Privacy Impact Assessment for Non-Ministry Public Bodies

Career Services Job Board

PIA#*[assigned by your privacy office(r)]*

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.

Part 1 – General

Name of Department/Branch:	Student Services		
PIA Drafter:	Adrian Lim		
Email:	adrianlim@ecuad.ca	Phone:	**604-844-3822**
Program Manager:	**Rachel Armstrong**		
Email:	rachelarmstrong@ecuad.ca	Phone:	**604-630-7424**

In the following questions, delete the descriptive text and replace it with your own.

1. **Description of the Initiative**

   This service will be provided for the Emily Carr University of Art + Design student, alumni, and greater creative communities to share and view opportunities for employment, experiential learning, and exhibitions. The creative community will benefit with this system by notifying, sharing, and learning of creative opportunities. It is a self-service model intended to support recruitment and career development initiatives in the creative community.

2. Scope of this PIA

The PIA should cover the lifespan of the project starting with initialization and carrying through to completion. In particular, this PIA should focus on the accessing of the data stored in Canada by 3rd parties not in Canada.

3. Related Privacy Impact Assessments

n/a

4. Elements of Information or Data

The data elements for users of the software are the following:

Students: Student name, student number, email address, mailing address, telephone number, program major, student status (domestic, permanent resident, international), documents (images, resumes, cover letters).

Employers: Company name, mailing address, telephone number, contact name, contact email, contact telephone number, images.

Opportunity postings: containing descriptions of jobs, opportunities, calls to artists, experiential learning (co-op) positions, volunteer positions.

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.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

The data will be stored within Canada on a cloud service, and will be accessed by service providers for maintenance, troubleshooting, and repair purposes. With consent, the user driven content and information may be accessed by 3rd parties outside of Canada

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;	**no**
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.	

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;	yes
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	yes
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.

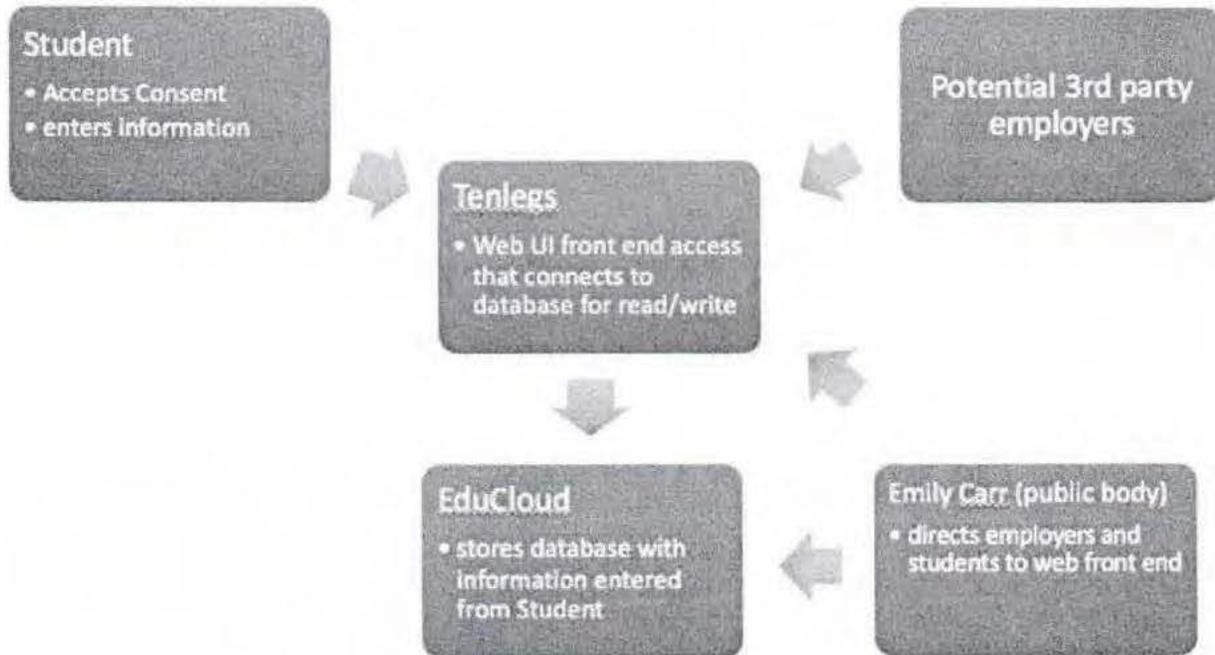8. **Personal Information Flow Diagram and/or Personal Information Flow Table**

   Please provide a diagram and/or table that shows how your initiative will collect, use, and/or disclose personal information (see examples below). Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. It should also outline the flows of personal information wherever it is transmitted or exchanged.

Student
- Accepts Consent
- enters information

Potential 3rd party employers

Tenlegs
- Web UI front end access that connects to database for read/write

EduCloud
- stores database with information entered from Student

Emily Carr (public body)
- directs employers and students to web front end

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Student Accepts consent that information may be accessed by 3rd parties	Disclosure/Consent	33.1
2.	Student Fills in information, submits	Collection	26(c)
3.	Service request transferred to service provider web front end	Disclosure & Use	33.2(c) and 32(a)
4.	Database remains in Canada owned and maintained by Emily Carr, but not accessed.	Disclosure and Use	32

9. **Risk Mitigation Table**

Risk Mitigation Table			
Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1. *Employees could access personal information and use or disclose it for personal purposes*	*Oath of Employment; contractual terms, etc.*	*Low*	*High*
2. *Request may not actually be from client (i.e. their email address may be compromised)*	*Implementation of identification verification procedures*	*Low*	*High*
3. *Client's personal information is compromised when transferred to the service provider*	*Transmission is encrypted and over a secure line*	*Low*	*High*
4. *Inherent risks in sending personal information to a client via email*	*Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail*	*Medium*	*Medium*

10. **Collection Notice**

The information collected for this service will be stored by Emily Carr University of Art + Design within Canada, under Section 26 of the Part 3 – Protection of Privacy – Division 1 – Collection, Protection and Retention of Personal Information by Public Bodies of the Privacy Act. Information uploaded by job seekers intended to be viewed by prospective employers will be shared with external parties for employment consideration. Should you have further questions relating to the collection or storage of information, please contact careerservices@ecuad.ca

Part 3 – Security of Personal Information

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

Key card access to building, security personnel, locked offices, password protected computers, password protected software system.

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

Firewalls, authenticated access

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

   Please contact Adrian Tees at adriantees@ecuad.ca

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.

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

   Information is organized into profiles, profiles are logged and view/access are tracked.

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?

   Users have access to update their own information and notes will be made by role-based accessors to individual user files.

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

   Yes. Student status (work authorization, program information), will determine eligibility for access to data points such as postings for the experiential learning program.

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.

   User entered data will be cross-checked with the student information system manually by role-based accessors.

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. Paper files of students participating in the experiential learning program are kept in a locked cabinet in a keyed office with security personnel for 7 years.

Part 5 – Further Information

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

   Only in extreme situations when requested by authorities.

   > ***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.

   > ***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).***

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. Role-based accessors will retrieve student user data via data points such as academic program information and work authorization.

   Employer users will access application documents containing personal information from Emily Carr students and alumni users.

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

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Privacy Officer/Privacy Office Representative	Signature	Date

BRITISH
COLUMBIA

Part 7 – Program Area Signatures

Rachel Armstrong

Program/Department Manager
    Signature
    Sept 28, 2016
    Date

Adrian Lim

Contact Responsible for Systems
Maintenance and/or Security
(Signature not required unless they
have been involved in this PIA.)
    Signature
    Sept.28/2016.
    Date

Head of Public Body, or designate
    Signature
    9/26/2016
    Date

AVP, HR
Chief Privacy Officer

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.