Privacy Impact Assessment
Emily Carr University of Art + Design
Graduway Platform for Alumni
PIA#2020-01

<div style="background:magenta">

Part 1 – General

</div>

Name of Department/Branch	University Advancement + Alumni Relations		
PIA Drafter:	Sára Molčan		
Email:	smolcan@ecuad.ca	**Phone:**	604-844-3870
Program Manager:	Chantale Lavoie		
Email:	clavoie@ecuad.ca	**Phone:**	604-844-3078

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

1. **Description of the Initiative**

   University Advancement and Alumni relations are looking to implement Graduway, a company that offers professional and social opportunities through an Emily Carr University branded alumni networking platform, available on both the web and mobile apps (iOS and Android). It provides us with a dynamic directory, interactive job board, events system, groups for faculties and allows us to locate lost alumni.

   Once the platform (called "The Leeway" at ECU) is live, Advancement will notify alumni to sign up for the platform. Users can access Graduway through the web, on desktop or mobile devices. Data is stored on Graduway's cloud database, with servers located within Canada.

   Users are responsible for providing and updating their personal information associated with their profile on the platform, adjust the privacy setting associated with their profile, and are able to view/connect with other alumni profiles.

   In signing the contract with Graduway, Graduway becomes a service provider under FIPPA.

   Graduway integrates with the university's fundraising database, Raiser's Edge, which allows Raiser's Edge to populate donor profiles with information from Graduway. Users consent to this use of their information when they agree to the terms and conditions upon signing up.

   The platform's terms of use can be found here: https://theleeway.ca/terms-of-use
   The platform's privacy policy can be found here: https://theleeway.ca/privacy-policy

2. Scope of this PIA

The platform provides a way to populate our internal alumni database, Raiser's Edge, with data provided by alumni during registration and when they change their profiles. It is moved through a secure server. The PIA covers the transition to and use of the Graduway platform.

3. Related Privacy Impact Assessments

N/A

4. Elements of Information or Data

The personal information collected by Graduway will largely depend on what the user chooses to disclose. Data could include alumni name, age, address, work/home email, work/home phone number, educational history, employment history, work status, photos, donation history, participation in events, and/or social/web URLs.

> 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

Graduway will store ECU data on Canadian servers as per the contractual agreement.

6. Data-linking Initiative*

In FIPPA, "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 the privacy office(r) at privacy@ecuad.ca to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FIPPA, "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.	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 privacy@ecuad.ca 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 the privacy office(r) to determine how to proceed with this notification.

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

Info: In the following table, 'user' refers to staff, faculty or alumni that register. There are separate entries for student users.

Personal Information Flow Table			
	Description/Purpose	Type	FIPPA Authority
1.	User signs up via social network or email	Collection	26(c), 26(d)
2.	User answers registration questions	Collection	26(d)
3.	User populates profile or updates profile	Collection	26(d)
4.	User information is used to match mentorship	Use	32(a), 32(b)
5.	User information is used to match jobs	Use	32(a), 32(b)
6.	User information is transferred to Raiser's Edge	Use	32(a), 32(b)
7.	User information is used to update mailing list	Use	32(a), 32(b)
8.	User uploads images	Collection	26(d)
9.	Student user signs up via social network or email	Collection	26(c), 26(d)
10.	Student user answers registration questions	Collection	26(d)
11.	Student user populates or updates profile	Collection	26(d)
12.	Student user information used to match mentorship	Use	32(a), 32(b)
13.	Student user information used to match jobs	Use	32(a), 32(b)
14.	Student information uploaded to RE only upon graduation and receiving alumni status	Use	32(a), 32(b)
15.	User or student user has trouble updating their profile and emails alumni relations to update it for them, providing explicit consent	Collection, Use	26(d), 32(b)

16.	User or student user requests to have their profile deleted manually	Use	32(b)
17.	User information is used to update alumni mailing lists	Collection, Use	26(c), 26(d), 32(a), 32(b)
18.	User information is used to updated advancement mailing lists	Collection, Use	26(c), 26(d), 32(a), 32(b)
19.	User or student user applies for job or creative opportunity	Use	32(a)
20.	User or student user connects with mentor/mentee	Use	32(a)

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	Code of conduct; contractual terms	Low	Med
2.	Request may not actually be from client (i.e. their email address may be compromised)	Implementation of identification verification procedures	Low	Med
3.	User's personal information is compromised when transferred to the service provider	Transmission is encrypted and over a secure line	Low	Med
4.	Inherent risks in sending personal information to a user via email	Policy developed to inform users of risk and ask if they would like the information via a different medium, such as through the mail	Medium	Medium
5.	Personal information could be inadvertently disclosed via email	Procedure developed to ensure personal information is only discussed with the party who it involves (see 2)	Low	Med

6.	Unauthorized individuals gain access to the system	Procedure regarding verification of authorized status	Low	Med
7.	System includes incorrect or inaccurate personal information	Users are responsible for inputting their own personal information	Medium	Low
8.	Unauthorized employees can access and use personal information.	There are only five administrator seats. Employees are welcome to join the platform as users. Departments that will have access to the platform at an administrative level are Advancement, Alumni Relations, and CD+WIL. Policy for protecting login information will be developed.	Low	Med
9.	Service provider privacy breach	Graduway has agreed in the Service Agreement to inform us immediately of any breach on their end. A breach mitigation strategy will be developed with the Privacy office.	Low	High
10.	Non-compliance with FIPPA privacy notification requirement	All users automatically receive a privacy notification detailing the collection, use and disclosure of their personal information on Graduway prior to creating an account. Users consent to the Graduway Terms of Use when they sign up for the account.	Low	Low

10. Collection Notice

The following collection notice will appear as part of the opt-in on the first page of registration, appearing as "Additional Terms of Use and Privacy Policy":

Graduway ("The Leeway") is a networking platform available to the Emily Carr University community of alumni, faculty, staff and students for the purposes of connecting with other users,

networking, and supporting university programs and activities, including but not limited to fundraising, fostering alumni engagement, updating Advancement mailing lists, and updating donor databases. The personal information you provide upon signing up and creating a profile (e.g., your name, contact information, education and employment history) is collected under the *Freedom of Information and Protection of Privacy Act* sections 26(c) and 26(d). By signing up and using the platform, you are consenting to the collection, use, and disclosure of your personal information as described in this Privacy Notice and in the Graduway Terms of Use and Privacy Policy.

If you have any questions about the collection, use and disclosure of your personal information, please contact [contact email].

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 IT Services 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).**

Only authorized users are to receive equipment or access to systems. Appropriate protection measures are to include but not be limited to (as per Graduway's security policy):

5.2. Restricting physical access to systems to authorized personnel only.

5.3. Securing systems and equipment (such as workstations with screen lock or logout) prior to leaving the area, to prevent unauthorized access.

5.4. Enabling a password-protected screensaver with a short timeout period to ensure that workstations that were left unsecured are kept protected.

5.5. Complying with all applicable password security policies and other policies, as set out herein.

5.6. Ensuring systems are used for authorized business purposes only.

5.7. Preventing the installation of unauthorized software on the systems.

5.8. Keeping food and drink away from equipment to avoid accidental spills and damage.

5.9. Securing equipment that contains sensitive information by using cable locks or locking laptops in drawers or cabinets.

5.10. Where possible, enabling portable equipment encryption.

5.11. Complying with the Anti-Virus policy set out herein.

5.12. Ensuring that monitors are positioned away from public view, if necessary, by installing privacy screen filters or other physical barriers to prevent public viewing.

5.13. Ensuring workstations can receive updates (for example, remaining powered up but logged off to facilitate after-hours updates, running exited applications, opening closed documents etc.).

5.14. Ensuring that all systems use a surge protector or have a robust UPS.

5.15. If a wireless network access is used, ensuring access is secure as set out herein in this policy.

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

All data is protected and encrypted. Please see Graduway's information security policy:
https://drive.google.com/file/d/1N_Ielgfw__Wv-6raDppqwcvtX-2YJoH4/view

Graduway's Ecryption Policy can be found here: https://drive.google.com/file/d/1lirmpSd-wYeRDsHTvatLpHCiZAWQYkv8/view

From the Encryption Policy: "Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Key lengths must be at least 128 bits. Graduway's key length requirements will be reviewed annually and upgraded as technology allows."

Graduway's Network and Server Security Policy can be found here:
https://drive.google.com/file/d/14rixPPTcNEH7zbqsX6DpAHPhwXTfLLvc/view

The Network and Server Security Policy requires "Appropriate controls are to be implemented to ensure the security of Graduway's sensitive information while transmitted over any network. These controls are to include network segregation, network connection control and appropriate encryption controls. All connections between Graduway's networks and networks outside of Graduway must pass through appropriate firewall controls."

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

The Advancement department keeps personal information on donors contained within locked filing cabinets, on the share drive, or on Raiser's Edge. Access is limited to the employees within the department. Only 3 people may be logged in to Raiser's Edge at one time.

The university security policies can be found online on the Policies website:
https://www.ecuad.ca/about/leadership-and-governance/policies

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.**

Graduway allows two administrators. This will limit access to the platform and only allow authorized users to make changes, being administrators or the person in question.

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

Log ins will be kept in a password protected file. Only the administrators will have access to this.

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. In the case of a user being unable to edit their profile, an administrator can make changes and notes will be made on a case file.

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

Yes, for the purpose of an appeal. When contact information is updated (ie: email), it will affect the annual appeal made to alumni from Advancement.

Users can opt-out from appeals/mailing list at any time.

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.**

The information is only updated by the user or by the user's request.

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?**

Personal information on alumni are kept within Raiser's Edge indefinitely. Users may request that their information be removed from Raiser's Edge by contacting Advancement. We do not destroy records of alumni unless requested by the alumni themself.

As per the contractual terms, upon termination of the agreement, the university can request that:

within 30 days of termination of the Agreement, Graduway shall within a reasonable time of such request

> *(i) return or, at Client's option, destroy the Client Materials (including erasure from Graduway's computer systems) within its possession or control and confirm in writing to Client when it has complied with this clause;*

> *(ii) transfer to Client any domain names used by Graduway in providing the Services; and*

> *(iii) transfer to Client all rights in the Derived Data;*

Derived data refers to data provided by users, data recorded relating to the activity of users, and all data derived from this data.

Part 5 – Further Information

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

For example: your department has a regular exchange of personal information (both collection and disclosure) with the federal government in order to provide services to your clients.

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.**

For example: your public body will be disclosing information to PhD students so that they can conduct research.

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 FIPPA. Under this same section, this information is required to be published in a public directory.**

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

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

Part 6 – Privacy Officer 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).

Audrey Chen	*[signature]*	May 4, 2020
Privacy Office Representative	Signature	Date

Part 7 – Program Area Signatures

Chantale Lavoie
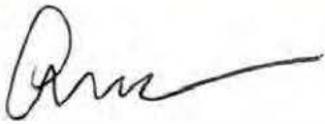
Program/Department Manager   Signature   **May 4, 2020**

                  Date

Sally Felkai

Contact responsible for Systems   Signature   May 5, 2020
Maintenance and/or Security
(Signature not required unless
they have been involved in the
PIA)

                  Date

Adrian Tees   May 8, 2020

Head of Public Body (or   Signature   Date
designate)

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

If you have any questions, please contact privacy@ecuad.ca or call the OCIO's Privacy and Access Helpline at 250 356-1851.