just a log entry for review months later?

45. How will those found to abuse access privileges be sanctioned ?

8 Privacy and Security Safeguards

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

[redacted]

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

NA

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

NA

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

NA

9 Privacy Risk Identification and Mitigation

50. Identify any privacy risks, even very unlikely ones, associated with the initiative and the mitigation strategies that will be implemented (see risk classification table).

Try to include at least one risk related to each step is the information cycle (collection, storage,access, disclosure, and destruction. **If you are disclosing or storing data outside of Canada you will need to identify additional risks related to storage/disclosure outside of Canada**

RISK	LIKELIHOOD	IMPACT	MITIGATION STRATEGY
[redacted]			
	Low Moderate High	Low Moderate High	
	Low Moderate High	Low Moderate High	

RISK	LIKELIHOOD	IMPACT	MITIGATION STRATEGY
	Low Moderate High	Low Moderate High	
	Low Moderate High	Low Moderate High	
	Low Moderate High	Low Moderate High	
	Low Moderate High	Low Moderate High	

10 Data Linking

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.

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

☐ Yes ☑ No

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

☐ Yes ☑ No

53. 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 Conclusions and Approvals

Individual leading the Program/Project:

Position:

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:_____

Director/Dean Overseeing the Program/Project:

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:_____

Name of Chief Information Security Officer

I confirm that this initiative to the best of my knowledge as written in the above sections, satisfactorily complies with the information security standards of the University of Northern British Columbia.

Signature:_____ Date:_____

Name of Privacy Officer: Christopher Ross

Position: Governance Officer Access Privacy and Records Management

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:[redacted] Date:_____

12 Privacy Notice

The text below should be used in the correspondence inviting individuals to review the strategic plan.

The University of Northern British Columbia is embarking on a renewal of its Strategic Plan that will inform and guide the direction of the University for the next 5 years (2023-2028). To do this we have partner with Prime Strategy consulting company. Your feedback is important to us, use the link below to review and comment on the Draft Strategic Plan. Your personal information is collected under the authority of section 26 (e) of the Freedom of Information and Protection of Privacy Act (FIPPA). This information will be used for the purpose of informing the development of a strategic plan for UNBC. By submitting your feedback, you are consenting to the storage of this information on a secure server located in the United States. Questions about the collection of this information may be directed to Arleta.Lucarelli@unbc.ca.

13 Key Terms

"**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.

Risk Classification Table

*Risk Levels	Likelihood	Harm
Low	Little possibility that the risk will occur due to mitigating factors	Compromise would likely not result in any significant harm to the privacy, safety, or economic standing of individuals or the corporation.
Moderate	A possibility that the risk will occur if no additional measures are taken.	Compromise would likely cause some harm to the privacy, safety, or economic standing of individuals or the corporation.
High	Near certainty that the risk will occur in the future if no corrective measures are taken.	Compromise would likely cause significant and immediate harm to the privacy, safety, or economic standing of individuals or the corporation.