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:	**Microsoft 365: MS Editor and MS Forms**
Organization:	**University of Northern British Columbia**
Branch or unit:	**Information Technology Services**
Your name and title:	**Lori Olson- ITS Process Coordinator**
Your work phone:	**250-960-6730**
Your email:	**Lori.olson@unbc.ca**

Initiative Lead name and title:	**Trevor Fuson** **Chief Information Officer**
Initiative Lead phone:	**250-960-5687**
Initiative Lead email:	**Trevor.fuson@unbc.ca**
Privacy Officer:	**Doris Marshall - Greenlaw**
Privacy Officer phone:	**250-960-5139**
Privacy Officer email:	**privacy@unbc.ca**

General information about the PIA:

Data linking

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

Editor and Forms are part of the Microsoft Cloud platform and suite of products. It will integrate with other parts of the platform

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

Any data housed within the M365 platform is not explicitly linked, rather integrated to enhance the use of the platform and its toolset

Is this initiative a data-linking program under FIPPA Section 36?

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** ☐ **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** ☐ **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.

This PIA addresses the use of two Microsoft 365(M365) products and services that UNBC IT is making available for use by UNBC faculty, staff, and students.

- **MS Editor: will be used to check grammar and style refinements like clarity, conciseness, formality, vocabulary suggestions, and highlight similarities in other publications.**
- **MS Forms: will be used as a survey tool to replace Survey Monkey for non-research purposes.**

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?

The scope of this PIA is the implementation of M365 products and services for direct use by UNBC faculty, staff, students, and other individuals who are authorized to use these products and services.

What is out of scope of this PIA?

The scope of this PIA excludes review and considerations of:

- **The content or use of the content of files created, stored, or shared by users via M365 and MS Azure service offerings**
- **Enterprise implementation and/or use of previously installed Microsoft Office products and services.**
- **Physical security and other controls associated with devices used to access services**

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.

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure
Microsoft 365 Account.	https://privacy.microsoft.com/en-us/privacystatement#mainmicrosoftaccountmodule With a Microsoft account, you can sign in to Microsoft products, as well as those of select Microsoft partners. Personal data associated with your Microsoft account includes credentials, name and contact data, payment data, device and usage data, your contacts, information about your activities, and your interests and favorites. Signing in to your Microsoft account enables personalization and consistent experiences across products and devices, permits you to use cloud data storage, allows you to make payments using	Direct

<table>
<tr>
<td></td>
<td>payment instruments stored in your Microsoft account, and enables other features.

There are three types of Microsoft account:

When you create your own Microsoft account tied to your personal email address, we refer to that account as a personal Microsoft account.
When you or your organization (such as an employer or your school) create your Microsoft account tied to your email address provided by that organization, we refer to that account as a work or school account.
(not applicable to UNBC) -When you or your service provider (such as a cable or internet service provider) create your Microsoft account tied to your email address with your service provider's domain, we refer to that account as a third-party account.</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>The data elements used to synchronize users' Enterprise Active Directory accounts to Microsoft's Azure Active Directory. As described in the M365 PIA- "Azure Active Directory is a modern identity management solution spanning on premises and cloud, providing the necessary security capabilities for application access control,
federation, identity management, user provisioning, information protection, standard protocols support, comprehensive development libraries, and more."

Elements of User Data that will be synchronized with Microsoft Azure Active Directory

<table>
<tr><th>Attribute</th><th>IsExported</th><th>IsMandatory</th><th>Comments</th></tr>
<tr><td>accountEnabled</td><td>TRUE</td><td>TRUE</td><td>Defines if an account is enabled</td></tr>
<tr><td>accountName</td><td>TRUE</td><td>FALSE</td><td></td></tr>
<tr><td>altRecipient</td><td>TRUE</td><td>FALSE</td><td></td></tr>
<tr><td>assistant</td><td>TRUE</td><td>FALSE</td><td></td></tr>
<tr><td>authOrig</td><td>TRUE</td><td>FALSE</td><td></td></tr>
<tr><td>c</td><td>TRUE</td><td>FALSE</td><td>Country Abbreviation</td></tr>
<tr><td>cloudUserCertificate</td><td>TRUE</td><td>FALSE</td><td></td></tr>
</table>
</td>
<td>Direct</td>
</tr>
</table>

	cloudUserSMIMECertificate	TRUE	FALSE		
	cn	TRUE	FALSE	Common Name	
	co	TRUE	FALSE	Country Code	
	company	TRUE	FALSE	UNBC	
	countryCode	TRUE	FALSE	Region Code	
	dLMemRejectPerms	TRUE	FALSE		
	dLMemSubmitPerms	TRUE	FALSE		
	department	TRUE	FALSE	Department – populated from banner into AD on premise	
	description	TRUE	FALSE	UNBC filled in on occasion to help distinguish work accounts	
	deviceId	TRUE	FALSE		
	deviceOSType	TRUE	FALSE		
	deviceTrustType	TRUE	FALSE		
	displayName	TRUE	FALSE	The customizable name – the preferred or given name in some cases	
	distinguishedName	TRUE	FALSE	The full location path within active directory.	
	domainFQDN	TRUE	FALSE		
	domainNetBios	TRUE	FALSE		
	employeeID	TRUE	FALSE	This is not the UNBC	

				number – and is not populated by default	
	extensionAttribute1	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute10	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute11	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute12	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute13	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute14	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute15	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute2	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute3	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute4	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute5	TRUE	FALSE	Custom Attribute	

				from UNBC-AD	
	extensionAttribute6	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute7	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute8	TRUE	FALSE	Custom Attribute from UNBC-AD	
	extensionAttribute9	TRUE	FALSE	Custom Attribute from UNBC-AD	
	facsimileTelephoneNumber	TRUE	FALSE	Not populated	
	givenName	TRUE	FALSE	Name	
	hideDLMembership	TRUE	FALSE		
	homePhone	TRUE	FALSE	If populated by the user	
	info	TRUE	FALSE		
	initials	TRUE	FALSE	Single Initial	
	ipPhone	TRUE	FALSE	Not populated	
	isIntuneManagedDevice	TRUE	FALSE	This is about a computer object, so is not PII	
	l	TRUE	FALSE	City	
	legacyExchangeDN	TRUE	FALSE	System attribute	
	mail	TRUE	FALSE		
	mailNickname	TRUE	FALSE		
	managedBy	TRUE	FALSE	Contact information – if employee	
	manager	TRUE	FALSE	Contact information	

				– if employee
member	TRUE	FALSE		
middleName	TRUE	FALSE		
mobile	TRUE	FALSE		If populated by user – some UNBC mobiles are published
msDS-HABSeniorityIndex	TRUE	FALSE		
msDS-PhoneticDisplayName	TRUE	FALSE		
msExchArchiveGUID	TRUE	FALSE		
msExchArchiveName	TRUE	FALSE		
msExchAssistantName	TRUE	FALSE		
msExchAuditAdmin	TRUE	FALSE		
msExchAuditDelegate	TRUE	FALSE		
msExchAuditDelegateAdmin	TRUE	FALSE		
msExchAuditOwner	TRUE	FALSE		
msExchBlockedSendersHash	TRUE	FALSE		
msExchBypassAudit	TRUE	FALSE		
msExchBypassModerationLink	TRUE	FALSE		
msExchCoManagedByLink	TRUE	FALSE		
msExchDelegateListLink	TRUE	FALSE		
msExchELCExpirySuspensionEnd	TRUE	FALSE		

	msExchELCExpirySuspensionStart	TRUE	FALSE		
	msExchELCMailboxFlags	TRUE	FALSE		
	msExchEnableModeration	TRUE	FALSE		
	msExchExtensionCustomAttribute1	TRUE	FALSE	Custom Attribute from UNBC-AD	
	msExchExtensionCustomAttribute2	TRUE	FALSE	Custom Attribute from UNBC-AD	
	msExchExtensionCustomAttribute3	TRUE	FALSE	Custom Attribute from UNBC-AD	
	msExchExtensionCustomAttribute4	TRUE	FALSE	Custom Attribute from UNBC-AD	
	msExchExtensionCustomAttribute5	TRUE	FALSE	Custom Attribute from UNBC-AD	
	msExchHideFromAddressLists	TRUE	FALSE		
	msExchImmutableId	TRUE	FALSE		
	msExchLitigationHoldDate	TRUE	FALSE		
	msExchLitigationHoldOwner	TRUE	FALSE		
	msExchMailboxAuditEnable	TRUE	FALSE		
	msExchMailboxAuditLogAgeLimit	TRUE	FALSE		

	msExchMailboxGuid	TRUE	FALSE		
	msExchModeratedByLink	TRUE	FALSE		
	msExchModerationFlags	TRUE	FALSE		
	msExchRecipientDisplayType	TRUE	FALSE		
	msExchRecipientTypeDetails	TRUE	FALSE		
	msExchRemoteRecipientType	TRUE	FALSE		
	msExchRequireAuthToSendTo	TRUE	FALSE		
	msExchResourceCapacity	TRUE	FALSE		
	msExchResourceDisplay	TRUE	FALSE		
	msExchResourceMetaData	TRUE	FALSE		
	msExchResourceSearchProperties	TRUE	FALSE		
	msExchRetentionComment	TRUE	FALSE		
	msExchRetentionURL	TRUE	FALSE		
	msExchSafeRecipientsHash	TRUE	FALSE		
	msExchSafeSendersHash	TRUE	FALSE		
	msExchSenderHintTranslations	TRUE	FALSE		
	msExchTeamMailboxExpiration	TRUE	FALSE		

msExchTeamMailboxOwners	TRUE	FALSE		
msExchTeamMailboxSharePointLinkedBy	TRUE	FALSE		
msExchTeamMailboxSharePointUrl	TRUE	FALSE		
msExchUserHoldPolicies	TRUE	FALSE		
msOrg-IsOrganizational	TRUE	FALSE		
msRTCSIP-ApplicationOptions	TRUE	FALSE		
msRTCSIP-DeploymentLocator	TRUE	FALSE		
msRTCSIP-Line	TRUE	FALSE		
msRTCSIP-OptionFlags	TRUE	FALSE		
msRTCSIP-OwnerUrn	TRUE	FALSE		
msRTCSIP-PrimaryUserAddress	TRUE	FALSE		
msRTCSIP-UserEnabled	TRUE	FALSE		
oOFReplyToOriginator	TRUE	FALSE		
objectSid	TRUE	FALSE	Used to ensure that AAD and ADDS are in sync	
onPremisesUserPrincipalName	TRUE	FALSE		
otherFacsimileTelephoneNumber	TRUE	FALSE		

	otherHomePhone	TRUE	FALSE	Not populated	
	otherIpPhone	TRUE	FALSE	Not populated	
	otherMobile	TRUE	FALSE	Not populated	
	otherPager	TRUE	FALSE	Not populated	
	otherTelephone	TRUE	FALSE	Not populated	
	pager	TRUE	FALSE	Not populated	
	physicalDeliveryOfficeName	TRUE	FALSE	UNBC address	
	postOfficeBox	TRUE	FALSE	N/A	
	postalCode	TRUE	FALSE	UNBC Address	
	preferredLanguage	TRUE	FALSE		
	proxyAddresses	TRUE	FALSE		
	publicDelegates	TRUE	FALSE	Contact information	
	pwdLastSet	TRUE	FALSE	Used by both password synchronization application and federation tools	
	registeredOwnerReference	TRUE	FALSE		
	reportToOriginator	TRUE	FALSE		
	reportToOwner	TRUE	FALSE		
	securityEnabled	TRUE	FALSE		
	sn	TRUE	FALSE	Surname	
	st	TRUE	FALSE	UNBC Work Street	

	streetAddress	TRUE	FALSE	UNBC Work Address
	targetAddress	TRUE	FALSE	
	telephoneAssistant	TRUE	FALSE	
	telephoneNumber	TRUE	FALSE	
	thumbnailPhoto	TRUE	FALSE	Photo – if they have put one into outlook or OWA.
	title	TRUE	FALSE	Title
	unauthOrig	TRUE	FALSE	
	url	TRUE	FALSE	
	usageLocation	TRUE	FALSE	Used for license assignment
	userCertificate	TRUE	FALSE	Public Key Certificate
	userPrincipalName	TRUE	TRUE	Contact Information – UPN is the login ID for the user
	userSMIMECertificate	TRUE	FALSE	S/MIME Public Key Certificate
	wWWHomePage	TRUE	FALSE	

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 ☐

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.

We use Multi-factor authentication to sign into M365 account.

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**
Step 1: UNBC ITS set up accounts using Employee UNBC login credentials	Collection	Section 26
Step 2: User inputs username and password	Collection	

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
Step 3: Single sign on gets authentication from the active directory file system (first name, last name, and email)	Use	Section 32
Step 4: Users access M365 apps and saves work on M365 servers	Use	

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.

Upon opening Forms, the following is displayed:

Permissions

This app has the following permissions:

- Receive messages and data that I provide to it.
- Send me messages and notifications.
- Access my profile information such as my name, email address, company name and preferred language.
- Receive messages and data that team or chat members provide to it in a channel or chat.
- Send messages and notifications in a channel or chat.
- Access information from this team or chat such as team or chat name, channel list and roster (including team or chat member's names and email addresses) - and use this to contact them.

- Access information from this meeting such as meeting name, schedule, join link, and roster.
- Mute and unmute the incoming audio of this meeting.

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 ☐

No ☐

8. Does your initiative involve sensitive personal information?

Yes ☐

No ☐

- 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)?

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?

Microsoft Forms data is stored on servers in the United States, and Editor is stored in Canada.

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?

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

Microsoft will:

- not collect or use student personal data beyond that needed for authorized educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioral targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorized educational or school purposes or as authorized by the parent, guardian, or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the educational service, if any, are obligated to implement these same commitments for student personal data.

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

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

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

Yes ☐

No ☐

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

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- not collect or use student personal data beyond that needed for authorized educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioral targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorized educational or school purposes or as authorized by the parent, guardian, or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the educational service, if any, are obligated to implement these same commitments for student personal data.

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

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

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

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.

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 ☐

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?

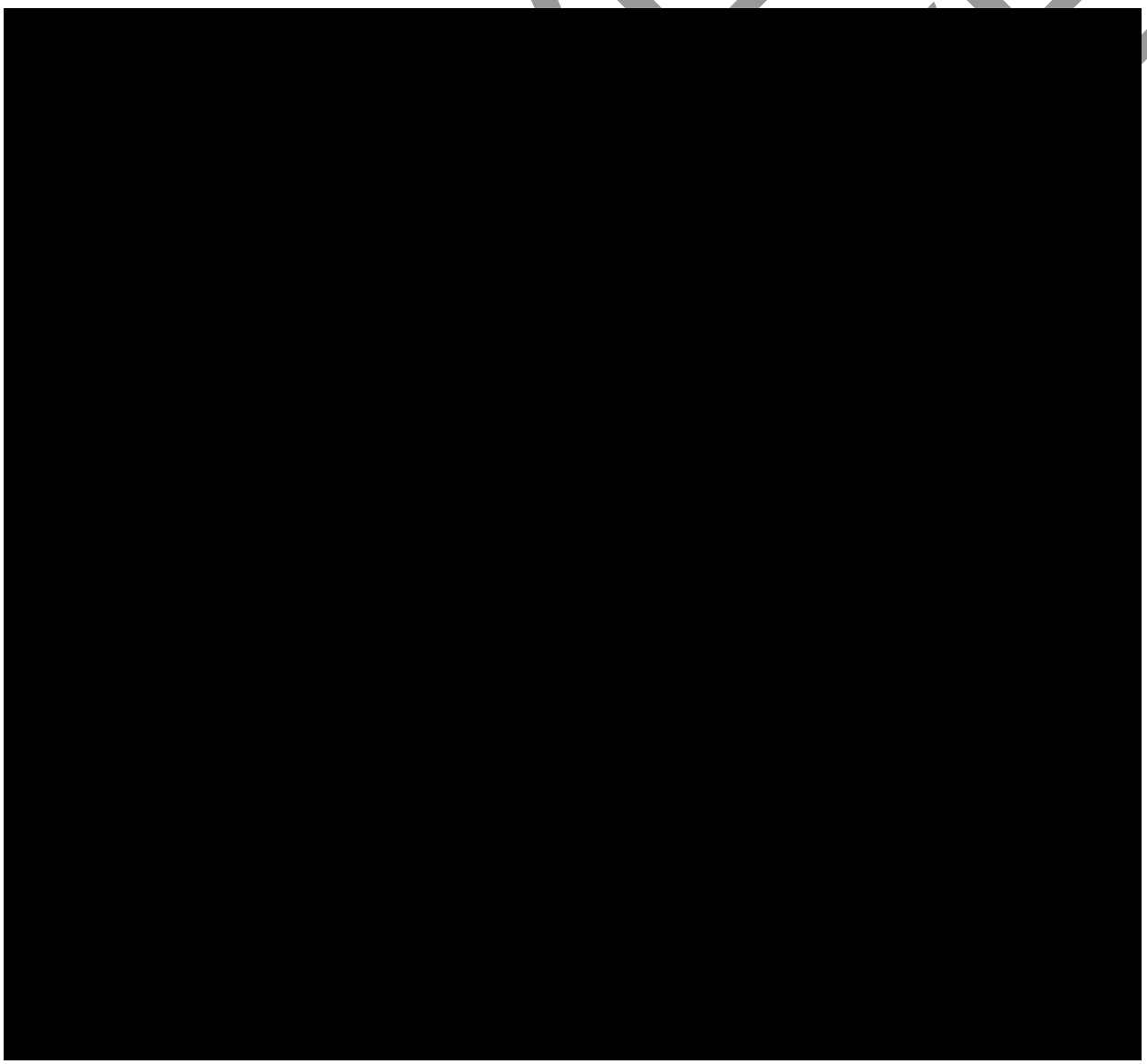
Yes ☐

No ☐

- 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.



[redacted]

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	
[redacted]	

Strategy	
Describe any additional controls:	
[redacted]	

[redacted]

[redacted]

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.

HR and Registrars office manages the records of students and staff.

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 ☐

No ☐

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 ☐

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 ☐

No ☐

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

Yes ☐

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 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

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

Yes ☐

No ☐

- If yes, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

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**
[redacted]	[redacted]

Possible risk	Response
[redacted]	

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

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	Doris Marshall-Greenlaw	[redacted]	2 Sept 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	Lori Olson	[redacted]	Sept 2, 2022
Program/Department Manager	Trevor Fuson		9/2/2022
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA	David Kubert		Sept. 02,2022
Head of public body, or designate (if required)			