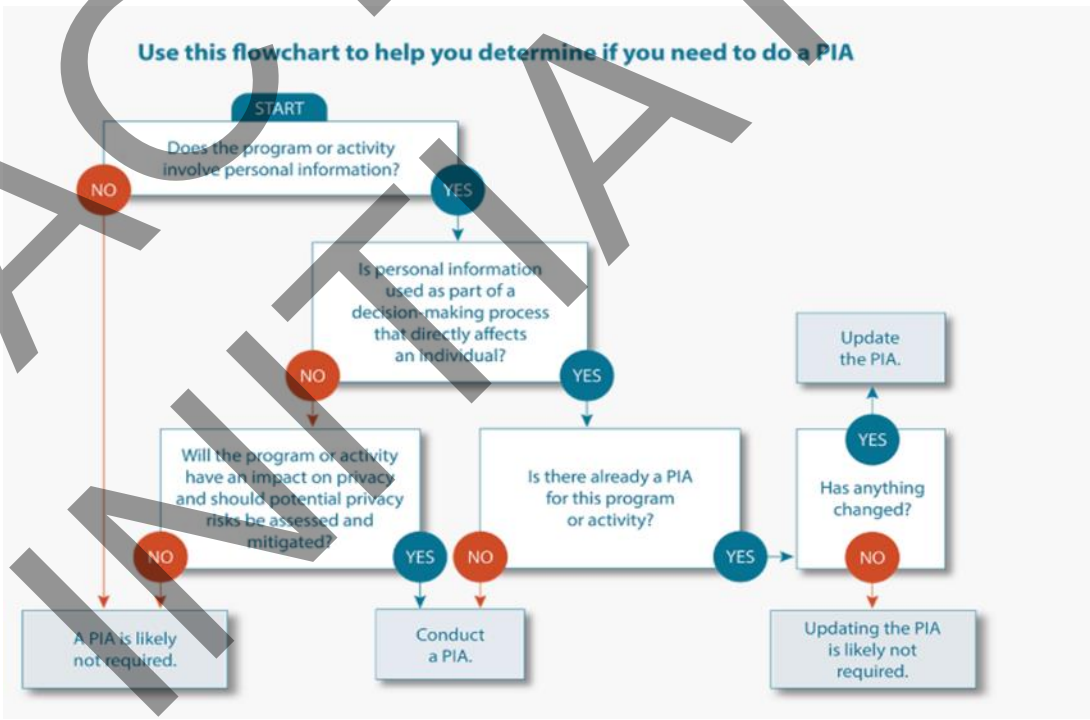
UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

**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.**

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

## PART A

.

**Document Version, Review and Approval History**

| Version | Author | Nature of Change | Date |
|---|---|---|---|
| **1.0** | | | |
| | | | |
| | | | |

## 1. Introduction

How will you carry out the initiative?

1. General Description

In consultation with Carleton Technologies (maker of Bookware), the UNBC Bookstore will implement a new ERP system Bookware that will encompass the POS systems (for in-store and web) as well as inventory control system. This new ERP will cover all existing processes and add additional functionality to the services we can offer students, faculty, and staff.

**a) Name of Program or Service**

What is the initiative?

A system change over from Nebraska's WinPrism to Carleton Technologies Bookware.

Where will the initiative take place?

UNBC Bookstore, in store and online.

Does the work happen online, in person, or both?

Both

Will there be public events?

No

Will you hold meetings over the phone, face-to-face, or online?

Online primarily, but some phone meetings may be required.

**b) Name of Department, Branch and Program Area**
UNBC Bookstore

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

**c) Name of Program or Service Representative**
Carleton Technologies product Bookware

**d) Key Program or Service Dates**

When will the initiative take place?

March 2022-Aug 2022

Is this a one-time event?

This is a one-time system change over, but future implementations of additional service modules and support have been discussed.

Will the initiative go on for a short time or for the foreseeable future?

Production go live must occur before Aug. 1, 2022 as that is when our current POS system will be end of support, but there may be additional tweaking that may be required leading up to Sept. semester.

Do you have an end date planned?

Implementation of new ERP will be completed by Fall of 2022, additional module inclusion may be in future.

## 2. Description

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

**i. Purposes, Goals and Objectives**
Address deficits of existing ERP system, streamline payment processing, add functionality for users and customers, and improve service delivery for securing revenue streams.

**ii. List of All Stakeholders Impacted / Involved**

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

| Stakeholder | Role |
|---|---|
| **Finance** | Handle Moneris account for university (payment processor), consult on financial reporting functionality, and assess accounting procedures |
| **ITS** | Assist with implementation of new ERP (networking and system integrations with Banner), as well as vetting PCI and other regulatory compliance |
| **Office of Registrar** | Approval of integration with student information (i.e. student ID, course registrations) |
| **Bookstore** | Accountable for service delivery and responsible for running system |

### iii. The Need

Why are you doing the initiative?

Current ERP is ending support for POS this year, and end of life 2023. This US based company has plans to upgrade other aspects of ERP but not for at least 2 years. The Bookstore has used this system for over 20 years and the functionality no longer fits with our service standards and operational plans. The system is overcomplicated, not well supported, and no longer meets the Bookstore needs.

What need does the initiative meet?

Bookware is a Canadian product, run by many Canadian schools (several in BC), understands the industry specific needs of Bookstores, and is compliant with regulatory requirements.

The change also creates efficiency with processes, allows for better customer service, and allows us to plan for future changes more effectively.

### iv. Governance Model

Accountability – who is ultimately accountable for the program or system

### v. Relevant Existing Policies

ITS, Bookstore, Finance

### vi. Related PIAs

ITS, Bookstore, Finance

### vii. Relevant contracts

Bookstore

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

### viii. Research / Health System Use

Do you anticipate that data collected by this program / system will be used for research or health system use? If so, please explain and provide details of data state (aggregate, de-identified, anonymized etc.)

No

### b) The Intended Scope (Project and PIA)14

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

i. Scope of PIA
Compliance of regulations related to privacy, financial and cyber security, and additional compliance that is applicable to retail businesses in an academic environment.

ii. Out of Scope of PIA
Additional module integrations that we are not planning to implement for the 2022 product go live launch.

### c) Definitions

| 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 |
| **Merchant** | The Merchant is a business that uses the Software |
| **Personal Information -PI** | means recorded information about an identifiable individual other than contact information |
| **Personal Information Banks** | A PIB is any collection or set of personal information where personal information is organized by:<br>• The individual's name;<br>• An identifying number or symbol; or<br>• Other particular identifier assigned to the individual. |

**PIA: 22-07 Bookware (Carleton Technologies)**

**d) User Access**

How is the project, system, application or initiative accessed by users?

Users access Bookware through a desktop/laptop "client". There is also a Mobile app that can be used; it also functions as a "client" of the server.

Users also access the Bookware system through Point of Sale (POS) terminals. The POS terminals also function as a "client" of the server.

Are there different levels of access dependent on roles?

Yes; Bookware enforces role-based access to programs and the functionality within those programs

## 3. Personal Information Flow Diagram and Explanation

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

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

| Data Element | Rationale for collection, use or disclosure | Method of Collection or Disclosure |
|---|---|---|
| Information that customers of the UNBC bookstore submit about themselves such as, but not limited to, name, address, email address, phone number | This information is collected and used for the purposes of providing customer service. | This information is collected when customers place orders with the bookstore. It is collected either through the e-commerce platform when the customer places an order or it is collected via phone or in person when a customer places an order using either of those methods. |
| Information that the UNBC bookstore collects about its users, such as but not limited to their name, email address, phone number. | This information is collected by the UNBC bookstore to add functionality to Bookware, such as delivering scheduled reports. This information is also stored to identify who is accessing Bookware to meet legal and compliance requirements. | The UNBC bookstore can collect this information however they want. It is then entered into Bookware using the User Configuration application. |
| (Optional) Student numbers | Student numbers are optionally collected by some bookstores to provide the ability to bill a third party who sponsors a student. | Generally, the student numbers (and associated names) are provided to the bookstore through the campus department responsible for managing sponsored student, bursaries, etc. This information is entered into Bookware using the Sponsored Student application. |
| (Optional) Campus identity information such as | This information is optionally collected to identify and correlate an | This information is collected through an export from the campus student information |

| | | |
|---|---|---|
| name,<br>email address, single sign<br>on identity, and student or<br>faculty number. | individual to specific<br>courses. | system or campus registrar system |



## 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**

**All data collected is owned by the Merchant.**

**Customer Privacy**

| What information is collected? | How is it used? |
|---|---|
| Information that Customers submit about themselves:<br>• Name<br>• Address<br>• Phone number<br>• Email address | This information is collected by the Merchant to complete and deliver a Customer order and communicate regarding an order. |

| | |
|---|---|
| • Single Sign On unique identifier | |
| Order History:<br>• Items purchased<br>• Method of payment (no sensitive card holder data is transmitted, processed or stored at any time) | This information is retained in order to provide Customer service. |
| Usage Data, including:<br>• IP address<br>• Web browser<br>• Other data submitted automatically by the Customer's web browser | Logs of when the Software is used by a Customer are collected to meet legal and compliance requirements and are used to improve Bookware's Software. |

**Merchant Privacy**

| What is collected? | How is it used? |
|---|---|
| Information that the Merchant collects about Customers:<br>• Name<br>• Address<br>• Phone number<br>• Email address<br>• Single Sign On unique identifier | This information is collected by the Merchant to complete and deliver Customer orders and communicate regarding orders. |
| Order History:<br>• Items purchased | This information is retained in order to provide Customer service. |

| | |
|---|---|
| • Method of payment (no sensitive card holder data is transmitted, processed or stored at any time) | |
| Usage Data, including:<br>• IP address<br>• Web browser<br>• Other data submitted automatically by the Customer's web browser | Logs of when the Software is used by a Customer are collected to meet legal and compliance requirements and are used to improve the Software. |
| Information that the Merchant collects about Customers who are Sponsored Students:<br>• Student number<br>• Name<br>• Address<br>• Phone number<br>• Email address<br>• Single Sign On unique identifier<br>• Sponsor<br>• Sponsorship amounts | Student numbers are collected by some Merchants to provide the ability to bill a third party who sponsors a student. |
| Information that the Merchant collects about their Vendors:<br>• Vendor name<br>• Contact name<br>• Address<br>• Phone number<br>• Fax number | This information is collected by the Merchant to enable the Merchant to place purchase orders and communicate with the Vendor. |

| | |
|---|---|
| • Email address<br>• Web address | |
| Information that the Merchant collect about their Users, including faculty and staff:<br><br>• Name<br>• Address<br>• Phone number<br>• Email address<br>• Single Sign On unique identifier | This information is collected by the Merchant to add functionality to the Software such as delivering scheduled reports.<br><br>This information is also stored to identify who is accessing the Software to meet legal and compliance requirements. |

Collection is only permitted through knowledgeable implied or express consent.

**Consent**

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:**
https://www.bookstore.unbc.ca/site_terms_of_use.asp? We would provide something similar for content on new website.

**ii. Use**

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

**PIA: 22-07 Bookware (Carleton Technologies)**
***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.*

**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-NA**

**v. Research / Open Data-NA**

**b) The Sources and Accuracy of the Personal Information**

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

Individual customers will provide information, additional information may be verified by their banking institution. Information, such as course materials, may be populated and shown to the customers via integration with Banner if they use SSO.

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

The information should be up to date if the customer wants to receive the correct purchases.

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?

Accounts can be set up and contact information can be updated by customers.

UNBC bookstore users (employees) can correct personal information when necessary through the Customer Maintenance application in Bookware.

### 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), (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?
No

Does any user of the information managed in this initiative access this information from outside of Canada beyond during short-term temporary travel?
No; all of CTI's employees reside in Canada.

Does this initiative have any components that temporarily process information outside of Canada?
No; all data remains in Canada at all times.

Does this initiative store information for operational use outside of Canada?
No; all data remains in Canada at all times.

Does this initiative back up or make additional or redundant copies of information outside of Canada?
No; all data remains in Canada at all times

Will it be stored on portable devices?
No; Bookware data is stored on a server and accessed via a desktop/laptop client application. The data is not stored on the desktop/laptop

Will the data be interfaced with data from other systems? (Data matching or linkage)
No

**Data Linking**

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

Is personal information from one database linked or combined with personal information from another database?
No

Is the purpose for the linkage different from the original purpose for which the personal information in each database was originally obtained or compiled? **NO**

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**

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?
No services are provided through a public body.

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?
No services are provided through a public body.

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,*

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

*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.*

Data retention is defined by the Merchant; Carleton Technologies will delete data only on the request of the Merchant who owns the data.

## 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.
All personal information is stored in a single table in the Bookware database. No other partners or organizations are 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.
Yes

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.
A database table is used for storing personal information. Personal information is stored in an organized manner with a unique code assigned to each database record. All personal information records contain the same types of information

Name:

Location:

Description:

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:

**PIA: 22-07 Bookware (Carleton Technologies)**
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?
Personal information is not de-identified or anonymized as is never leaves the Bookware system

**f) Users of Personal Information**

Please list all users of PI including third parties
The UNBC bookstore will use the personal information for providing customer service. If desired by UNBC, customer email address information will be shared with third party digital product providers (eg. CampusEBookstore.com, Willo Labs, VitalSource) in order for students to purchase/retrieve their digital course materials.

The purchases through the digital product providers are optional, unless the e-textbooks is required and no physical book is available. It may be possible to work with the vendors to provide students a paper copy of the access code in order to retrieve the course material, but the purchase would have to be directly with the Bookstore in this case.

**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).

All actions taken in Bookware are logged and associated with the user who accessed the data.

For all audits, full activity logs can be made available to the auditor, or alternatively, CTI's professional services can be utilized to retrieve audit data on request

## 5. Access Rights for Individuals to their Personal Information

**Access Request Management**

How will you manager access to information requests?
All access of information requests will be referred to UNBC.

If aggregate or de-identified data only to be released, who responsible to do so and how is that done?
No data is released by Carleton Technologies.

**Request for Personal Information from Persons to Whom It Relates**

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**
How will personal requests for access be managed?
All personal requests for access will be referred to UNBC.

**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

### Application Access Controls

[redacted]

UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

[redacted]

**Policy**

[redacted]

**Technical**

[redacted]

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

## 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.

| | |
|---|---|
| [redacted] | |

UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

| | |
|---|---|
| | |

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

## 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:** Zarrah Holvick, Retail Services Manager
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: [redacted] Date: March 14, 2022

**Director or Dean Overseeing the Program/Project:** Lisa Haslett, Director of Business Services & Continuing Studies

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: [redacted] Date: March 15, 2022

**Governance Officer: Doris Marshall Greenlaw**

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 [redacted] ate:15 March 2022

## 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.

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**

| | |
|---|---|
| **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.<br><br>Without restricting the generality of the foregoing, personal information may include, for example:<br>• information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,<br>• 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,<br>• any identifying number, symbol or other particular assigned to the individual,<br>• the address, fingerprints or blood type of the individual.<br>• 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.<br>• 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.<br>• the views or opinions of another individual about the individual.<br>• 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,<br>• 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,<br><br>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,<br>• the fact that the individual is or was an officer or employee of the government institution,<br>• the title, business address and telephone number of the individual,<br>• the classification, salary range and responsibilities of the position held by the individual<br>• the name of the individual on a document prepared by the individual in the course of employment, and,<br>• the personal opinions or views of the individual given in the course of employment.<br>• 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,<br>• 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<br>• information about an individual deceased for more than twenty years. |
| **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:<br>• 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<br>• work with information and privacy commissioners during the investigation of a privacy complaint against an organization.<br><br>Privacy officers may also be responsible for managing changes to an organization's:<br><br>• information management practices, policies and procedures;<br>• staff training, vis-a-vis privacy and information handling;<br>• privacy policies and procedures; and<br>• 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. |

# 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: 22-07 Bookware (Carleton Technologies)**
**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: 22-07 Bookware (Carleton Technologies)**
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

# PIA Determination and Template

**PIA: 22-07 Bookware (Carleton Technologies)**
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: 22-07 Bookware (Carleton Technologies)**

## 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: _____