Privacy Impact Assessment

Table of Contents

Use this privacy impact assessment (PIA) template if you are starting a new initiative or significantly changing an existing initiative.

Before you start

- An initiative is an enactment, system, project, program, or activity
- Find information on the PIA review process and question-by-question guidance.
- If you have any questions, contact the CNC Privacy Office at foipp@cnc.bc.ca

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Devant International & Domestic Student Career Services
Organization:	College of New Caledonia

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 appendix.

As part of the user's account profile:

Required information:

- Name
- Email address
- Other study or employment-related and biographical information submitted

Optional information:

- Address
- Telephone number(s)
- Profile photo
- Identification number allocated by the student
- Education history
- Work experience
- Achievements and skill entered in CV/resume builder
- Personality and preference data, including personality traits, strengths, motivators, career aspirations
- Social media data a user chooses to provide
- Career coach or administrator, career intervention notes and other information relating to career development

Usage and log data is automatically collected when a user visits the site, including IP address and general location, device information, and progression through the site, areas viewed and where abandoned.

Students also have significant control of their data through the platform as outlined in the privacy document privacy terms presented to the students during registration.

3.1 Did you list personal information in question 3?

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.

Yes

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

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

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

N/A

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**	**FOIPPA authority**	**Other legal authority**
Step 1: Students sign up and create an account profile by uploading some or all personal data listed in Part 1: Q3 of this document, via the web browser	Collection	26(d)	
Step 2: Students may instruct the service to share their data with other users or groups/classes of users.	Disclosure	33(2)(c)	
Step 3: Data received is stored in a cloud environment in accordance with options selected by Client/Users.	Disclosure	33(2)(c) 33(2)(u)	
Step 4: Data received is processed for the purpose of providing white-labelled careers support tools and e-learning to CNC students	Use	32(b)	

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).

CNC

As this service is an optional service and there is no data exchanged between Devant and CNC there is no obligation for CNC to provide notification – please see Devant's notification below.

Devant

Privacy notice can be found here

When registering for an account:

> I confirm that I am at least 16 years of age or older
>
> I have read and accept any EULA, Terms and Conditions, Acceptable Use Policy, and/or Data Processing Addendum which has been provided to me in connection with the software, products and/or services.
>
> I have been fully informed and consent to the collection and use of my personal data for any purpose in connection with the software, products and/or services.
>
> I understand that certain data, including personal data, must be collected or processed in order for you to provide any products or services I have requested or contracted for. I understand that in some cases it may be required to use cookies or similar tracking to provide those products or services..
>
> I understand that I have the right to request access annually to any personal data you have obtained or collected regarding me. You have agreed to provide me with a record of my personal data in a readable format.
>
> I also understand that I can revoke my consent and that I have the right to be forgotten. If I revoke my consent you will stop collecting or processing my personal data. I understand that if I revoke my consent, you may be unable to provide contracted products or services to me, and I can not hold you responsible for that.
>
> Likewise, if I properly request to be forgotten, you will delete the data you have for me, or make it inaccessible. I also understand that if there is a dispute regarding my personal data, I can contact

someone who is responsible for handling data-related concerns. If we are unable to resolve any issue, you will provide an independent service to arbitrate a resolution. If I have any questions regarding my rights or privacy, I can contact the email address provided.

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?

Yes.

8. Does your initiative involve sensitive personal information?

Yes, the optional information may be considered sensitive.

- 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.

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

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

After you answer this question go to Part 5.

Servers are in the [redacted] England at Memset [redacted] 15(1)(l)

Amazon S3 London – Only video recordings are stored without any PII attached to them

Azure London – Live chat application data is stored

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. More help is available in the Guidance on Disclosures Outside of Canada.

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

* See page 14-16 of Career Centre Data protection factsheet attached

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Abintegro	Dedicated servers managed by Abintegro Data is stored in [redacted] There are also PDF, Word and Excel documents stored that are uploaded by the end users or administrators	Servers are in the UK at Memset [redacted] datacentres Amazon S3 London – Only video recordings are stored without any PII attached to it. Azure London – Live chat application data is stored
		For Backups Data Centre: Memset Location: [redacted]

15(1)(l)

15(1)(l)

15(1)(l)

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
		Backup Schedule: Daily Retention Period: 7days Encryption in Transit: [redacted] Encryption at rest: [redacted] Backups are automated and managed by Abintegro

15(1)(l)

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

By default, there isn't any data transfer to other systems however there are APIs available for customers/users to integrate to push and pull data.

For detailed information on third parties that have access to the data, please see the Sub processor schedule on pages 14-16 of *the Career Centre Data Protection Fact sheet* (attached).

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

Yes

- If yes, describe the contractual measures related to your initiative.

The Service Agreement privacy terms include access controls, non-disclosure clause, security requirements (storage, processing, transmitting, and testing), return or destruction of information upon request, user activity records, and breach response plan.

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

[redacted] 15(1)(l)

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

[redacted] 15(1)(l)

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 new 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.**
Unauthorized individuals at CNC access the personal information	Medium	Low	Medium	Users have unique login credentials that they are instructed to not share with third parties. [redacted]	No 15(1)(l)

				[redacted]	15(1)(l)
Unauthorized individuals at Devant or their third-party sub-processors access the personal information	Medium	Low	Medium	Access restrictions are outlined in the attached fact sheet. Security Agreements are in place for sub-processors.	No
Personal information is compromised during transmission	Medium	Low	Medium	[redacted]	No 15(1)(l)

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

18.1 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

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.

Technical security measures – Devant 15(1)(l)

[redacted]

CNC

[redacted] 15(1)(l)

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	
We only allow employees in certain roles access to information	YES
Employees that need standing or recurring access to personal information must be approved by the Director of Student Services	YES
We use audit logs to see who accesses a file and when	YES
Describe any additional controls:	Other areas of the software where actions are recorded and auditable: [redacted] 15(1)(l) [redacted] 15(1)(l)

Strategy	
	[redacted]

15(1)(l)

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 enter their own information and are responsible for ensuring it's accuracy.

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 can update their profile information themselves and contact Devant to have their information updated, annotated, or permanently deleted.

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. Will you document the request to correct or annotate the record?

N/A

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A

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

No

- If yes, go to question 24
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

N/A

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

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 and attach it to your PIA

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

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

Yes.

- If yes, please complete the table below.

Describe the type of information in the bank: Devant career student support services
Name of main organization involved: College of New Caledonia
Any other ministries, agencies, public bodies, or organizations involved: Devant
Business contact title and phone number for person responsible for managing the PIB: Gail Little Manager, Student Success & Retention 250 562-2131 Ext 5604 littleg@cnc.bc.ca

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.

Risks are identified in Part 4, #17 of this PIA.

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	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Bev Hooper, Hooper Access and Privacy Consulting Ltd.	[redacted]	Aug 4/22

22(1)

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	Electronic signature	Date signed	
Initiative lead	Gail Little	[redacted]	08/04/2022	22(1)
Program/Department Manager	Gail Little	[redacted]	08/04/2022	22(1)
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA				
Head of public body, or designate Only required if personal information is involved				