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, email Privacy.Helpline@gov.bc.ca or phone 250 356-1851

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Comevo Inc. New Student On-line Orientation
Organization:	College of New Caledonia

Branch or unit:	Student Services Department
Your name and title:	Gail Little, Manager Student Success & Retention
Your work phone:	250-562-2131 x5604
Your email:	Littleg2@cnc.bc.ca
Initiative Lead name and title:	Gail Little Manager Student Success & Retention
Initiative Lead phone:	250-562-2131 x5604
Initiative Lead email:	Littleg2@cnc.bc.ca
Privacy Officer:	
Privacy Officer phone:	
Privacy Officer email:	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? 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:
None

1. What is the initiative?

The Student Services department wants to engage Comevo Inc. to run a new student online orientation software to provide new students an introduction to CNC and the resources available to support student success during their first-year experience, e.g., Technology, Academics, Advising, Supports, Health and Safety, Financial Aid and Awards, Campus Life, Student Success, CNC policies, Student Union, Aboriginal Resource Centre, and Campus Housing. Comevo only collects the necessary amount of personal data (first name, last name, email, and student ID) to distinguish users within the system. Student emails are collected to 'push out' reminder notifications to complete the online orientation. Comevo Inc. uses a Higher Education Community Vendor Assessment Toolkit (HECVAT) to assess security risks with clients.

2. What is the scope of the PIA?

The PIA will assess the collection, use, disclosure, security, and storage of students' personal information in the Comevo online orientation platform. The delivery of new student online orientation, including welcome information for domestic, Aboriginal, and international students, tasks required to complete on entry, available student services, supports, and policies fall within the scope of the PIA.

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

The following information would be collected by Comevo Inc. as students log onto the online orientation:

- Student unique identifier number
- Student email
- Student first and last name
- Whether student is Aboriginal or International (optional)

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?

Not applicable

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: CNC collects student contact information when they register as a student at the College and identifies their program	Collection	26(d)	
[redacted]	Use	32(a)	
	Collection	26(d)	15(1)(d)
	Use	32(a)	
	Use Collection	32(a) 26(d)	

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**
[redacted]			
Step 6: Comevo provides a dashboard allowing designated CNC employees to log in and see completion data (no personal information is included in this report)	Use	32(a)	

15(1)(d)

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).

Following is the notification from CNC's Registration for Admission form:

> The information on this form is collected for the purpose of determining admission, registration, research, statistical analysis purposes, locker and U-Pass administration, student health plan, and the ongoing administration of the student experience. It is collected under the authority of the *College and Institute Act* and the *Freedom of Information and Protection of Privacy Act*. The information you provide is protected under the *Freedom of Information and Protection of Privacy Act*, which specifically limits how your information may be used or disclosed. If you have any questions about the collection

and use of your information, contact the College of New Caledonia Privacy Office at 250-562-2131, or foipp@cnc.bc.ca. All hard copied materials/information provided by you in support of your application to CNC becomes property of the college and will not be returned to the student.

PART 3: STORING PERSONAL INFORMATION

If you are 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.

- 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 question 10
- If no, go to Part 4

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

Not applicable.

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)?
Amazon	Amazon Web Services	AWS-West Oregon USA
JungleDisk – storage provider	Rackspace	Dallas-Fort Worth-Arlington Metropolitan Area, USA
JungleDisk – storage provider	Google Cloud Storage	Several regions throughout the USA

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

Not applicable.

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

Yes.

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

The Application Hosting Agreement states that access to the Application is limited to users with a valid username/password. Data entered and displayed on the Application may be secured, at

the Client's discretion, using [redacted] encryption. Comevo will not share or disclose information related to the Client's use of the Application and will comply with all applicable state and federal laws related to the protection and privacy of student records. 15(1)(l)

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

All User information is stored at a class 3 data center. Password protection is enabled. Access to the servers is logged. Firewall rules are in place limiting port access.

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

All access is logged. Access is limited to only authorized database administrators.

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.**
Comevo or backup data centres involved in data breach	Low	Low	Low	Data breach response protocols in place. No barriers to response time.	No

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?

CNC

15(1)(l)

15(1)(l)

COMEVO – See Appendix A for Comevo's Security Policy Overview and the following link for additional information: https://comevo.com/comevo-prospective-client-technical-documents/

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 executive lead	Yes
We use audit logs to see who accesses a file and when	Yes
Describe any additional controls:	Comevo truncate data within the development environment to reduce personal information exposure risk.

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 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.

Students enter their own personal information into the Comevo platform and are responsible for ensuring its accuracy.

21.1 Do you have a process in place to correct personal information?

Yes, students can contact the Office of the Registrar at CNC to have their personal information updated.

21.2 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?

Not applicable, students can contact the Office of the Registrar at CNC to have their personal information updated.

21.3 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?

Yes, CNC will ensure that other third parties are notified should the need occur.

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

No.

22. 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.

Not applicable.

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.

23. Does your initiative involve an information sharing agreement?

No.

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.

No

- If yes, please complete the table below.

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 PIB

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.

24. 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.

Add new rows if necessary.

Possible risk	Response
Risk 1: Employees of CNC access personal information and use or disclose it for unauthorized purposes.	Employees receive training on confidentiality of student information and will be reminded of this requirement with the Comevo data. Access will be restricted to only those who require access to support the program.
Risk 2: Employees of Comevo access personal information and use or disclose it for unauthorized purposes.	Only authorized staff at Comevo have access to the required systems and information. Comevo has privacy and security policies in place.
Risk 3: Student personal information is compromised during transmission to Comevo.	Data will be provided via login portal in a password protected platform.

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]	June 6/22

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		
Program/Department Manager	Gail Little Manager, Student Success & Retention	[redacted]	June 7, 2022
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			

22(1)

Appendix A

COMEVO
COMMUNICATION EVOLVED

Security Policy Overview

Policy Manual
Authored by:
Kimo Yoshida, Director of Technology

1. Introduction

Keeping customer data safe and secure is a huge responsibility and a top priority for Comevo. We work hard to protect our customers from the latest threats.

2. Access control and organizational security

Personnel

All our employees and contractors (workers) sign confidentiality agreements before gaining access to our code and data. Background checks are performed on all workers who have access to customer data. Everybody at Comevo is trained and made aware of security concerns and best practices for their systems. Remote access to servers is via our VPN and limited to workers who need access for their day to day work. We log all access to all accounts by IP address. Within our SaaS platform, we treat all customer data as equally sensitive and have implemented stringent controls governing this data. Awareness training is provided to our internal employees and contractors during the on-boarding / induction

process which covers the importance of and best practices for handling customer data.
Within Comevo, only authorized Comevo employees have access to customer data stored within our applications. Authentication is done via individual 2FA (two-factor authentication), and the servers only accept incoming SSH connections from Comevo Headquarters.

Training and Awareness
Our security training and awareness program does not just check compliance boxes but results in a genuine uplift in knowledge across the company. Our awareness program is built on the premise that security is everyone's responsibility. These responsibilities are extracted from our internal Written Information Security Program (WISP), and the training and awareness program is used as the primary vehicle for communicating these responsibilities to our staff.

Dedicated teams
Our Operations team and our Security, Infrastructure and Performance (SIP) team are in charge of access/identity management, network connectivity, firewalls and log file management. These two teams' responsibilities include:

- Maintain and support our automated test suite for development machines
- Build/operate Comevo's infrastructure, including logs, monitoring and authentication
- Review, test and design incident response processes
- Respond to alerts triggered by any security events
- Coordinate external audits and security and privacy certifications
- Monitor and alert on anomalous activity
- Coordinate vulnerability testing

Audits, Security Policies and Standards
Comevo itself has not completed a SOC audit. We can provide a copy of the SOC reports for the data centers we use, Amazon AWS, after completing an NDA.

We have an internally built system that monitors and automatically blocks suspicious activity (including vulnerability scanning, failed logins, and a host of other suspicious activities). We also have alerts in place for excessive resource use that escalates to our Ops team for manual investigation. Our products run on a dedicated network secured with firewalls and are carefully monitored.

3. Data protection and privacy

Data Location

Our primary data centers are in the United States through the use of Amazon AWS Cloud Services. All data is written to multiple disks are instantly backed up daily and stored in multiple locations. Customer files are stored on Amazon S3 servers that use modern techniques to remove bottlenecks and points of failure. Our software infrastructure is regularly updated with the latest security patches.

Encryption in transit and at rest

Over public networks we send data using strong encryption. We use SSL certificates issued by Sectigo RSA Domain Validation Secure Server CA. The connection uses AWS_256_CBC for encryption, with SHA2 for message authentication and ECDHE_RSA as the key exchange mechanism.
Any files that are uploaded are stored and encrypted at rest. Our storage system uses AES-256/ SHA-256 encryption. Files are encrypted with AES-256, sliced, replicated, and geographically dispersed to separate data centers on private, end-to-end encrypted network connections.

Business Continuity and Disaster Recovery

We strive to maintain strong Business Continuity (BC) and Disaster Recovery (DR) capabilities to ensure that the effect on our customers is minimized in the event of any disruptions to our operations.

Our Disaster Recovery Program consists of a few key practices to ensure the appropriate levels of governance, oversight, and testing:

1. Governance. Leadership involvement is key to how we run our DR Program. With leadership involved, we have both business and technical drivers accounted for in our strategy for resilience.
2. Oversight and maintenance. We take a disciplined governance, risk, and compliance approach when monitoring and managing our DR program. It enables us to operate more efficiently and effectively when monitoring, measuring, reporting, and remediating key activities within our DR program. Site Reliability Engineers are committed to ongoing Disaster Recovery meetings and represent their critical services. They discuss identified DR gaps with the risk and compliance team and focus on the appropriate levels of remediation as necessary.
3. Testing. We conduct regular testing and strive for continual improvement as part of our DR lifecycle to ensure your data and the use of your data is highly available and performant. Backup and restore procedures are in place and tested on a regular basis. This means that when data needs to be restored, we're prepared to get you up and running with well-trained support staff and fully tested procedures.

In addition to assurance of resiliency through governance, oversight, and testing, Comevo emphasizes on continual improvement throughout the DR Program.

As far as Business Continuity (BC) is concerned, Comevo is a cloud-based company, so it's very easy for us to arrange for our people to work from home. That means that our team can and will continue to support you wherever they are and wherever you are.

Backups

Application data is stored on resilient storage that is replicated across data centers. Application database backups for

Comevo Launch occur on the following frequencies: daily automated backups are performed and retained for 30 days with support for point in time recovery. All snapshot and backup data are encrypted. Backup data is stored offsite and is replicated to multiple data centers within a particular AWS region. We perform quarterly testing of our backups. Our backups of your data are encrypted using AES-256 best-in-class military-grade encryption.

Physical Security
The state-of-the-art AWS EC2 Cloud servers physical security begins at the perimeter layer. This layer includes many security features such as security guards, fencing, security feeds, intrusion detection technology and other security measures. Only authorized personnel have access to the data center. 24/7/365 onsite staff provides extra protection against unauthorized entry and security breaches.

Law enforcement
Comevo won't hand your data over to law enforcement unless a court order says we have to. We flat out reject requests from local and federal law enforcement when they seek data without a court order. Unless we are legally prevented from it, we will always inform you when we receive such requests.

Data deletion
All of your data can be deleted upon your request. Within 30 days of your request, all Comevo content will be permanently deleted from all servers and logs. This information can not be recovered once it has been permanently deleted. We also keep backups stored off-site for a maximum of 30 additional days. Therefore, after a cancellation, all data will be permanently deleted from backups within 60 days. A data deletion request will have to go through our "Data Deletion Request Process". An email sent to "datadeletion@comevo.com" will start the process. Upon receipt of the request, Comevo will send an online "Data Deletion Request" form to begin the formal request process.