UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

Here are a few examples of situations where you should consider a PIA:
•You collect, use or disclose new personal information that you did not collect, use or disclose before.
• You give access to personal information to new parties.
• You implement a new service delivery or management technology that stores, transmits, or retrieves personal information.
You implement a new or different electronic record system, or make changes to an existing one, such as adding portable devices with wireless network connections.
• You enter into an agreement with a new business partner or vendor who will have access to health information in your custody or control.
• You create a new organization that will collect, use or disclose personal information.

How big do changes have to be to trigger a PIA?
The most important question to ask yourself is, "Does this project pose any new risks to the privacy of personal information?"
Data matching is the creation of new information by combining two or more sets of data. The custodian who carries out the data matching is responsible for doing a PIA.

Please fill out PART A to determine your need for a full PIA.

PART A

.

Document Version, Review and Approval History

Version	Author	Nature of Change	Date
1.0			

1. Introduction

Answer the who, what, where, when, why and how of your initiative. Describe the initiative in full, including:

How will you carry out the initiative?

1. General Description

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

UNBC Continuing Studies is forming a Partnership with the Event Leadership Institute, to enroll UNBC CS students into their online courses. The Event Leadership Institute (ELI) provides progressive online education, training and professional development programs for event and meeting industry professionals. These courses are opt-in for students, and they would be paying per course.

a) Name of Program or Service

2. Description

a) Description of the New Program or Service or the Change

i. Purposes, Goals and Objectives

ii. List of All Stakeholders Impacted / Involved

Stakeholder	Role

iii. The Need

iv. Governance Model

Name of Department: **Continuing Studies**
PIA Drafter: **Nicole Neufeld**
Email: **Nicole.Neufeld@unbc.ca** Phone: **250-960-5912**
Oversight Provided by: **Nicole Neufeld**
Email: **Nicole.Neufeld@unbc.ca** Phone: **250-960-5912**

v. Relevant Existing Policies

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

vi. Related PIAs

vii. Relevant contracts

Commented [DM-G1]: May I see the contract please?

viii. Research / Health System Use

N/A

b) The Intended Scope (Project and PIA)14

Describe how much of the initiative you will assess in this PIA.

i. Scope of PIA

ii. Out of Scope of PIA

c) Definitions

From ELI Privacy Policy

Term/Acronym	Definition
Custody	The keeping, care, watch, preservation or security of the record for a legitimate business purpose
Control	The power or authority to make a decision about the creation, use, disposal or disclosure of the record
Personal Data	Personal Data means data about a living individual who can be identified from those data
Personal Information Banks	A PIB is any collection or set of personal information where personal information is organized by: • The individual's name; • An identifying number or symbol; or • Other particular identifier assigned to the individual.
Usage Data	Usage Data is data collected automatically either generated by the use of the Service or from the Service infrastructure may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data. If you are a customer (also referred to as subscriber, member, student, and/or learner) and

	you are logged in, this also includes records of your activities such as course progress and completion, video views, assessment (such as assignments, exams, quizzes) completion and scores.
Cookies	Cookies are small pieces of data stored on your device (computer or mobile device).
Data Controller	Data Controller means the natural or legal person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal information are, or are to be, processed ELI is the Data Controller
Data Processor	Data Processor (or Service Provider) means any natural or legal person who processes the data on behalf of the Data Controller.
Data Subject	Data Subject is any living individual who is using ELI and is the subject of Personal Data.

d) User Access

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*Students purchase the course from the UNBC Continuing Studies registration system (Bookking) using their Continuing Studies Account. Students will acknowledge the informed consent notice prior to purchase.*	*Collection*	
2.	*Student First Name, Last Name and Email will be shared with Event Leadership Institute via email, so the students can be registered into the Online Course with Event Leadership Institute.*	*Disclosure*	
3.	*Students will be receive an email from ELI with directions on how to create a student account with ELI.*	*Use*	
4.	*Students completion status will be shared with UNBC Continuing Studies, at which point the students status will be updated in Bookking as their record of completion.*	*Disclosure/ Stored*	

e)

How is the project, system, application or initiative accessed by users?
Are there different levels of access dependent on roles?

3. Personal Information Flow Diagram and Explanation

If you are collecting, using, storing, sharing, disclosing or retaining Personal Information you will need to proceed with the **Part B and C** of this document.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**
If not, please sign and send this determination document to the University Governance Office at privacy@unbc.ca

Think about the information you'll collect, use, store or share as part of your initiative and list it here. A major part of the PIA process is to make sure that you have authority under the *Freedom of Information and Protection of Privacy Act (FOIPPA)* to collect, use, store and disclose each of these pieces of information. Limit your collection of personal information to only what is necessary to complete the initiative.

In the table below, complete the Data Element (personal information usually) rationale and method for collection, use, or disclosure highlighting separately by row each instance that information is collected, used, stored, protected, disclosed and disposed of during this initiative.

Unless not possible, ensure these steps are arranged how they would occur chronologically in order to make a transparent workflow. The Privacy Officer will review your steps and determine which type of information management practice each entry is and ensure that the practice is compliant with sections under the Act.

c) List of Personal health information / personal information / sensitive information to be Collected, Used and/or disclosed and the Rationale for each.

Please identify each source of data that you intend to access and its business owner. Also indicate that you have contacted the owner and received permission to access the data.

EXAMPLE:

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure
Individual's Name	Required to register and correctly identify individual.	Direct
Individual's Phone Number	Required for notifying individual of test result.	Direct

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*Students purchase the course from the UNBC Continuing Studies registration system (Bookking) using their Continuing*	*Collection*	

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

	Studies Account. Students will acknowledge the informed consent notice prior to purchase.		
2.	*Student First Name, Last Name and Email will be shared with Event Leadership Institute via email, so the students can be registered into the Online Course with Event Leadership Institute.*	*Disclosure*	
3.	*Students will be receive an email from ELI with directions on how to create a student account with ELI.*	*Use*	
4.	*Students completion status will be shared with UNBC Continuing Studies, at which point the students status will be updated in Booking as their record of completion.*	*Disclosure/ Stored*	

If you do not use personal information in your initiative: how will; you reduce the risk of unintentionally collecting personal information?

For example, if you are collecting opinions as part of a public engagement strategy, participants may offer personal information about themselves or others, even though you've instructed them not to. If you do inadvertently receive or collect personal information, what steps will you take to:

- Destroy it
- Return it
- Transfer it to the correct recipient

FOIPPA section 27.1 describes under what circumstances personal information is considered not collected, despite you having received it. As long as you do nothing with the personal information you receive other than read and delete or return it, or transfer it to the appropriate public body, you have not collected the information according to FOIPPA.

UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

However, if you take any other action, including storing the information or using it in your own work, under FOIPPA you have collected personal information without authorization and that is considered a privacy breach.

I am not collecting, using, storing, sharing, disclosing, or deleting any personal information for this initiative.

Staff Name_____

Signature_____

Date_____

PRIVACY OFFICE USE ONLY

This initiative does not require a full PIA document.

_____

Governance Officer name

_____

Governance Officer Signature

_____

Date

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

PART B

4. Collection, Use and Disclosure of Personal Information

a) Legal Authority for the Collection, Use and Disclosure of Personal Information

Personal Information is being collected under the authority of the University Act and Section 26 of BC's *Freedom of Information and Protection of Privacy Act.*

a) Consent Requirements for Collection, Use and Disclosure (for each party to the system or program)

i. Collection

As you work through the description of the information flows, consider whether each element of personal information is necessary for delivering your initiative, or whether you could collect less personal information without risking the success and efficacy of your initiative. Limiting the amount of personal information you collect is one of the 10 internationally recognized privacy principles. (*See CSA Model Codes Appendix B for more details*)

Collect only the information you need for your initiative to work. Collecting more personal information than you need to do your work may lead to a privacy breach.

Section 26 states that personal information may be collected only if such collection is authorized by or under legislation, essential for operating programs or activities, or collected for law enforcement purposes.

Purpose for which personal information may be collected
26 A public body may collect personal information only if

(a) the collection of the information is expressly authorized under an Act,

(c) the information relates directly to and is necessary for a program or activity of the public body,

(d) with respect to personal information collected for a prescribed purpose,

(i)the individual the information is about has consented in the prescribed manner to that collection, and

(ii)a reasonable person would consider that collection appropriate in the circumstances,

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

(e)the information is necessary for the purposes of planning or evaluating a program or activity of a public body,

How personal information is to be collected
27 (1)A public body must collect personal information directly from the individual the information is about unless

(a)another method of collection is authorized by

(i)that individual,

(ii)the commissioner under section 42 (1) (i), or

(iii)another enactment,

Collection is only permitted through knowledgeable implied or express consent.

Consent

If your initiative is collecting personal information directly or indirectly from individuals, you must ensure that all individuals involved are told the following:

- The purpose for which the information is being collected
- The legal authority for collecting it, and
- The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

Please include your proposed wording for a collection & consent notice and where it will be located for individuals to read before collection takes place in the space below. The Privacy Officer will review and provide feedback.

You may not need a collection notice if:
- You collect personal information indirectly, meaning you get the information from another public body and not from the individual who owns the information
- You collect personal information for law enforcement
- You collect information by observing a person at a public event

FOIPPA section 27(3) and (4) tells you more about when you do not need a collection notice. If you determine that you do not need a collection notice, explain why.

Copy/Paste or Fill in your Privacy/Consent Notice here:
(See Appendix C for an example)

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

I hereby consent to the disclosure of my personal information between UNBC Continuing Studies and the Event Leadership Institution pertaining to my participation and completion of course(s) with the Event Leadership Institution. The collection, use and disclosure of my name, email address and completion information are required for the purposes of:

- *Registering Students into the Event Leadership Institutes Courses.*
- *Documentation of completion of the courses in UNBC Continuing Studies Registration System.*

The University of Northern British Columbia collects information and transmits and stores the information on Event Leadership Institutes servers under section 26 (d) of the Freedom of Information and Protection of Privacy Act for the purpose of providing the student the opportunity to learn online.

By signing below, I understand and I accept the use of Event Leadership Institute as a facilitator of this Continuing Studies course.

I understand that personal information such as my full name, email address, completion records will be stored outside of Canada in Liquid Web servers that are located in Lansing, Michigan and be accessed from the New York and/or Vancouver Offices. I understand that my consent is required under section 30.1 (a) of the Freedom of Information and Protection of Privacy Act before my information can be stored in the United States as a requirement to complete a course at the University of Northern British Columbia. I understand that I am responsible for accurately entering my personal information Event Leadership Institutes student profile. I will report any corrections that need to be made to my instructor(s) if I cannot make the corrections myself.

I understand that by refusing to sign this waiver, I will not be able to participate in this course.

If you have any questions regarding the storage, use and disclosure of your personal information, please contact the Coordinator at Lesley.haines@unbc.ca.

Please enter your details below:

Full Name: _____
(Please Print)

Mailing Address: _____

Phone Number: _____

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**
ii. Use

FOIPPA was amended effective November 26, 2021 and those amendments affect this section.

Use of Personal Information
Section 32
A public body may use personal information in its custody or under its control only

(a)for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),

(b)if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or

(c)for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

Event Leadership Institute uses the collected data for various purposes:
To provide and maintain their Service

To issue certificates and digital credentials

To submit continuing education credits or course transcripts or certification information to certifying bodies

To inform about relevant information about the course(s), content, and event(s) registered for

To allow communication with course instructors and/or facilitators

To notify about changes to their Service

To allow participation in interactive features of their Service To provide customer support

To gather analysis or valuable information to improve their Service

To monitor the usage of their Service

To detect, prevent and address technical issues

To provide news, special offers and general information about other goods, services and events unless users opted not to receive such information

iii. **Disclosure**

Disclosure of personal information

33 *A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3*

iv. **Health System Use**

v. **Research / Open Data**

b) The Sources and Accuracy of the Personal Information

It is your responsibility to make sure that the personal information you collect, store, use and disclose is accurate and complete, especially if the information will be used to make a decision that affects an individual. Ways to make sure personal information is accurate and complete include verifying the information with the person it is about prior to recording it.

- Who is providing the information – the individual or another source (e.g. another government department, a family member, provincial program database)?

- Is the information as accurate and up to date as is necessary for the purposes for which it would be used and disclosed?

FOIPPA section 29 states that a person can ask you to correct any of their personal information in your custody or control. If you cannot correct the record itself, you must make a note on the record (annotate the record). If you've disclosed the personal information to any other public body or third party in the last year, you must also notify them of any corrections you make.

- How does the information get corrected?

c) The Location of the Personal Information

FOIPPA was amended effective November 26, 2021 and those amendments affect this section.

Disclosure inside or outside Canada
33. A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:
in accordance with Part 2;
if the information or disclosure is of a type described in section 22 (4) (e), (f),

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

(h), (i) or (j);
if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

Does the information manager, vendor, and / or service provider operate from an office outside of Canada?

Does any user of the information managed in this initiative access this information from outside of Canada beyond during short-term temporary travel?

Does this initiative have any components that temporarily process information outside of Canada?

Does this initiative store information for operational use outside of Canada?

Does this initiative back up or make additional or redundant copies of information outside of Canada?

Will it be stored on portable devices?

Will the data be interfaced with data from other systems? (Data matching or linkage)

Data Linking

In FOIPPA, "data linking" and "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 and you must comply with specific requirements under the Act related to data-linking initiatives.

Is personal information from one database linked or combined with personal information from another database?)

Is the purpose for the linkage different from the original purpose for which the personal information in each database was originally obtained or compiled?

Is the data linking is occurring between either two or more public bodies or one or more public bodies and one or more agencies?

If you have answered yes to the above three questions, you will need to work with the Privacy Officer to ensure you meet the requirements for a data-linking initiative?

Common or Integrated Program or Activity

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

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.

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

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

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

Please note: If your initiative involves a "data-linking initiative" or a "common or integrated program or activity", advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC) as well. Contact the Governance Officer – Access, Privacy and Records Management to determine how to proceed with this notification and consultation in the early stages of developing the initiative, program or activity.

d) The Retention Schedule and Method of Destruction for Personal Information

Retention of personal information

31 *If an individual's personal information*

(a)is in the custody or under the control of a public body, and

(b)is used by or on behalf of the public body to make a decision that directly affects the individual,

the public body must ensure that the 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.

Think about whether you use personal information in your initiative to make a decision about an individual. Examples of using personal information to make decisions include but are not limited to:

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

- Using a person's date of birth or income to decide whether a person qualifies for a benefit
- Using a person's employment history to decide whether they can move forward in a job competition
- Using a person's health information to decide the level and type of care they receive

Keeping information for one year after it is used to make a decision that affects an individual is the minimum requirement under FOIPPA.

You may have other operational or administrative requirements that dictate how long records must be kept and when they must be disposed of. It's important to maintain the records in your initiative according to an approved records schedule.

Answer here or state N/A:

If you answered yes above, please describe retention schedules that apply where retention exceeds the one-year requirement under the Act. Please contact the Governance Officer – Privacy, Access and Records Management if you require assistance.

Answer here or state N/A:

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

Briefly describe your personal information bank and the partners and organizations involved.

Will a database or series of folders be created in this initiative that organizes information by name, identifying number, symbol, or other particular identifier of each individual involved.

If yes, will the records or information collected about the individual contain similar types of personal information. If yes, I will contact the Privacy Officer to ensure that I am identifying that this is a Personal Information Bank (PIB) and identifying the legislatively required descriptors listed in section 69 (6) of FOIPPA.

Name:

Location:

Description:

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

Authority: This personal information is begin collected under the authority of the *University Act* and section 26 (a), (c), and (e) of the *Freedom of Information and Protection of Privacy Act (FOIPPA).*

Purpose:

Category of Users:

e) Method of De-identification/Anonymization/Aggregation for Personal Information

Please explain how Personal Information will be de-identified or anonymized and by whom?

f) Users of Personal Information

Please list all users of PI including third parties

g) Audits

This question is about how you will know if the sensitive personal information is accessed, including access by service providers. The answer should include a description of what information is available through logs and how the ministry will access logs (e.g. in real-time or by request).

i. Audit Logs
ii. Record of user activity
iii. Proactive Audit

iv. Focused Audits

5. Access Rights for Individuals to their Personal Information

Access Request Management

Section 4 of FOIPOP gives individuals the right to access any record under the custody or control of a public body. UNBC is a public body under the Act.

How will you manager access to information requests?

If aggregate or de-identified data only to be released, who responsible to do so and how is that done?

Request for Personal Information from Persons to Whom It Relates

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**
How will personal requests for access be managed?

Please note*
Individuals do not have to make a formal FOI request to access their own information held by UNBC

6. Privacy and Security Safeguards

This question is about the controls you have in place to protect against unauthorized collection, use, disclosure or storage of sensitive personal information. These include preventing or managing access to sensitive personal information.

Describe technical, security, administrative and/or policy measures (e.g. the access controls that protect the sensitive personal information). If you are using a cloud-based service provider, include a description of controls at each layer in the stack (software level, platform level, infrastructure level).

A digital tool, database or information system may leave personal information exposed or otherwise vulnerable to security threats. Security assessments are used on information systems and other digital tools to assess and document security risks, risk ratings and planned risk responses. An in-depth security assessment known as a STRA (Security Threat and Risk Assessment) results in a document called the statement of acceptable risk.

a) Security Safeguards

- **Administrative Safeguards**

[redacted]

- **Technical Safeguards**

[redacted]

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

[redacted]

- **Physical Safeguards**

This question is to identify how you reduce the risk that you store personal information in a computer system or physical location where unauthorized access can happen.

Technical records are records that are stored electronically, including but not limited to records stored:

- In a database
- On a LAN (local area network)
- On a hard drive
- On a mobile device or laptop

Technical security includes any digital or electronic system set up to keep your records secure, including:

- Using UNBC firewalls
- Encrypting personal information before it is stored or transferred
- Relying on how your cloud service provider protects information in the cloud
- Using passwords to protect digital files and laptops

If your records are not stored on UNBC servers, use this question to list technical security on the system where records are stored.

Physical records include but are not limited to:

- Paper records
- Film or video
- Photographs
- Audio recordings
- Maps

Physical security is anything you do to keep physical records safe and secure, including:

- Locking filing cabinets and rooms
- Having security guards that patrol the building
- Restricting access to rooms or buildings where information is stored
- Using alarm systems in the building or room where information is stored

If your physical records are not kept in UNBC buildings with standard UNBC security, use this question to list the physical security in the building and rooms in which records are kept.

[redacted]

- **Identify any outside partners or companies involved that may have access to the personal information**
- **Website Domain Ownership (if applicable)**

7. Privacy Risk Identification and Mitigation

Please identify any privacy risks, even very unlikely ones, associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. The Privacy Officer will help identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Please explain the risks in detail using the associated CSA Model Code (Appendix B).

EXAMPLE

Risk # 1 Data that is no longer needed is at risk of being breached because it is being retained in the IT platform longer than necessary.	**Cause:** Data is not being deleted from the IT platform in a timely manner once it is no longer needed.
	Probability: Low
	Impact: High

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

Related CSA Principle: **Safeguards**	**Mitigation:** Implement a process on the IT platform that automatically deletes data once it is no longer needed, per the policy established by X

Risk # 1 **Related CSA Principle:**	**Cause:**
	Probability:
	Impact:
	Mitigation:

Risk # 2 **Related CSA Principle:**	**Cause:**
	Probability:
	Impact:
	Mitigation:

Risk # 3	**Cause:**

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

Related CSA Principle:	**Probability:**
	Impact:
	Mitigation:

PART C

8. Conclusions and Approvals

Once the PIA has been approved with or without conditions, the Privacy Officer will collect signatures from the individuals provided below. A copy of the PIA will be distributed to all signatories for convenience or to attach to a requisition or file with a contract.

Name of Individual leading the Program/Project: _____
I confirm the information management practices in this initiative have been documented on Form A, and B as applicable, as accurately as I am aware and I commit to communicating appropriate information management practices to all individuals participating in this initiative as appropriate. 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 or Dean Overseeing the Program/Project: _____

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

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:_____

_____

Contact Responsible for Records Maintenance: _____

I am responsible for ensuring that I understand how records are being maintained within paper, digital or other information systems within this PIA and that I communicate concerns regarding the feasibility, accuracy, or security of information management in this initiative.

Signature:_____Date:_____

_____

Governance Officer: _____

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

Signature:_____Date:_____

APPENDIX 1
DEFINITIONS

Confidentiality	The assurance that information about identifiable persons, the release of which would constitute a privacy breach, will not be disclosed without consent, except as allowed by law.
Consent	Consent, in the context of personal information, means the agreement of someone to provide their personal information for the purposes identified to them. In some cases, consent may not be possible (e.g., medical emergency) or may not be required (e.g., collection by police of information relating to a suspect where the collection is not a search or seizure). Consent is generally given by a specific act of the individual, but sometimes it can be implied. In the public sector, consent is not

always a requirement for the collection of personal information – having the legal authority to collect personal information is.

Core privacy principles

In March 1996, the Canadian Standards Association (CSA) developed a national, voluntary code that sets basic principles for safeguarding personal data. The Code establishes 10 basic principles for all organizations that collect or use personal information. In some cases, certain principles may not apply to public sector regimes. For example, in the public sector, the "consent" principle listed as number three below is often substituted for "legal authority".

1. *Accountability* - An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. *Identifying Purposes* - The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. *Consent* - The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

4. *Limiting Collection* - The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. *Limiting Use, Disclosure and Retention* - Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

6. *Accuracy* - Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

7. *Safeguards* - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. *Openness* - An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.

9. *Individual Access* - Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information,

	and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. 10. *Challenging Compliance* - An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.
Data (information) flows	Mapping the flow and manipulation of information within and across systems or business processes.
Data matching	An activity that involves comparing personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Included in this definition of data-matching is data linkage, also known as data profiling.
Personal information	For data to be categorized as *personal* information (rather than just information, in general), it must have details sufficient to identify an individual. Individual identification is thus the threshold for transforming general information into personal information and where rights, protections, and requirements associated with the proper handling of personal information are triggered. Without restricting the generality of the foregoing, personal information may include, for example: • information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, • information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, • any identifying number, symbol or other particular assigned to the individual, • the address, fingerprints or blood type of the individual. • the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations.

- correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence.
- the views or opinions of another individual about the individual.
- the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and,
- the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

In some jurisdictions, personal information **may not include** information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

- the fact that the individual is or was an officer or employee of the government institution,
- the title, business address and telephone number of the individual,
- the classification, salary range and responsibilities of the position held by the individual
- the name of the individual on a document prepared by the individual in the course of employment, and,
- the personal opinions or views of the individual given in the course of employment.
- information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,
- information relating to any discretionary benefit of a financial nature, including the granting of a license or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and
- information about an individual deceased for more than twenty years.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

Privacy	The interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations.
Privacy officer	A privacy officer is a person within an organization whose job it is to: • encourage compliance with sound privacy principles, prevailing privacy policies and privacy laws; • respond to requests for access to and correction of personal information and general issues within a public body concerning personal information; and • work with information and privacy commissioners during the investigation of a privacy complaint against an organization. Privacy officers may also be responsible for managing changes to an organization's: • information management practices, policies and procedures; • staff training, vis-a-vis privacy and information handling; • privacy policies and procedures; and • inquiry and complaint processes.
Privacy protection	Preventing unauthorized collection, use and disclosure of an individual's personal information.
Program manager	The person responsible for managing and directing the projects of a public body, with emphasis on coordinating and prioritizing resources, and managing the risks which emanate from projects in development or underway. Program managers are responsible for ensuring that the projects they lead or direct are compliant with government policies and the law.
Risk assessment	The process of quantifying the impact of implementing a particular idea, process, system or strategy.
Threat and Risk Assessment (TRA)	A risk management process used to evaluate the security threats associated with information technology projects, including potential system vulnerabilities and impacts on data integrity and confidentiality. TRAs, when completed in conjunction with a PIA, can help provide recommendations to lower information and privacy risks to acceptable levels.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

APPENDIX B
CSA MODEL CODES

1. Accountability

The principle of **Accountability** states that an organization shall designate someone to be accountable for the management of personal information. This includes the collection, usage, disclosure, retention, and transfer of personal information to third parties for processing.

2. Identifying Purposes

The principle of **Identifying Purposes** states that an organization must clearly identify the purposes for which personal information is collected, either before or at time of collection. This also helps organizations comply with the Openness and Individual Access principles.

3. Consent

The principle of **Consent** states that the knowledge and consent of individuals are required when an organization collects, uses, or discloses personal information, and it must be in such a way that the individual clearly understands.

For example, if an organization offers application forms which require personal information, it may not use ambiguous wording to trick individuals into giving their consent for purposes they cannot reasonably understand. It must be clear and concise.

An organization also cannot refuse to provide a product or service to an individual if that individual refuses to provide personal information that is not required or related to the product or service (e.g. drivers licenses for product returns).

4. Limiting Collection

The principle of **Limiting Collection** states that the personal information an organization collects should only be limited to that which is necessary for the purposes identified.

PIA#: (assigned by Privacy Office) **Topic:**
Information Handling Policies and Procedures

An organization's privacy officer or person(s) responsible for privacy compliance should create information handling policies and procedures and specify what type of personal information is collected. This works in tandem with the Openness principle.

Fair and Lawful Means

An organization must collect personal information by fair and lawful means. Whether collecting personal information in-person, on the phone, or through an application form, an organization shall identify the purposes for doing so, obtain proper consent, and do so in such a way that is clear and straight-forward.

An organization may not use deception, trickery, or ambiguity to construe the purposes for which personal information is used.

5. Limiting Use, Disclosure, and Retention

The principle of **Limiting Use, Disclosure and Retention** states that an organization shall limit the ways it uses, discloses and retains personal information.

This means that an organization should not use or disclose personal information for purposes other than those which it has identified purposes for and received consent for. The organization should only retain personal information for as long as is necessary to fulfill its purposes.

6. Accuracy

The principle of **Accuracy** states that an organization should ensure that the personal information it collects should be accurate, complete, and up-to-date for the purposes for which it is being used.

How Accurate?

An organization should ensure that personal information is accurate, taking into consideration what the personal information is being used for and also taking into consideration the best interests of the individuals.

PIA#: (assigned by Privacy Office) **Topic:**

For example, if an organization collects personal information to conduct pre-employment screening, it should ensure that it makes a serious effort to ensure its accuracy. Not making reasonable strides to ensure the collection of accurate personal information means that an individual's employment could be at stake.

Updating Personal Information

An organization shall not routinely update personal information unless it was collected for a purpose that requires its continual use. This also includes information that is disclosed to third parties.

For example, if customers or clients provide their contact information to subscribe to a company's newsletter, it would be reasonable to ensure that personal information is routinely updated so that the organization can continue to provide subscriptions.

7. Safeguards

The principle of **Safeguards** states that an organization should protect personal information with security safeguards that are appropriate for the sensitivity of personal information held.

Personal information should be protected against loss or theft, unauthorized access, disclosure, copying, use or modification, regardless of what format it is stored in (paper, electronic, etc).

What type of Safeguards Should a Business Use?

If someone owns a small business and collect customers' email addresses for an online newsletter, for example, she might store the emails in a spreadsheet. It then may be reasonable to password protect the spreadsheet and/or encrypt it so that if the spreadsheet were stolen, it would be difficult to decrypt and retrieve the email addresses.

If an organization were to collect more sensitive personal information, such as credit card numbers, the organization would be expected to have much stronger safeguards in place to protect that information.

8. Openness

The principle of **Openness** states that an organization shall make its policies and procedures about how it manages personal information readily available.

It should not provide barriers to access — if an individual is making a request to know about your organization's information handling practices, the request should be done without an unreasonable effort.

When providing the information, it should be available in a form that's generally understandable. The information should be provided in plain, simple English that someone without a university degree can understand — save legalese for your lawyers and contracts

9. Individual Access

The principle of **Individual Access** states that upon an individual's request, an organization shall make known to the individual the existence, use, and disclosure of personal information and give access to it.

If an individual challenges the accuracy or completeness of his or her personal information, the organization shall amend the information where appropriate. This can involve correcting, deleting, or adding personal information.

Where appropriate, your organization should transfer the amended information to third parties.

Exceptions

An organization may deny access to some personal information for a number of reasons.

For example, a request may be denied if information is solicitor-client privileged or if by granting access it would reveal confidential commercial information.

If an organization or public body denies access to personal information, it must notify the individual of the reason for doing so and it must be a legitimate reason allowable by privacy legislation.

The organization should also provide the individual information about their complaint procedures or how to contact the Privacy Commissioner of Canada if the individual wishes to file a complaint about the denied access request.

Requesting Identification

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

Before providing access to or amending personal information, an organization should verify that it is communicating with the correct individual.

Some organizations choose to do this by asking for government-issued identification. Others may ask an individual on the phone to verify his or her account information by providing information such as a maiden name or password before proceeding.

An organization should only collect this information for identification purposes. Once the individual has been identified, the organization should not continue to hold that information, as it has already fulfilled its purpose.

An organization should also not seek to use stringent identification requests as a barrier to access.

Third Party Disclosure

If an individual desires to know which third parties his or her personal information has been disclosed to, the organization shall let the individual know.

If it is difficult to know which third parties personal information may have been disclosed to, then the organization should mention all third parties to which the information *may have been* disclosed to.

Reasonable Time and Costs

An organization should respond to access requests in a reasonable amount of time and at a minimal or no cost to the individual.

An organization shall reply in no longer than 30 days from receipt of the request. If an organization legitimately requires more time to fulfill a request, it must send a notice of extension to the individual, provide the reason for doing so, and notify the individual of his or her right to make a complaint with the Privacy Commissioner of Canada.

Making Information Accessible

If an organization uses abbreviations or codes, it should provide an explanation of what they mean to an individual.

10. Challenging Compliance

The principle of **Challenging Compliance** states that individuals shall be able to challenge an organization's compliance on any of the privacy principles of PIPEDA.

This means that an organization must have procedures in place to receive and respond to complaints and inquiries. The procedures should be simple and easy to use.

An organization must not only have them in place, but also notify individuals who make inquiries or complaints about its existence.

Investigating Complaints

If an organization receives a complaint, it should investigate it — not ignore it. If the complaint is justified, the organization should take appropriate measures to remedy it. This may involve amending the organization's practices and policies.

The organization's privacy officer (or person responsible for privacy compliance) is responsible for accepting and investigating inquiries and complaints.

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

PIA Determination and Template

PIA#: (assigned by Privacy Office) **Topic:**

APPENDIX C

SAMPLE PRIVACY AND CONSENT NOTICE

WE NEED TO COLLECT INFORMATION FROM YOU

UNBC Continuing Studies needs to collect information from you to:

1. Enroll you
2. Confirm sponsorship arrangements
3. Process your payment
4. Generate a class list for instructors
5. Ensure that grades and certificates are assigned to the correct student
6. Assist our partners in verifying certificate validity

WE HAVE PERMISSION TO DO THIS

The University of Northern British Columbia collects, uses, shares, discloses, maintains and when applicable deletes and destroys Personal Information provided on this form according to the *Freedom of Information and Protection of Privacy Act* [RSBC 1996 c. 165].

HOW WE WILL USE AND SHARE YOUR INFORMATION

Continuing Studies must directly disclose some information on this form and your course completion status to your sponsor, including your employer if you are sponsored through your job. Continuing Studies may need to share the information on this form with anyone repairing or maintaining electronic systems involved in this Continuing Studies course.

UNBC Continuing Studies is the training agency chosen to deliver the Wildlife Dangerous Tree Assessor courses on behalf of the Wildlife Dangerous Tree Committee of BC (WDTC). Under the terms of our agreement with the WDTC, Continuing Studies provides a list of current assessors upon request. Under the terms of this agreement UNBC also provides a list of current Fire assessors to BC Wildfire Services (BCWS), twice a year to support certificate verification. Personal information on this form will be shared confidentially with members of the WDTC. Certificate status, certificate number and copies of certificates may be shared upon request by contractors and employers for the purpose of confirming qualifications.

You have the right to revoke consent to the collection, use, retention, and disclosure of personal information at any time, but doing so will result in consequences including, but not limited to, forfeiting registration in the course.

HOW WE WILL PROTECT YOUR INFORMATION

UNBC is obligated to protect your personal information and has various processes in place to ensure it is secure.

HOW LONG WE WILL KEEP YOUR INFORMATION

The *Freedom of Information and Protection of Privacy Act* allows us to keep your Personal Information for at least one year after collection and when its period of usefulness is over we will securely delete or destroy it. In the case of the Wildlife Dangerous Tree Assessor Certificate Program, hardcopy materials are kept for the life of the Certificate, which is four years, before being destroyed.

WHAT TO DO IF THE INFORMATION WE HAVE COLLECTED FROM YOU IS INCORRECT, OR YOU HAVE QUESTIONS?

Please contact UNBC Continuing Studies at: 250-960-5980 OR cstudies@unbc.ca

If you still have questions or concerns, please contact: Doris Marshall-Greenlaw, Governance Officer for Access, Privacy and Records Management at 250-960-5139 OR privacy@unbc.ca

By registering for this course, you indicate you have read, understand, and agree to the privacy statement. You also understand that you have the option to ask questions about any part of this statement before registering.

Signature: _____ Date: _____