Privacy Impact Assessment for Non-Ministry Public Bodies
Library Bookware

Royal Roads
UNIVERSITY

Part 1 – General

Name of Department/Branch:	Library
PIA Drafter:	Maureen Changwo and Carolina Carrara
Email:	maureen.changwo@royalroads.ca carolina.carrara@royalroads.ca	Phone:	250.391.2600 ext. 4265
Program Manager:	Rosie Croft
Email:	rosie.croft@RoyalRoads.ca	Phone:	250.391.2600 ext. 2699

1. Description of the Initiative

Bookware software by Carleton Technologies Inc. (CTI) is to be implemented as a Library solution for complete inventory management, point of sale and e-commerce. It is the interface between students and Library. The objective of the Bookware project is to:

- Enable the Library to manage their inventory more efficiently.
- Increase productivity and profitability.
- Improve customer services and cost effectiveness.
- Improve processes and reporting.

It will be implemented as a cloud-based solution that supports both general merchandise and textbook items, including integrated support of new, used and digital copies of textbooks. Once an item is created it is available for use through out the system and tracked as it moves through the purchasing process. Detailed inventory reports can be printed for count discrepancies as well as sales analysis and profit reports. This solution will include;
- Bookware retail management application version 7
- Point of sale (POS) hardware
- Bank drivers for Moneris
- e-Solution version 4.

Phase 1 project scope will include;
- Back office
- Installation of Point-of-Sale (POS) hardware
- Website

- Modules
- Data conversion
- Installation and training
- Campus eBookstore (code sales)

2. Scope of this PIA

The scope of this PIA covers the implementation of the Bookware cloud-based solution: the collection, use, disclosure, security and storage of customers, vendors and student personal information.

3. Related Privacy Impact Assessments

There are no other PIA's that have been developed for this initiative.

4. Elements of Information or Data

a) To set up RRU Library staff on the system and training schedule first name, last names and emails of Library staff will be shared with the vendor.
b) If sponsor cards will be used the student's unique identifier like student number may be shared with the vendor.
c) During payment non-sensitive card holder Information such as name, masked card number, address verification. This is collected for fraud prevention, legal, and compliance requirements.
d) Identity Information such as name, email and student or faculty number.
e) Usage data: IP address, web browser and other data submitted automatically by the customer's web browser.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

5. **Storage or Access outside Canada**

   Data will be stored within Canada in Ottawa and is only accessible only within Canada.
   All data is always stored in Canada. The main office has two stage, two factor authentications to access the server room.

   The physical security of the facility is monitored 24hrs/day, 7days/week; additional CCTV security cameras monitor the interior of the facility 24hrs/day, 7days/week. The data center is temperature and humidity controlled.

   The data center has 2N power redundancy, 2N redundant uninterrupted power supply (UPS) systems, high capacity continuous dual-fuel generators with fuel for a minimum of 24 hours of operation, and 24hrs/day, 7days/week power monitoring.

6. **Data-linking Initiative***

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.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	No
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

* 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). Contact your public body's privacy office(r) to determine how to proceed with this notification and consultation.

For future reference, public bodies are required to notify the OIPC of a" data-linking initiative" or a "common or integrated program or activity" in the early stages of developing the initiative, program or activity. Contact your public body's privacy office(r) to determine how to proceed with this notification.
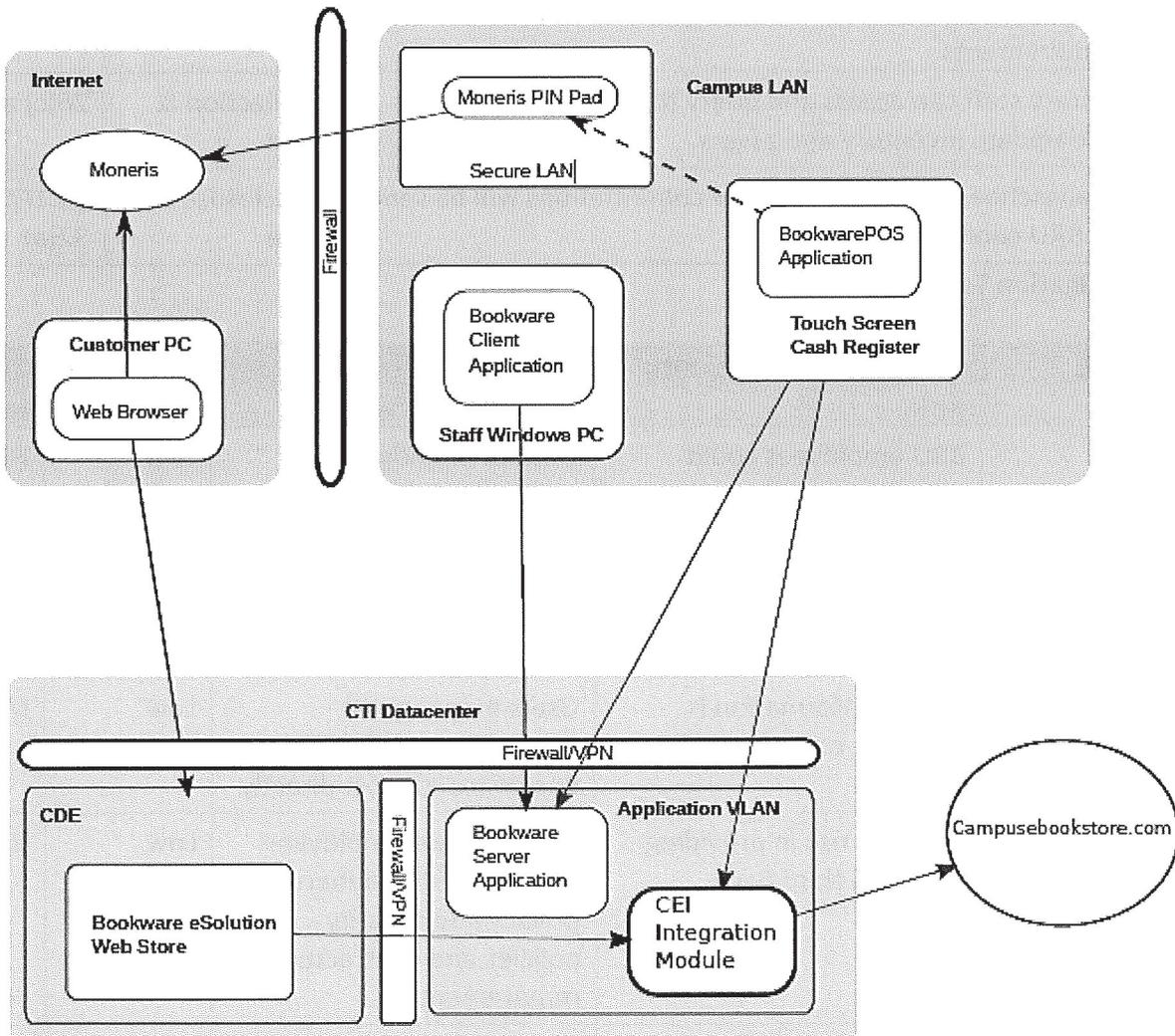
8. **Personal Information Flow Diagram and/or Personal Information Flow Table**

Royal Roads System Integration Diagram

TLS v1.2+ Connection

TLS v1.2+ Card Holder Data Connection

TLS v1.2+ Private/Customer Data Connection

Personal Information Flow Table

	Description/Purpose	Type	FOIPPA Authority
1	Identity Information such as name, email, and student or faculty number.	Use	32(a)
2	During payment non-sensitive card holder Information such as name, masked card number, address verification. This is collected for fraud prevention, legal, and compliance requirements.	Use	32(a)
3	Library staff can access and query the system for reports and update inventory and assets.	Collection & Use	26(c) and 32(a)
4	Transactions receipts and order confirmations will be sent to RRU configured email.	Disclosure & Use	33.1(7) and 32(a)

9. **Risk Mitigation Table**

Risk Mitigation Table

	Risk	Mitigation Strategy	Likelihood	Impact
1.	RRU employees could access personal information via the Point of Sale interface and use or disclose it for personal purposes	Oath of Employment; contractual terms, etc.	Low	High
2.	System information is incorrect or inaccurate	Users may request correction by contacting Bookware support directly	Low	Medium
3.	Inherent risk in providing access to third party	All Bookware employees are required to adhere to privacy and security policies and contractual requirements	Low	High
4.	Customer, student's personal information is compromised in Bookware	Bookware has physical and security measures in place as well as privacy and security policy and contractual requirements	Low	High

5.	Personal Information is compromised when transferred to the service provider	Transmission is encrypted and over a secure line	Low	High
6.	Service provider could move its data centre outside of Canada	Contractual Terms	Low	Medium
7.	A service provider's system upgrade could introduce a security vulnerability	Contractual terms, high security standards and policies	Low	High
8.	Service provider could be compromised by an external attacker resulting in a breach	Contractual terms, high security standards and policies	Low	High

10. Collection Notice

Your personal information is collected under the authority of the *University Act* and is subject to the *Freedom of Information and Protection of Privacy Act*. Your personal information will be used to complete a sales, purchase or support request submitted by you and will be confidentially and consequently shared with our contracted services provider managing this system and will not be disclosed to any other external third parties unless we are directed to do so by you. For more information regarding the collection and use of your personal information please contact Royal Road's University's Privacy Officer via regular email privacyofficer@royalroads.ca

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

11. Please describe the physical security measures related to the initiative (if applicable).

RRU

Section 15(1)(l)

Bookware

Section 15(1)(l), Section 21

12. Please describe the technical security measures related to the initiative (if applicable).

RRU

Section 15(1)(l)

Bookware

Section 15(1)(l), Section 21

13. Does your branch/department rely on any security policies?

RRU

Information Security Policy: http://policies.royalroads.ca/policies/information-security-policy IT Security Policy: IT Services Information Security Framework | Policies & Procedures (royalroads.ca)
Privacy Policy: Privacy | Policies & Procedures (royalroads.ca)

Bookware

Yes, for more information contact privacy@bookware3000.ca

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

RRU

Access to the system is granted based on an individual's role. Staff access may be tracked based on RRU login and Bookware login.

Bookware
Section 15(1)(I), Section 21

15. Please describe how you track who has access to the personal information.

RRU
Audit Trails and physical sign-in and sign-out at the points of sale.

Bookware
Audit trails and CCTV security cameras monitor the interior of the facility 24hrs/day, 7days/week.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

Customers will be responsible for keying in their own information on the website. At the points of sale updates and corrections may be made by the authorized staff. Staff may contact Bookware support directly for any issue.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

    No

    > *Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).*

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

    No

    > *Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).*

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

    No

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Privacy Impact Assessment for Non-Ministry Public Bodies
Library Bookware

Part 6 – Privacy Office Comments

This PIA is based on a review of the material provided to the Privacy Office as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office.

Don Devenney Privacy Officer Royal Roads University	Signature	Date February 9, 2021

Part 7 – Program Area Signatures

Rosie Croft University Librarian Royal Roads University	Signature Rosie Croft	Date Feb 25, 2021
Carolyn Levesque PMP CPHR Associate Vice President, Operations & Resilience Royal Roads University	Signature CLevesque	Date 8 Apr 21
Don Ostergard CIO Royal Roads University	Signature Donald J Ostergard	Date 9 April 2021
Cheryl Eason Vice-President & CFO Royal Roads University	Signature	Date April 27, 2021

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.