Capilano University

Privacy Impact Assessment

[Blackbaud Award Management BBAM]

PIA #[number]

Table of Contents

PART 1: GENERAL INFORMATION 1

PART 2: COLLECTION, USE AND DISCLOSURE 4

PART 3: STORING PERSONAL INFORMATION 6

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 6

PART 5: SECURITY OF PERSONAL INFORMATION 9

PART 6: ACCURACY, CORRECTION AND RETENTION 11

PART 7: AGREEMENTS AND INFORMATION BANKS 13

PART 8: ADDITIONAL RISKS 14

PART 9: SIGNATURES 14

PART 1: GENERAL INFORMATION **Initiative Title:**	Blackbaud Award Management Software
Organization:	Capilano University
Branch or Unit:	Philanthropy & Alumni Relations / Financial Aid & Awards
PIA Drafter Name:	Jennifer Bryan and Cary Gaymond
PIA Drafter Phone:	604.986.1911
PIA Drafter Email:	Jenniferbryan@capilanou.ca
Initiative Lead Name and Title:	Cary Gaymond
Initiative Lead Phone:	(604) 983-7572
Initiative Lead Email:	carygaymond@capilanou.ca
Privacy Officer:	Jacquetta Goy
Privacy Officer phone:	604-984-4915
Privacy Officer email:	jacquettagoy@capilanou.ca

General information about the PIA:

Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner. 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. No
Related PIAs, if any: This is part of our existing Blackbaud CRM software system, it is an add-on program. Our CRM has undergone a previous privacy assessment.

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.

Blackbaud Awards Management Software (BBAM) is a software tool to manage our scholarships, bursary, and awards (SBA) process, from application to disbursement, while also supporting donor reporting for SBA gifts.

BBAM will help:

- Improve student access to awards
- create impactful stewardship practices
- enhance cross-functional visibility throughout the process

1. Improve Student Access to Scholarship Funds and Awards

A single website makes it easy to promote all scholarships on campus to your student population. Every student receives a unique view of scholarships for which they are most qualified. Nightly integration with our student information management system shortens the time it takes to complete applications and improves the quality and accuracy of data on each application.

2. Create impactful ways to steward scholarship and non-scholarship donors

Key donor data from our existing Blackbaud Raiser's Edge CRM, will be combined with fund financial data, thank-you letters, and other fund beneficiary information in a single platform to share impact with donors. With easy access to data, we will discover new and effective ways to steward more

donors such as creating donor reports with the click of a button to mail, email, print, or view online. Will can provide donors with an online scrapbook experience to see their complete impact throughout the lifetime of their gift.

3. **Enhance cross-functional visibility throughout the scholarship process**

Gives all cross-functional stakeholders access to one central awards platform. Flexible permissions capabilities provide access to scholarship processing information while keeping student data protected. Also, the global view of scholarship recipients makes it easy to complete campus-wide audits for fund utilization and compliance purposes.

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?

The full Award Management Software integration is covered in this PIA and interfaces with our existing donor management CRM system with Blackbaud, Raiser's Edge.

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

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 a table below or in an attachment.

Elements of information or data collected as part of this initiative include

the student's first and last name,

date of birth,

previous last name (if applicable)

address,

phone number,

student ID,

program/area of study etc.

It will integrate with Financial Aid management systems and the existing Blackbaud CRM system for donor management with the Philanthropy and Alumni Relations team.

Did you list personal information in question 3? Yes

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.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer (privacy@capilanou.ca) You do not need to complete the rest of the PIA template**.**

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

Only students interested in applying for a scholarship, bursary or award would provide their personal information. This information will be provided directly by the student applying, not by CapU staff. There will not be a general gathering of student information. Donor information will only be accessed through the existing CRM and only what the donor provides to the awards page. Full integration with the existing CRM system with its privacy protections.

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.

5. 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**	**FIPPA authority**	**Other legal authority**
Step 1: Student create a login to apply for funding through Financial Aid using the software,	*Collection*	*26(c)*	

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**	**FIPPA authority**	**Other legal authority**
providing their personal information (name, address, phone, email, student number).			
Step 2: Financial Aid staff review applications and contact students if successful.	*Disclosure*	*26(c)*	
Step 3: Donors can login to view if their fund has been awarded to a student.		X	
Step 4: Donors can top-up/donate to their award fund through the donor page that integrates with the existing CRM.		X	

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.

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Attach or link to the collection notice to be used.

We are committed to protecting your privacy and personal information through responsible information management practices. We collect, use, retain, disclose and dispose of personal information in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), other applicable legislation and Capilano University privacy management practices.

This application collects personal information to allow Capilano University to learn about the students that are applying with the Financial Aid & Awards Office so that they can provide suitable services to students. It is collected by Capilano University under (s)(26)(c) of FIPPA. By submitting this form, you are providing your consent for Capilano University to collect and use this information for this purpose. If you have any questions, please contact *fdn@capilanou.ca*

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.

7. Is any personal information stored outside of Canada? **No**.

8. Does your initiative involve sensitive personal information? **Yes**

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)? No

FOIPPA Section 33(2)(f) states that a public body may disclose personal information if the information is made available to the public under an enactment that authorizes or requires the information to be made public.

- If yes, go to question 10
- If no, go to Part 4

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

Describe exactly where the personal information is being stored, e.g., on premise servers, data centres, and in what cities.

n/a

After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

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

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

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

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

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

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

- If yes, describe, attach or link to the *contract and/or other* contractual measures related to your initiative.

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

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

17. 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 additional rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering 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, please describe.

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 17. **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.

18. Does your initiative involve digital tools, databases, or information systems? **Yes**.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30? No.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

No, it was determined that a separate security assessment was not required for this additional Blackbaud module.

19. What technical and physical security do you have in place to protect personal information?

Describe where the digital records for your initiative are stored (e.g., on your organization's LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.

If you have completed a security assessment, you may want to append it to the PIA.

How are digital records stored?

This is a Schedule 15 The Schedule 15 system used by CapU encourages enhanced security with the Schedule 15 and other security measures across multiple systems, reducing the risk of unauthorized access and data breaches.

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	**Yes/No**
We only allow PAR employees and VP of UR to access the Blackbaud database and all names are recorded and managed by our Data Analyst PAR	Yes
Employees that need standing or recurring access to personal information must be approved by Director of PAR	Yes
We can, and do, use audit logs to see who accesses a file and when	Yes
Describe any additional controls:	

Strategy	Yes/No
If you have methods for controlling and tracking access to personal information that are not listed in the table, add additional methods here. Software allows for different access levels. Staff only receive the level of access needed to conduct their job duties.	

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

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

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

Students will have required fields to complete to create their login information and accounts. They will not be able to create their account or apply for awards if their information is incomplete.

22. 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.

22.1 Do you have a process in place to correct personal information? Yes.

Students and donors can request corrections via the Foundation office, email or phone number. The Data Analyst for the Philanthropy & Alumni Relations office confirms the corrections to donor accounts, the Financial Aid & Awards office will make corrections to student account.

22.2 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?

Describe how records will be corrected / how notes will be recorded

The Blackbaud CRM systems allow for notes to be added to donor students records for information edits that can't be made.

22.3 If a request for correction is received from an individual and a disclosure of their personal information has occurred in the last year, FOIPPA requires notification to the other public body or third party of the request for correction.

Describe how disclosures be tracked and notifications be made if necessary.

No personal information will be disclosed to public bodies or third parties.

23. Does the initiative use personal information to make decisions that directly affect an individual? Yes

- If yes, go to question 25
- If no, skip ahead to Part 7

24. FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. Is there an information schedule in place related to personal information used to make a decision? No

- If no, describe how the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

All student and donor records will remain on file.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement? No

- If yes, please complete the Information Sharing Agreement Supplement (*Appendix B)* and attach it to your PIA

26. Will your initiative result in a personal information bank? Yes.

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

- If yes, please complete the table below.

Describe the type of information in the bank: name, address, birthdate, email, phone, student number, awards received
Name of main organization involved: Capilano University
Any other ministries, agencies, public bodies, or organizations involved: none
Business contact title and phone number for person responsible for managing the PIB: Data Analyst, Capilano University 604-984-4983

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.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing, or disclosing personal information in your initiative that have not been addressed by the questions on the template.

No additional risks identified

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering 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, please describe.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

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	Signature	Date Signed
Privacy Officer / Privacy Office Representative	Jacquetta Goy	Jacquetta Goy	May 2023

Program Area 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.

Program Area Comments:

Role	Name	Signature	Date Signed
Initiative Lead	Cary Gaymond	Cary Gaymond	May 3 2023
Program/Department Manager	Cary Gaymond	Cary Gaymond	May 3 2023
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA	n/a		
Head of public body, or designate	Jennifer Ingham	Jennifer Ingham	May 8 2023

Appendix B

Information Sharing Agreement Supplement

Information Sharing Agreements

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.

Please provide information about your ISA.

Description of ISA:
Name of main ministry or agency involved:
Any other ministries, agencies, public bodies, or organizations involved:
Business contact title and phone number for person responsible for maintaining the ISA:
ISA start date:
ISA end date: