



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our [PIA Guidelines](#) for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?

Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

3

Part 1 – General

Name of Institution:	Northern Lights College		
PIA Drafter:	[REDACTED]		
Email:	[REDACTED]	Phone:	[REDACTED]
PIA Reviewer:	[REDACTED]		
Email:	[REDACTED]	Phone:	[REDACTED]
Program Manager:	[REDACTED]		
Email:	[REDACTED]	Phone:	[REDACTED]
Privacy Officer:	[REDACTED]		
Email:	[REDACTED]	Phone:	[REDACTED]

1. Description of the Initiative

Northern Lights College has recently launched an Alumni program at NLC and we are looking to implement a platform where we can engage with past alumni and collect their information to share opportunities available at Northern Lights College.



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

The initiative involves the implementation of Almadase, a cloud-based alumni and donor management platform, to centralize and manage information for alumni engagement and donor relations. Almadase will serve as the institution's primary platform for managing alumni and donor records, tracking fundraising efforts, organizing events, and fostering stronger relationships with the alumni community. This platform will enable the institution to:

- Collect and maintain up-to-date alumni and donor information.
- Streamline event registration and participation management.
- Track and manage financial contributions and donor engagement history.
- Provide a secure, centralized system for all alumni and donor data.
- Support outreach through personalized email campaigns and engagement reports.

The implementation aims to enhance operational efficiency, improve alumni and donor engagement, and increase transparency in data management practices.

2. Scope of this PIA

This Privacy Impact Assessment (PIA) evaluates the privacy implications of implementing **Almadase** as Northern Lights College's alumni and donor management platform. The scope includes the following key areas:

1. Initial Implementation:

- Assessing the suitability of Almadase for collecting, managing, and storing personal information in compliance with the Freedom of Information and Protection of Privacy Act (FOIPPA) of British Columbia.
- Reviewing contractual obligations between Northern Lights College and Almadase as a third-party vendor, including data hosting on **Microsoft Azure's Canada-based data centers**.

2. Ongoing Use and Management:

- Examining how staff will use Almadase to engage with alumni and manage donor relations, including event management and fundraising activities.
- Ensuring proper implementation of access controls, role-based permissions, and audit logging to align with privacy and security best practices.

3. Data Storage and Sovereignty:



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

- *Confirming that all personal information is stored within Canada using Microsoft Azure's Canadian infrastructure.*
- *Evaluating measures to mitigate risks related to data breaches, unauthorized access, and compliance with FOIPPA's data sovereignty requirements.*

4. **Stakeholder Transparency:**

- *Developing clear processes to inform alumni and donors about the collection, use, and disclosure of their personal information.*
- *Providing appropriate **privacy notices** and obtaining consent where necessary to ensure compliance and transparency.*

5. **Privacy Risk Mitigation:**

- *Identifying potential privacy risks associated with the platform and implementing appropriate safeguards to reduce risks to an acceptable level.*
- *Addressing areas such as unauthorized access, data transfer, and security breaches to ensure personal information remains secure.*

3. **Related Privacy Impact Assessments**

Not applicable

4. **Elements of Information or Data**

The personal information elements collected, stored, and processed through Almadase include:

Alumni Information:

- *Full name*
- *Contact information (email, phone number, mailing address)*
- *Graduation details (year of graduation, degree, program of study)*
- *Employment details (current employer, job title, industry, city)*
- *Engagement records (events attended, email campaigns opened, communications sent)*

Donor Information:

- *Donation history (amount, date, purpose of donation)*



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

-
- *Payment details (type of payment, transaction reference)*
 - *Tax receipt information*
 - *Pledge history (amount pledged, timeline)*

Event Information:

- *Registration details (name, contact information, event preferences)*
- *Attendance records*
- *Surveys and feedback provided by attendees*

Platform Usage Data (optional):

- *User activity logs (frequency of engagement with emails or platform tools)*
- *Campaign response data (opened emails, clicked links)*

The collection, use, and disclosure of these data elements will comply with FOIPPA and will be guided by the institution's internal privacy policies and agreements with Almadase.

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.



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[]

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Almabase hosts all data for its Canadian partners exclusively on [REDACTED] Canada-based data centers. No production, development, or test data is stored outside Canada. [REDACTED]

[REDACTED] Measures implemented to ensure compliance with FOIPPA Section 33.1 include:

- Encrypted data storage and transmission to protect personal information at rest and in transit.
- Regular audits of Microsoft Azure to verify adherence to Canadian privacy and security standards.
- Contractual obligations that require Almabase to notify Northern Lights College in the event of any data breach or unauthorized access.

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;	Yes
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.	



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

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.



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Email received from client requesting service	Collection	26(c)
2.	Email client back requesting more information	Disclosure	33.1(7)
3.	Service request transferred to service provider contracted by public body	Disclosure & Use	33.2(c) and 32(a)

9. Risk Mitigation Table

Risk Mitigation Table					
	Risk	Mitigation Strategy	Likelihood	Impact	
1.	Employees could access alumni personal information and use or disclose it for personal purposes	Oath of Contract; contractual terms, very limited access with high degree of access logging.	Low	High	
2.	Request may not actually be from client (i.e. their email address may be compromised)	Data will only be available through [REDACTED] [REDACTED] [REDACTED]	Low	High	
3.	Client's personal information is compromised when transferred to the service provider	[REDACTED] [REDACTED] [REDACTED] [REDACTED]	Low	High	

10. Collection Notice

For initiatives that involve collecting personal information directly from individuals, the following information will be provided as part of the collection notice:

1. Purpose:

Personal information is being collected to manage alumni relations, donor stewardship, and engagement activities, including event registrations and fundraising campaigns.

2. Legal Authority:

Personal information is collected under Section 26(c) of the **Freedom of Information and Protection of Privacy Act (FOIPPA)** of British Columbia.



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

3. **Contact Information:**

For questions regarding the collection, use, or disclosure of personal information, individuals may contact:

- **Name:** [REDACTED]
- **Title:** Chief Information Officer
- **Business Address:** Northern Lights College, 11401 8th St, Dawson Creek, BC V1G 4G2
- **Business Telephone Number:** [REDACTED]

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).

Almabase data is hosted on Microsoft Azure's Canada-based data centers, which employ industry-standard physical security measures, including:

- *24/7 on-site security personnel.*
- *Biometric access controls and key card entry for restricted areas.*
- *Surveillance systems with cameras covering critical areas.*
- *Regular security audits and facility monitoring.*

For more on Azure's physical security, please visit <https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security>

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

- **Encryption:** All data is encrypted both at rest and in transit using strong encryption protocols [REDACTED]
- **Access Management:** Multi-factor authentication (MFA) is enforced for all users accessing the system.



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

- **Firewall Protection:** Advanced firewall solutions and intrusion detection systems are in place to prevent unauthorized access.
- **System Updates:** Regular software updates and patches are applied to mitigate vulnerabilities.
- **Data Backups:** Automated and encrypted backups ensure data recovery in case of system failure or data breach.

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

The institution relies on its **IT Acceptable Use Policy**, which outlines expectations for the appropriate use of IT systems, data protection requirements, and penalties for policy violations.

[IT Acceptable Use Policy](#)

Key highlights from the policy relevant to this initiative include:

- Restricted access to sensitive systems and data.
- Obligations to protect institutional data from unauthorized use.
- Procedures for reporting and responding to security breaches.

Any questions regarding security policies should be directed to [REDACTED] CIO.

[REDACTED]

[REDACTED]

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.

- **Role-Based Access Control (RBAC):** Access to Almadabase is restricted based on user roles, ensuring employees only access data necessary for their job functions.
- **Audit Logs:** All additions, deletions, and modifications of personal information are logged for accountability.
- **Approval Processes:** Changes to critical data require management approval.
- **Deactivation Protocols:** Accounts for employees who leave the organization or change roles are promptly deactivated to prevent unauthorized access.

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

- **Access Logs:** Almadabase maintains detailed logs of user activity, including access to personal information, which are reviewed regularly.



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

- **Periodic Audits:** IT staff conduct periodic audits to verify that access permissions align with current job responsibilities.
- **Automated Notifications:** The system generates alerts for unusual activity or unauthorized access attempts.
- **Access Requests:** Any requests for new or expanded access are documented and subject to approval by management and IT.

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?

Individual information is updated through a [REDACTED]
[REDACTED] If updates or corrections are not feasible (e.g., due to technical or procedural limitations), the information will be annotated in the system to reflect its inaccuracy.

When personal information is disclosed to others (e.g., external partners or government agencies), the public body will notify these entities of any updates, corrections, or annotations to ensure data consistency and integrity.

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

Yes. The personal information collected will be used to make informed decisions about alumni engagement strategies. This includes tailoring communication, identifying opportunities for collaboration, and fostering relationships that benefit both alumni and the institution.

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.

To maintain accuracy and completeness:

- [REDACTED]
- Information will be cross-referenced with records from the Student Information System (SIS).
- If necessary, information will also be verified with data from other government agencies, in compliance with applicable privacy laws.



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

- Regular audits and validation processes will be conducted to identify and address any discrepancies.

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?

Yes. The institution adheres to the **Northern Lights College (NLC) Records Management and Retention Policy**, which ensures personal information is retained **for at least one year after it is used in decision-making processes**. This policy aligns with the requirements of the **Freedom of Information and Protection of Privacy Act (FOIPPA)** and institutional best practices for records management.

Part 5 – Further Information

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

No. This initiative does not involve systematic disclosures of personal information to third parties. All disclosures, if any, will be handled on a case-by-case basis and will comply with the requirements of the **Freedom of Information and Protection of Privacy Act (FOIPPA)**.

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. The program does not involve the use of personally identifiable information for research or statistical purposes. The primary purpose of the initiative is to manage alumni engagement and donor relations.

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).

☐



Privacy Impact Assessment for Non-Ministry Public Bodies

[ALMABASE]

PIA#[/]

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.

Yes. A Personal Information Bank (PIB) will result from this initiative to store and manage alumni and donor information. The PIB will include the following legislatively required descriptors as per Section 69(6) of FOIPPA:

- 1. **Name of the bank:** Alumni and Donor Management Database.*
- 2. **Location of the bank:** Microsoft Azure Canada-based data centers.*
- 3. **Legal authority for collection:** FOIPPA Section 26(c).*
- 4. **Types of personal information stored:** Name, contact details, donation history, event participation, engagement activities, and other relevant alumni records.*
- 5. **Purpose of the bank:** To support alumni engagement, donor relations, event management, and fundraising activities.*
- 6. **Categories of individuals whose information is included:** Alumni, donors, and affiliated stakeholders.*
- 7. **Use and disclosure of information:** Used internally by authorized staff for alumni and donor engagement; disclosures are limited and compliant with FOIPPA.*

This information will be published in a public directory as required by law.

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