

Privacy Impact Assessment

PIA # and Name- APRM_PIA2322_Pay My Tuition

Legislative Requirement

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

A PIA needs to be conducted

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

1. Accountability

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

Finance - specifically the Treasury Services sub-department

1.2 Identify UNBC role responsible for the Initiative

Manager, Treasury Services

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

Finance and Treasury Services will be the budgetary and operational owner of the Pay My Tuition SAAS solution

1.4 Timeline for the initiative

Anticipated start date for the initiative,

5/1/24

Is this a one-time event?

Yes

No

2. Overview

2.1 Describe the New Program or Service or the Change.

PayMyTuition (PMT) offers a comprehensive all-in-one plug-and-play payment solution. PMT integrates with Banner to process and resolve transactions for tuition, fees, and other payment requirements. PMT can handle both domestic and international transactions and can process refunds.

PMT is integrated into the Student Portal. When students go to make a payment, some of their information will be populated into PMT in order to reconcile the transaction to the correct account.

2.2 Describe the Purposes, Goals and Objectives.

Finance goal is to improve the options to students for paying their tuition and enhance the student online payment experience. While a service improvement for the student, an external SAAS solution also acts as a risk mitigation for the management of credit card information and possible privacy/security breaches.

Benefits of PayMyTuition solution:

Reduce UNBC IT development and maintenance on implementing/upgrading payment options - PMT does all the updates independently
Software already has full Banner integration - plug n play; payment components are compartmentalize and can be switched on/off in Banner.
PayMyTuition can keep up with development/regulations and build products/features to be customer oriented (payment portals)
UNBC pays a small annual maintenance fee
Can continue to work with our current suppliers - Moneris, Western Union, billpay with bank partners
Adds eTransfer as an additional payment and refund option (option requested by payors).
Creates efficiencies for Finance to refund online bank payments (paperless banking information held).

2.3 List any Relevant PIAs

2.4 List any relevant contracts or software purchases.

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

Pay My Tuition (in progress)

2.5 List all interested parties impacted / Involved

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

Interested Party	Role in the initiative
Clients (UNBC students and non-students)	Use PMT to make payments
Manager, Treasury Services	Administers user access and runs audit reports
Treasury Services Staff	Reconcile payments and initiates refunds
ITS Staff	Troubleshooting or support

ACTING INITIATIVE

3. Collection of Personal Information

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

Data Element name, email, id#, grade	Rationale for collection	Method of Collection	FIPPA Authorization
Payment information	Required to process payment	Direct Indirect NA	26(c)
Name of payee	Required to process payment	Direct Indirect NA	26(c)
Email of payee	Required to confirm payment or follow up with any discrepancies	Direct Indirect NA	26(c)
UNBC student ID number	Link the transaction to the account in Banner	Direct Indirect NA	26(c)
Address of payee	Required to process payment	Direct Indirect NA	26(c)
		Direct Indirect NA	TBD
		Direct Indirect NA	TBD

3.2 Describe how personal information is to be collected.

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

Students will log into Ellucian Experience UNBC Student Portal. When they go to make a payment, some of their information will be populated into PMT. Users will then enter their payment information into PMT and the transaction will be processed. PMT will then reconcile payments with the user's Banner account. UNBC staff will not have access to any financial information collected by PMT.

4. Use of Personal Information

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

User (UNBC Roles e.g Governance officer)	How the info is used	FIPPA Authorization
Manager, Treasury Services	- Will use transaction data for reporting - Will use data for auditing	32(a)
Treasury Services Representative	- Payment reconciliation and refunds	32(a)
Financial Services Officer	- Payment reconciliation and refunds	32(a)
		TBD

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

Does the initiative involve using personal information to make a decision about an individual?

Yes No

Does the initiative have a retention schedule regarding personal information used to make decisions?

Yes No

If the initiative involves using personal information to make a decision about an individual, but does not have a record retention schedule, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

Transaction information will be noted in the student's Banner account. This information will be stored for at least one year in order to process any necessary refunds.

5. Research/ Health System Use of Personal Information

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

Yes

No

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

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

Empty text box for response to question 5.2.

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

Empty text box for response to question 5.3.

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

Empty text box for response to question 5.4.

6. Storage of Personal Information

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

Yes

No

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

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

Yes

No

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

- PMT uses AWS and Microsoft Azure servers in both Canada and the United States for storage.
- Transaction confirmation will be stored in Banner.
- Transaction reports may be stored within UNBC systems (G drive, sharepoint, etc.).

7. Disclosure of Personal Information

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

Yes

No

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

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

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

8. Accuracy and Correction of Personal Information

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

- Payees will be required to enter payment information themselves. If the information entered is not accurate or complete, then the transaction will fail to go through. UNBC will not have access to this financial information, and so will not be able to verify its accuracy.
- Information that is automatically populated by Banner is verified when students are registered.

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

Yes

No

8.3 If yes, please describe your process below?

- Any user information that is automatically populated can be corrected in Banner.
- There is no process to correct information entered into PMT directly.

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

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

The department receiving such a request would coordinate with Privacy to ensure adherence to the proper notification process.

9. Personal Information Bank

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

Personal information banks contain personal information that is:

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

9.1 Will your initiative result in a personal information bank?

Yes

No

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

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

AG INITIATIVE

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

AG INITIATIVE

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

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

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

Manager, Treasury Services	Name, student number, email, payment amount, and audit logs.
Treasury Services Representative	Name, student number, email, and payment amount.
Financial Services Officer	Name, student number, email, and payment amount.

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

- Manager, Treasury Services
- Other approved Finance or Treasury Services administrators

9.6 Describe the process for auditing user access.

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

Treasury Services will define the data available and develop the audit process in the first year of this initiative.

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

Yes

No

9.8 Are the audit logs immutable?

Yes

No

9.9 Is the system responsive or passive?

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

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

Users will have their access revoked.

10. Common or Integrated Program or Activity

In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.

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

Yes

No

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

Yes

No

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

Yes

No

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

11. Privacy and Security Safeguards

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

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

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

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

12. Privacy Risk Identification and Mitigation

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

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

--	--	--	--	--

13. Collection Notice

All collection notices must include the:

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

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

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

13.1 Privacy notice

Be sure to include all 3 required parts of the notice

Your personal information is being collected by UNBC in order to process your payment. UNBC is authorized to collect this information under the Freedom of Information and Protection of Privacy Act section 26(c). If you have any questions about the collection of your personal information, please contact [email].

13.2 Location of Privacy Notice

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

When student are directed to make a payment after logging into the Student Portal.

14. Signing and Approval

Individual leading the Program/Project: William Chew

Position: Manager, Treasury Services

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

Signature: _____

Date: May 5, 2024

Director/Dean Overseeing the Program/Project: Director, Finance

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: May 9, 2024

Vice-President authorizing the Program/Project: Vice-President, Finance and Administration

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

Signature: _____

Date: May 9, 2024

Privacy Officer reviewing the Program/Project: Christopher Ross

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

Signature: _____

Date: 5/10/24

15. Reference Tools

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

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

Privacy Impact Risk assessment:

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

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

[Return to Risk Matrix](#)