



Privacy Impact Assessment for:

Canadian Letters & Images Project

Initiative:	Past Perfect for Canadian Letters and Images Project (CLIP)
Department or Service Area Name:	History

Part 1 – General Information and Overview	2
Part 2 – Collection, Use, and Disclosure	5
Part 3: Storing Personal Information.....	11
Part 4: Assessment for Disclosures of Sensitive Personal Information	11
Part 5: Security of Personal Information	12
Part 6: Accuracy/Correction/Retention of Personal Information	14
Part 7 – Personal Information Banks.....	15
Part 8 – Further Information.....	16
Part 9 – Summary and Proponent Responsibility	16
Part 10: Signatures.....	17

Canadian Letters & Images Project

Part 1 – General Information and Overview

1.1 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.

For over twenty years the Canadian Letters & Images Project (CLIP) has worked to digitize and publish (online at <https://www.canadianletters.ca>) the wartime correspondence, photographs, and related memorabilia of individual Canadians. Over one thousand collections have been donated, to be scanned, transcribed, and posted on the project's website. Collections are borrowed, not permanently acquired, and are returned once they have been digitized, allowing donors to share their family legacies while still retaining ownership. CLIP was founded as an individual initiative by Dr. Stephen Davies, History Professor, VIU, and has operated solely under his administration as Project Director. VIU has provided IT support through hosting and maintaining of the project's website, and through yearly funding a number of student work-op positions to assist with archival material processing (e.g., scanning, transcription). For the past few years funding has been available through various sources for a full-time Collections Manager position. The project's offline digital archival files reside on VIU's servers, organized so that each collection has its own main file folder with all files for that collection stored in that folder. VIU's IT department provides CLIP with two distinct drives on the server. Access to the main drive is restricted to the Project Director and and Collections Manager only; there is a second "WorkingFiles" drive that work-op students are granted access to to work on specific collection files as needed. CLIP has been granted funding to purchase museum collection management software. The program we will be installing, PastPerfect 5.0 (<https://museumsoftware.com>), is one of the most widely used programs in the industry. First released in 1998, it has a solid reputation for functionality, stability, and client support. The PastPerfect software will be installed by VIU's IT department. Its implementation will not change where the project's files are located; it is to be used in an organizational capacity and as such the project will continue to hold the same data within the same hardware framework, but with the improved functionality of a collection management-specific software environment.

1.2. 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?

Canadian Letters & Images Project

This PIA is a requirement for the acquisition of PastPerfect Museum Management Software by the Canadian Letters & Images Project.

1.3. Are there any related Privacy Impact Assessments?

Please indicate if this an update on an existing PIA or an additional module that was not covered in the original PIA.

CLIP has no pre-existing PIAs.

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

In the table below, 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 an appendix.

Information Type	Information Collected
Personal Information	<p>From Students: As required by VIU’s HR department for work-op employment purposes.</p> <p>From Third Parties: Genealogical-type personal information is often provided by collection donors in email correspondence during the donation process. This often includes biographical details such as how they are related to the creator of the materials, or help in identifying names in correspondence (e.g. letters written by the donor’s grandfather to “Jenny” were to Jennifer Smith, who later became their future grandmother).</p> <p>From VIU Employees: As required by VIU’s HR department for employment purposes.</p>
Contact details	<p>From Students: As required by VIU’s HR department for work-op employment purposes.</p> <p>From Third Parties: Donor contact information is stored with the collection files, and generally includes their full mailing address, email address, and phone number.</p> <p>From VIU Employees: As required by VIU’s HR department for employment purposes.</p>
Account information: what info is required to set up an account?	Accounts allowing students to access to the “WorkingFiles” drive, and employee access to the main collections drive is managed by VIU’s IT department.
Commercial information	n/a

Canadian Letters & Images Project

1.4a. Did you list [personal information](#) in question 1.4?

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- see the table below for examples of Personal Information.

Business contact information, in turn, is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, as well as business telephone number, address, email or fax number of the individual. BC FIPPA does not protect business contact information.

Examples of Personal Information

- | | |
|--|---|
| <ul style="list-style-type: none"> • Name, age, sex, weight, height • Home address, phone number • Race, ethnic origin, sexual orientation • Medical information • Health history • Number or symbol assigned to the individual • Income, purchases and spending habits • Blood type, DNA code, fingerprints | <ul style="list-style-type: none"> • Marital or family status • Religion • Education • Financial information • Criminal information • Employment information • Personal views or opinions, except if they are about someone else |
|--|---|

- If yes, go to [Part 2](#)
- If no, answer question 1.5 and submit questions 1 to 1.5 to pia@viu.ca. You do not need to complete the rest of the PIA template.

Click or tap here to enter text.

1.5. How will you reduce the risk of unintentionally collecting or disclosing personal information?

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

Click or tap here to enter text.



Canadian Letters & Images Project

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 Four point “Necessity Test” for the collection, use, and disclosure of Personal Information.

To determine if the Personal Information from your initiative meets the necessity threshold, apply the following four-point test to each element of PI from 1.4 above. Note that each element of PI must meet all four points of the test.

Four point “necessity test” for collecting personal information ([OIPC Canada, 2016](#)).

1. The information is rationally connected and demonstrably necessary to an operating program or activity
2. The information is likely to be effective in meeting the objectives of the program or activity
3. There are no other less privacy-invasive ways to effectively achieve the objectives of the program or activity
4. The loss of privacy is proportional to the objectives of the program or activity

Personal Information element	Does it meet all four points of the necessity threshold?	Reasons for keeping or excluding from initiative
<ul style="list-style-type: none">• Name, age, sex, weight, height• Marital or family status	yes	Name is the only one of these elements purposefully collected by the project (e.g. needed in arranging Purolator pickup of a collection). Age, sex, and marital status are never requested by us but are often knowingly disclosed by the donor in correspondence (e.g. if a WWII letter collection was created by someone’s father, it’s not hard to make a reasonable guess at their age.)

Canadian Letters & Images Project

<ul style="list-style-type: none"> • Home address, phone number 	yes	Usually required for shipping purposes, and for follow-up questions that may arise during processing.
<ul style="list-style-type: none"> • Race, ethnic origin, sexual orientation • Religion 	yes	Uncommon and never solicited by us, but may rarely be purposely disclosed by the donor if they believe it is important to the context or content of the collection (e.g. materials include a picture of a memorial plaque recently placed by the family in their local church).
<ul style="list-style-type: none"> • Medical information • Health history • Number or symbol assigned to the individual • Income, purchases and spending habits • Blood type, DNA code, fingerprints • Financial information • Criminal information • Employment information • Personal views or opinions, except if they are about someone else 	n/a	n/a

2.2 Does your initiative involve the use of Artificial Intelligence (AI)? If so, please fill out Appendix One: GenAI Analysis Questions
No.

Canadian Letters & Images Project

2.3 Personal Information Flow Diagram and/or Personal Information Flow Table

In the table below, list the personal information from question 1.4. Think about how each element of information flows through your project. Your Privacy Officer can help you figure out whether each step is a collection, use, or disclosure, and whether you have the legal authority for the way you're working with the information. Alternatively, you can attach a flow diagram to this PIA. Add rows as necessary.

	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 or other legal authority
	Donor contact information and other possible donor-provided personal information	<i>Collection</i>	<i>FIPPA 26(c) "info relates to and is necessary for a program or activity"</i>
1.	Donors contact CLIP through the project's VIU hosted email to enquire about donating materials. In a very small number of cases, first contact may be by VIU-hosted phone, which is then followed-up by email correspondence. The email account is accessible by Project Director Stephen Davies only. Most donations involve a number of emails back and forth with donors, with questions about the collection's contents (what types of materials? how many? what war?). Some donors may be able to drop off a collection in person, but in most cases shipping information (mailing address) is needed. Emails are sent to confirm materials have arrived at VIU, and to confirm receipt once they have been shipped back. Donors are often contacted once the collection has been posted to let them know it is up on website.	Collection & Use	<i>FIPPA 26(c) "info relates to and is necessary for a program or activity"</i>
2.	Emails are retained (within the VIU email account system) by Stephen Davies. There is often a time delay, sometimes stretching to many years, between a collection's initial intake and scanning, and its final processing and posting	Use	<i>FIPPA 26(c) "info relates to and is necessary for a program or activity"</i>



Canadian Letters & Images Project

	<p>online. Donor’s emails may need to be referenced during final processing to help understand material content, e.g. if letters seem to be signed “Glenn” but the soldier’s service record spells his name as “Glen” it can be helpful to check which spelling the donor may have used.</p> <p>Excerpts from donor emails which include contact information and important collection-related information (e.g. letter’s authors and recipients and the relationships between them (son/mother? brother/sister?)) are copied to a <i>Donor-Info.docx</i> file. This donor document is create for every new collection, and is stored in the collections main digital file folder. Main collection folders are stored on the projects main data drive, which is accessible to senior administrative staff only (currently the Project Director and Collections Manager).</p>		
3.	<p>CLIP occasionally receives requests from external individuals, e.g. academic researchers, asking for donor contact information. The project never ever releases donor contact information, but we will generally pass the request along to the donor so that they may initiate contact if they choose to (e.g. we were contacted in 2023 by Veterans Affairs, who were hoping to ask the donor of the Alexander White collection if they would consider lending White’s physical journal to be part of an upcoming exhibition at the Vimy Visitor Education Centre in Vimy, France. CLIP passed the request to the donor, who very happily got in touch with Veterans Affairs to make arrangements for the journals voyage to Vimy.)</p>	Use	<i>FIPPA 26(c) “info relates to and is necessary for a program or activity”</i>
4.			
5.			

Canadian Letters & Images Project

6.			
----	--	--	--

2.4 Risk Mitigation Table

Thinking through the information flow, identify where there are risks for privacy incidents or data breaches. For each risk, identify a mitigation strategy, as well as the likelihood of an incident, and level of impact or harm if people's information were breached.

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact/harm
1	Unauthorized access to the Donor-Info files stored on the main project drive.	Work with IT to periodically ensure the list of who has access to this drive is correct.	Low	Almost all the donor information CLIP holds is already publicly available. The personal information shared with is often already being shared publicly by donors elsewhere, e.g. on genealogy websites. (Donors are often a bit disappointed with our policy that we don't identifying information with the donated collection.)
2				



Privacy Impact Assessment for:

Canadian Letters & Images Project

3				
4				
5				

2.5. Collection or Privacy Notice

If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice, also known as a privacy notification.

A collection notice must contain the following elements:

- The legal authority and section under FIPPA under which you are collecting personal information.
- The purpose for which you are collecting the personal information and how it will be used.
- The contact information of an employee or officer at VIU who can answer questions about the collection of personal information.

Contact the privacy office for a collection/privacy notice template.

If applicable, paste your privacy notice here.

Canadian Letters & Images Project

Part 3: Storing Personal Information

3.1. Is any personal information being stored outside of Canada?

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

Click or tap here to enter text.

No

3.1.1. Where is the personal information stored?

Click or tap here to enter text.

3.2. Does your initiative involve sensitive personal information?

Examples of sensitive personal information include personal health information, genetic and biometric data, personal finances, geolocation data, criminal records, counselling records, HR records, payroll records, racial or ethnic origin, sexual orientation, religious, philosophical, or political beliefs, etc.

NO

If **yes**, please complete [Part 4: Assessment for Disclosures of Sensitive Personal Information](#).

If **no**, skip to [Part 5: Security of Personal Information](#)

Part 4: Assessment for Disclosures of Sensitive Personal Information

Complete this section if you are disclosing sensitive personal information. You may need help from your organization's Privacy Officer.

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

Click or tap here to enter text.

Canadian Letters & Images Project

If yes, fill out the table below, then go to question 4.3. If no, continue to [question 5](#).

Information about Service Provider

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

4.2. Provide details on the disclosure, including where and how the personal information is stored.

Answer this if question 4.1 does not apply. Be specific about where and how the information is being stored.

4.3. Is there a contract that includes privacy-related terms?

If there is a contract with the provider, please describe any privacy-related terms in the contract, or attach the privacy schedule.

Part 5: Security of Personal Information

Section 30 of FIPPA imposes a duty on the public body to prevent unauthorized access to Personal Information both internally and with any contracted third parties. As such, we need to make sure that personal information is safely secured in both physical and technical environments. **For each item in this section, please describe the security measures for both the service provider and for VIU internally.**

5.1. Please describe the physical security measures related to the initiative (if applicable).

For example, physical security measures may include: the security environment of vendor's data centres; storing records containing PI in locked storage rooms, offices, and/or filing cabinets with controls over distributions of keys/access; locked workstations that do not permit others to view your screen (including when working remotely, etc).

Canadian Letters & Images Project

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

E.g. Encryption standard for data in transit and data at rest; firewalls, strong passwords; MFA; encrypted documents, etc.

Server security managed by VIU IT

5.3 Tracking Access / Access Controls. In this section, you will describe how the unit will minimize the risk of unauthorized access to Personal Information.

5.3.1. FIPPA section 30 requires public bodies to manage access to PI based on the principle of “need to know” – that users may only access information that is necessary to do their job. This is frequently accomplished by assigning role-based access controls (RBAC), and by establishing a security matrix that describes which positions/roles are permitted to access specific types or groups of Personal Information. Access to personal information should only be permitted to those who demonstrate their right of access on the security access chart. **Please describe how access controls work in the department, or with this initiative.**

Personal Information is stored within each collection’s main collection folder on the VIU-managed “Research_CanadianLetters” drive, which is accessible only by senior project staff (currently Project Director Stephen Davis and Collections Manager Margaret Hampshire). It is not accessible by work-op students who have password-protected login access to the physically separate CLIP_WorkingFiles drive only.

5.3.2 How will you know if sensitive personal information is accessed, including access by service providers? This should include a description of what information is available through logs.

VIU IT controls all security related matters.

Canadian Letters & Images Project

5.3.3 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.

Access controls and limitations as described above.

5.4 What controls does the provider have in place to prevent unauthorized access to sensitive personal information?

Describe technical, administrative, and/or policy measures in place to protect PI. If using a cloud-based service provider, include a description of controls in each layer of the stack: software level, platform level, infrastructure level.

Managed by VIU IT.

Part 6: Accuracy/Correction/Retention of Personal Information

[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. In this section, you will demonstrate how you intend to keep personal information on file accurate and complete.

6.1 How is an individual's information updated or corrected?

[FIPPA section 29](#) states that a person can ask you to correct their personal information in your custody or control. If it is not possible to update or correct (for physical, procedural or other reasons) it must be noted on the record. **Please explain how it will be updated or annotated. If personal information will be disclosed to others, how will VIU notify them of the update, correction, or annotation?**

Normally, donor contact info, etc. is entered at the time of collection donation, and is not usually updated or changed. If the individual contacted us with updated information, it would be updated in the donor information Word document in relevant collection's main folder.

6.2. Does your initiative use personal information to make decisions that directly affect an individual(s)?

Canadian Letters & Images Project

No

6.2.1. If you answered “yes” to question 6.2, 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.

Click or tap here to enter text.

6.3. Do you have a records management schedule in place?

How long will you keep the personal information collected? Is there a plan in place for retention and deletion? Please also use this question to note how long it will be stored by the service provider (if applicable).

Information provided by the donor is retained in the collection files as a permanent part of the collection acquisition record.

Part 7 – Personal Information Banks

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

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

No

If yes, please complete the table below:



Privacy Impact Assessment for:

Canadian Letters & Images Project

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 – Further Information

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

No

8.2. Will the information collected be used for research or statistical purposes?

No

Part 9 – Summary and Proponent Responsibility

This section is for Privacy Office recommendations as well as any limitations due to privacy concerns.

There are no privacy concerns with this initiative.



Privacy Impact Assessment for:

Canadian Letters & Images Project

Part 10: 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.

Reviewed by	Privacy Officer
Approved by	History Department
Date:	2025-03-12