PART 1: GENERAL INFORMATION

Initiative title:	Springshare LibGuides CMS
Department or program area:	Learning Commons and Academic Success Centre
Initiative Sponsor (usually administrator overseeing implementation):	VP Student Affairs
Initiative Lead name and title:	Ignacio Albarracin, Director, Learning Commons and Academic Success Centre
Initiative Lead phone:	5298
Initiative Lead email:	albarracini1@cnc.bc.ca
PIA Contributors (name, title and contact information)	Click or tap here to enter text.
Privacy Officer:	Elyse Giddens
Privacy Officer phone:	250-565-2131 ext 5479
Privacy Officer email:	foipp@cnc.bc.ca

1.1. General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
☐ Yes ☒ No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
☐ Yes ☒ No
Related PIAs, if any:
Click or tap here to enter text.

1.2. What is the initiative?

LibGuides is a versatile platform tailored to meet libraries' needs, allowing users to create and share online guides on various topics, subject areas, courses, services, and collections. It

also includes helpful features for customizing, managing, and organizing web content. One of its standout features is the A-Z Database List, which makes it easy for patrons to search and browse research databases. With LibGuides, you can easily create and organize guides and make them accessible to patrons. Patrons can find published guides on the LibGuides homepage or search for relevant guides on our site.

1.3. What is the scope of the PIA?

The use of LibGuides for web content and online guides. Other modules of LibGuides are not part of this PIA.

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

CNC Learning Commons faculty and staff will create admin accounts to create and edit web content. They will use their name and CNC work email address to create their account.

1.5. Did you list personal information in question 1.4?

☐ Yes, go to Part 2

☒ No, answer question 1.6 and submit Part 1 the Privacy Officer. You do not need to complete the rest of the PIA template.

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

Faculty and staff will be required to use their CNC email address to create their admin 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.

2.1 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	FOIPPA authority	Other legal authority
Step 1: Click or tap here to enter text.	☐ Collection ☐ Use ☐ Disclosure	Click or tap here to enter text.	Click or tap here to enter text.
Step 2: Click or tap here to enter text.	☐ Collection ☐ Use ☐ Disclosure	Click or tap here to enter text.	Click or tap here to enter text.
Step 3: Click or tap here to enter text.	☐ Collection ☐ Use ☐ Disclosure	Click or tap here to enter text.	Click or tap here to enter text.
Step 4: Click or tap here to enter text.	☐ Collection ☐ Use ☐ Disclosure	Click or tap here to enter text.	Click or tap here to enter text.
Step 5: Click or tap here to enter text.	☐ Collection ☐ Use ☐ Disclosure	Click or tap here to enter text.	Click or tap here to enter text.
Step 6: Click or tap here to enter text.	☐ Collection ☐ Use ☐ Disclosure	Click or tap here to enter text.	Click or tap here to enter text.
Step 7: Click or tap here to enter text.	☐ Collection ☐ Use ☐ Disclosure	Click or tap here to enter text.	Click or tap here to enter text.

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.
Click or tap here to enter text.

2.2 Collection Notice

Click or tap here to enter text.

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.

3.1 Is any personal information stored outside of Canada?

☐ Yes
☐ No

3.2 Does your initiative involve sensitive personal information?

☐ Yes, go to question 3.3
☐ No, go to question 3.4

3.3 Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

☐ Yes, go to Part 4
☐ No, go to question 3.4

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

Click or tap here to enter text.

- After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section ONLY if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

4.1 Is the sensitive personal information stored by a service provider?

☐ Yes, fill in the table below (add more rows if necessary) and go to question 4.3

☐ No, go to question 4.2

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

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

Click or tap here to enter text.

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

☐ No

☐ Yes

- If yes, describe the contractual measures related to your initiative.
  Click or tap here to enter text.

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

Click or tap here to enter text.

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

Click or tap here to enter text.

4.6 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	Level of privacy risk (consider 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, describe.
Click or tap here to enter text.	Click or tap here to enter text.	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	Click or tap here to enter text.	Click or tap here to enter text.

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 4.6. **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.

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

☐ No

☐ Yes

- If yes, complete the Security Checklist below. This checklist will help determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30. If a service provider or vendor is involved in the initiative, have them complete the "Third Party" section of Appendix A.

5.2 What physical security safeguards are in place to protect Personal Information in this initiative? Identify the elements of physical security that protect where the records for your initiative are stored (Check all that apply. Specify, "Other" if applicable)

Safeguard	At CNC	At Third Party
Restricted access to property (i.e. key card access)		☐
Security monitored building		☐
Locked doors		☐
Locked filing cabinets		☐
Chain of custody process		☐
"Clean desk" practices		☐
Other (describe)		☐

What technical security safeguards are in place to protect Personal Information in this initiative? Describe the elements of technical security that protect where the records for your initiative are stored (e.g. secure passwords, encryption, firewalls, etc.)

Safeguard	At CNC	At Third Party
Authentication control: Strong Password Management		☐
Authentication control: Multi Factor Authentication ("MFA")		☐
Role-based access		☐
Encrypted in transit		☐
Encrypted at rest		☐
Isolation Control: Application		☐
Isolation Control: Network		☐
Isolation Control: Database		☐
Vulnerability Scan		☐
Vulnerability Penetration Testing		☐
Configuration Management		☐
Patch Management		☐
Technical control: Perimeter firewalls		☐
Technical control: Web application firewalls		☐
Technical control: Distributed denial of service		☐
Technical control: Intrusion prevention systems to control traffic flow		☐

What administrative safeguards are in place to protect Personal Information? Describe the elements of administrative security that protect where the records for your initiative are stored (e.g. aliasing, aggregation, policies/procedures, standards of practice, etc.)

Safeguard	At CNC	At Third Party
Agreement/contract		☐
Privacy/data protection policy		☐
Documented business practices and processes for proper collection and management of Personal Information		☐
Privacy training specific to the initiative		☐
Staff security awareness training		☐
Dedicated information security staffing		☐
Information security policy		☐
Vendor third party compliance and certifications (i.e. ISO, SOC Type 2, CSA)		☐
Role-based access to initiative data and personal information		☐
Audit logs of file access		☐
Security incident response plan		☐

5.3 Controlling and tracking access

Describe any additional strategies used to control and track access, if not indicated above.

Click or tap here to enter text.

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.

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

Click or tap here to enter text.

6.2 Requests for correction

FOIPPA 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.

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

☐ Yes
☐ No

6.2.2 Sometimes it's not possible to correct the personal information. FOIPPA 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
☒ N/A

6.2.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA 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
☒ N/A

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

☐ Yes, go to 6.4
☒ No, proceed to part 7

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

FOIPPA 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.
  Click or tap here to enter text.

PART 7: AGREEMENTS AND INFORMATION BANKS

Provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank. If your initiative includes or will be part of a regular and systematic exchange of personal information with partners in or outside of government, you may require an information sharing agreement (ISA).

7.1 Does your initiative involve an information sharing agreement?

☒ No

☐ Yes

- If yes, complete the Information Sharing Agreement Supplement below and attach the ISA to this PIA.

Description of ISA: Click or tap here to enter text.
Name of main ministry or agency involved: Click or tap here to enter text.
Any other departments, public bodies, or organizations involved: Click or tap here to enter text.
Business contact title and phone number for person responsible for maintaining the ISA: Click or tap here to enter text.
ISA start date: Click or tap here to enter text.
ISA end date: Click or tap here to enter text.

7.2 Will your initiative result in a personal information bank?

☒ No

☐ Yes

- If yes, complete the table below.

Describe the type of information in the bank: Click or tap here to enter text.
Name of main department involved: Click or tap here to enter text.
Any other ministries, agencies, public bodies or organizations involved: Click or tap here to enter text.
Business contact title and phone number for person responsible for managing the PIB: Click or tap here to enter text.

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.

8.1 Risk Response

Possible risk	Mitigation strategies
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.

PART 9: 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 department or program area will engage with their Privacy Office and if necessary, complete a PIA update.

Privacy Office Comments:

If the use of LibGuides is expanded in the future to additional modules, another PIA will need to be completed to determine whether personal information will be collected and if so, how it will be protected, used, and disclosed in compliance with FIPPA.

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	Elyse Giddens	Elyse Giddens	June 12 2023

Program Area Signatures

Role	Name	Electronic signature	Date signed
Initiative lead	Ignacio Albarracin	Ignacio Albarracin	June 12, 2023
Initiative Sponsor Usually administrator overseeing implementation	Click or tap here to enter text.		
IT Services Representative Only required if they have been involved in the PIA	Click or tap here to enter text.		