Privacy Impact Assessment for Non-Ministry Public Bodies

Table of Contents

Use this privacy impact assessment (PIA) template if you work for or a service provider to a non-ministry public body in B.C. and are starting a new initiative or significantly changing an existing initiative.

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Touch Net
Organization:	UNBC
Branch or unit:	Information Technology Services
Your name and title:	Sam Broadfoot, IT
Your work phone:	N/A
Your email:	Sam.broadfoot@unbc.ca

Initiative Lead name and title:	Lisa Haslett, Director, Business Services and Continuing Studies
	William Chew, Manager, Treasury Services
	Pat Herbert, Manager, Enterprise Systems and Projects
Initiative Lead phone:	250-960-6443
Initiative Lead email:	Lisa.haslett@unbc.ca
Privacy Officer:	Rahim Somani
Privacy Officer phone:	250-960-5235
Privacy Officer email:	Rahim.Somani@unbc.ca

General information about the PIA:

Data linking

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 this initiative a data-linking program under FIPPA Section 36?
Yes [Yes]
No [ ]
If this PIA addresses a data-linking program, the privacy Office must submit this PIA to the Office of the Information and Privacy Commissioner, and be subject to their examination, advice and timelines.
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?
Yes [ ]
No [No]

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?
Yes [ ]
No [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.
Related PIAs, if any:

1.   What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

The initiative is to transition from on-premise software to a cloud-hosted software upgrade and to replace UNBC's current ID card system that approached end of life effectively September 1, 2022. This cloud-base software will combine the current two step print and encoding process, reduce workload for ongoing support in ITS for upgrades and system maintenance, and provide enhanced services to students, staff, and faculty through either an online platform or mobile app for self-service photo uploads and management. In addition, the cloud-hosted system will maintain existing functionality of the current ID Card, including utilization of existing card reader equipment on Ricoh multi-functional printer devices.

Key stakeholders and functionalities include:

Facilities Management - Electronic Access Controls

Dana Hospitality – Meal plans, currently a manual process matching of ID Cards against the master UNBC student report for tracking of meal plan balances

Treasury Services – Printing of photo ID cards for students, staff, and faculty

Library – Photo ID –bar code and number scanning to match and create patron accounts in the Library system

3

This initial step is part of a broader proposal to assess the current student fee structure towards a sustainable revenue approach. Upgrades, testing, and implementation of the cloud-hosted software is anticipated for December 2022. With assumptions that in the second year of the five-year agreement with Touchnet, a full assessment of modules available within the Touchnet enterprise solution will be undertaken. This will identify opportunities for expanding the use and functionality that may be implemented beyond the current ID and door access functions.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

The scope of the PIA is to combine the current two-step print and encoding process and transition from on-premise software to a cloud-hosted software upgrade.

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

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

EXAMPLE:

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure
First & Last name	Required to register and correctly identify individual.	Direct
ID Number	Required for UNBC identification	Direct
Library Number	Required for UNBC identification	Direct

3.1   Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes | yes |

No | |

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4.   How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5.   Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority	Other legal authority
Step 1: Student/Employee information is stored in Banner	Collection	26(c)	

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority	Other legal authority
Step 2: Student/Employee information is imported into Touchnet	Collection	26(c)	
Step 3: Student/Employee information is printed on the ID Card	Use	26(c)	

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

6.   Collection Notice

If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice (except in limited circumstances).

Review the sample collection notice and write your collection notice below. You can also attach the notice as an appendix.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7.   Is any personal information stored outside of Canada?

Yes   Yes

No

8.   Does your initiative involve sensitive personal information?

Yes

No   No

6

- If yes, go to question 9

- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FIPPA section 33(1)? N/A

Yes `-----`

No `----`

If yes, go to question 10

- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

Atlanta, Georgia (United States)

After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer. More help is available in the https://www.oipc.bc.ca/resources/guidance-documents/

11. Is the sensitive personal information stored by a service provider? N/A

Yes `-----`

No `-----`

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12.   Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored. N/A

13.   Does the contract you rely on include privacy-related terms? N/A

Yes | ----- |

No | ----- |

- If yes, describe the contractual measures related to your initiative.

15. What controls are in place to prevent unauthorized access to sensitive personal information? N/A

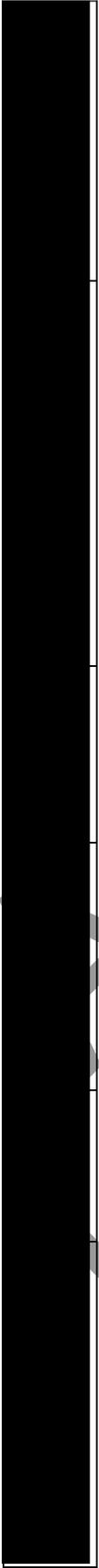**16. Provide details about how you will track access to sensitive personal information.**

N/A

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

ACTIVE
INITIATIVE

> **Outcome of Part 4**
>
> The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

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

Yes | yes |

No | |

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FIPPA section 30

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FIPPA section 30?

Yes | |

No | No |

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

Describe where the digital records for your initiative are stored (e.g., on your organization's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.

If you have completed a security assessment, please append it to the PIA.
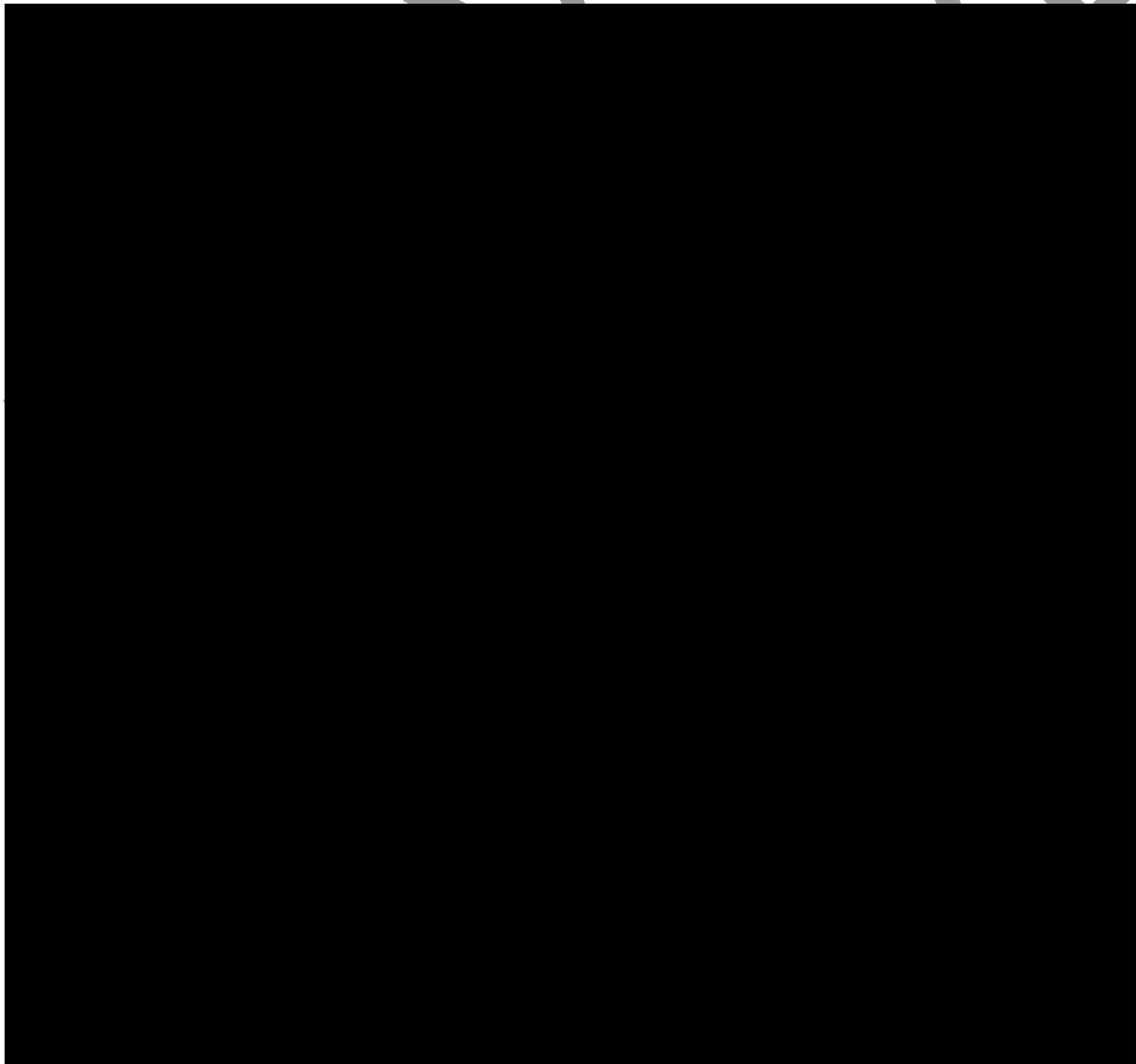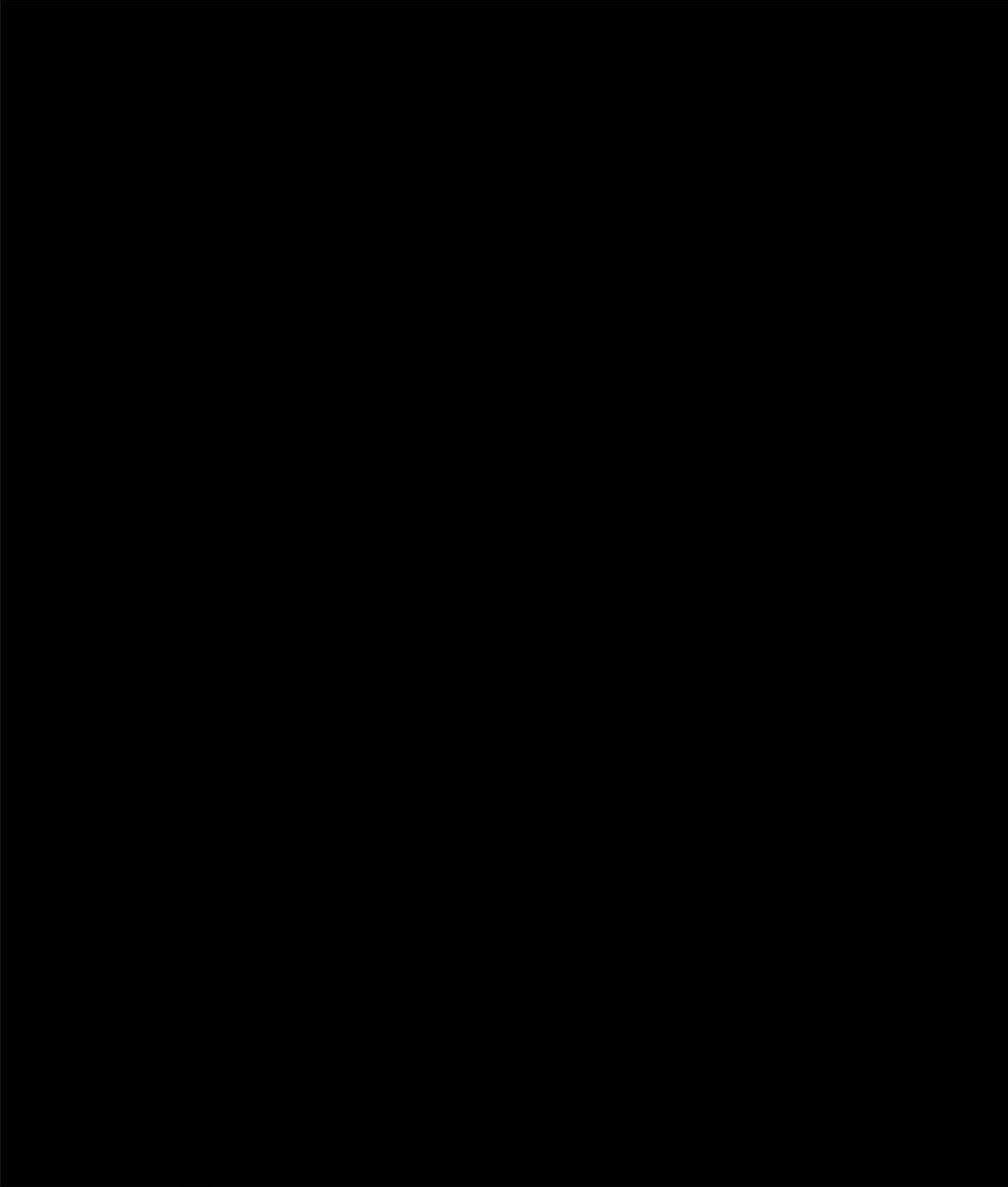
20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	**yes**
Employees that need standing or recurring access to personal information must be approved by executive lead	**yes**
We use audit logs to see who accesses a file and when	**yes**
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

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

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

22. Requests for correction

FIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

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

Yes | yes |

No | |

14

Sometimes it's not possible to correct the personal information. **FIPPA** requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Yes | yes |

No | |

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

Yes | yes |

No | |

23. Does your initiative use personal information to make decisions that directly affect an individual?

Yes | |

No | no |

- If yes, go to question 25
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the **Information Management Act** requires that you dispose of government information only in accordance with an approved information schedule.

Yes | -------- |

No | -------- |

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: PERSONAL INFORMATION BANKS

A <u>personal information bank</u> 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

25. Will your initiative result in a personal information bank?

Yes | X |

No | |

- If yes, please complete the table below.

Describe the type of information in the bank
First and Last Name
UNBC ID
"Expiry Date"
If person is a student
If person is an employee
Photo of person
Name of main organization involved
TouchNet
Any other ministries, agencies, public bodies or organizations involved
Not applicable, but when the product is expanded in the future the involvement of other organizations needs to be considered.

16

Business contact title and phone number for person responsible for managing the Personal Information Bank

Financial Services – Treasury Services

William Chew, Manager, Treasury Services, 250-960-5516

Information Technology Services

Jim Raposo, ITS Solutions Architect, 250-960-5162

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

26. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Add new rows if necessary.

Possible risk	Response
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Chief Information Security Officer Signature	[REDACTED]	Date signed	Dec 20, 2022

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Rahim Somani, VP Finance and Administration	[REDACTED]	December 19, 2022

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead	Lisa Haslett, Director Business Services and Continuing Studies	[REDACTED]	Nov 29, 2022
Program/Department Manager	William Chew, Manager, Treasury Services and Pat Herbert, Manager	[REDACTED]	Dec 12, 2022 — 2022-12-12

18

Role	Name	Electronic signature	Date signed
	Enterprise System and Projects		
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA	Jim Raposo, Solutions Architect, ITS		
Head of public body, or designate (if required)	Rahim Somani, VP Finance and Administration		