Privacy Impact Assessment
ClockWork

Part 1 – General

Name of Department:	Student and Enrolment Services		
PIA Drafter:	Norman Chang		
Email:	nchang@vcc.ca	Phone:	604-868-1068
Department Mgr:	Sheri Wiwchar		
Email:	swiwchar@vcc.ca	Phone:	604-871-7204

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

1. **Description of the Initiative**

   - Online booking portal for Disability Services and Counselling (existing)
   - Configuration for intake and tracking files in Arbiter of Students Issues office
   - Outlook calendar sync (existing)
   - On-Line Appointment Booking (existing)
   - On-line staff calendar (existing)
   - ClockworkMigration from on-premise ClockWork to Cloud (Azure Canada)
     - Database migration
     - New data sync
     - New authentication (SSO)
   - Activate online booking portal for test accommodations
   - Activating intake form
   - Collect student documentation through Cloud portal
   - Generate Accommodation Letters through Cloud portal

2. **Scope of this PIA**

   This PIA covers the existing and the new additions of Clockwork implementation. Clockwork is utilized by Disability Services, Counselling, and the Arbiter of Student Issues. The responses within this PIA should assist in analyzing the possible impacts on employee and student privacy, describing privacy design techniques and risk mitigation measures in place as a part of the solution and

ensuring that privacy considerations are first and foremost in the design of the proposed system and within the project overall.

3. **Related Privacy Impact Assessments**

The data is hosted in Canada within the Microsoft Azure infrastructure. The use of MS product suite is covered by the BCNET PIA.

4. **All Elements of Information or Data**

The elements of information or data utilized various based on the integration of service.

User interaction with Clockwork:

- *VCC student number*

- *VCC student email address*

- *Personal email address*

- *Personal contact information (address, emergency contact etc.)*

- *Identity information (gender, pronouns, etc.)*

- *Medical documentation*

- *Disability status*

- *Confidentiality release*

- *Educational history (information related to enrollment and participation in VCC programs and courses)*

- *Opinions and recorded opinions/evaluations about an individual*

If personal information is involved in your initiative, please continue to the next page to complete 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**

   Data for this initiative will only be stored and accessed in Canada.

   Access to the data in this initiative is restricted to VCC staff only.

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;	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 Officer 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;	No
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.	

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

s. 15(1)(l)

Dataflow path 1: Browser -> Internet -> Application Server -> Azure

Dataflow path 2: Workstation client -> Internet -> Application Server -> Azure

Dataflow path 3: Outlook -> Azure

9. **Risk Mitigation Table**

Risk Mitigation Table		Mitigation Strategy	Likelihood	Impact
1.	Employees could access personal information and use or disclose it for personal purposes	Staff and contract instructors bound by employee/contractor agreement; staff bound by Standards of Conduct	Low	High
2.	Hosted infrastructure compromised	Comprehensive infrastructure design, monitoring and alerts. Data and documents encrypted in transit and at rest with secure key storage.	Low	High
3.	Client's personal information is compromised when transferred to the service provider	Transmission is encrypted.	Low	High
4.	Injection attack	Secure development and deployment policies and practices. Monitoring, Scanning and alerts.	Medium	High
5.	Exploiting vulnerabilities within the technology offering	Intrusion prevention system is implemented. Integrated threat intelligence: looks for known bad actors by leveraging global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds. Behavioral analytics: applies known patterns to discover malicious behavior. Anomaly detection: uses statistical profiling to build a historical baseline. It alerts on deviations from	Medium	High

		established baselines that conform to a potential attack vector.		

10. Collection Notice

If your initiative is collecting personal information directly from individuals you must ensure that all individuals involved are told the following:

1. *The purpose for which the information is being collected*
2. *The legal authority for collecting it, and*
3. *The title, business address and business telephone number of an officer or employee who can answer questions about the collection.*

Please include your proposed wording for a collection & consent notice and where it will be located for individuals to read before collection takes place. You can also attach a screen shot or a copy of your form where the collection notice would be located.

VCC privacy page link is added to the website:

https://www.vcc.ca/about/college-information/privacy-policy/

Within the above policy, a summary of the approach has been provided with link to disclaimer as well as contact information (#3).

More detail information is included under the information disclaimer section:

https://www.vcc.ca/about/college-information/disclaimer/

Why We Collect (#1)

We collect personal information:

- *For the purpose of sending you official correspondence related to your education at VCC, communicating with you in an instructional capacity, and gathering essential information for operating purposes.*

- *For the purpose of providing students with the opportunity to participate in former student outcome surveys. The results of these surveys are used to improve the quality and effectiveness of instruction and services that we provide.*

The Ministry uses this information in order to monitor institutional progress and comply with government stated objectives.

To conduct institutional research on education policy issues, such as quality of education, student satisfaction, ease of transfers, student access, future student needs, evaluate training needs for a variety of population groups such as insert students, transfer students, first nations students, international student etc.

Under What Authorization We Collect (#2)

We collect personal information from you as authorized by the College and Institute Act. The personal information we collect is necessary to:

- *obtain a personal education number (PEN) for the student*

- *carry out institutional responsibilities related to operating program or activity*

- *prepare and submit budgets, financial statements, reports and other information that the minister considers necessary to carry out the minister's responsibilities in relation to institutions*

- *conduct institutional research and statistical analysis*

The Freedom of Information and Protection of Privacy Act has directed that we provide you with this background. You may be assured that we will take all reasonable measures to ensure that your information is treated in a confidential manner.

Consent forms

In addition to general VCC privacy policy, individuals (students) will complete additional consent and intake forms depending on the department (Disability Services, Counselling, Arbiter of Student Issues) in order to provide their information to the system. Collection notices on these consent and intake forms will provide notice of collection under s. 26(c) and the purpose of that collection, depending on the responsible department/office, and a contact within each department who can answer questions about the collection and use of that personal information.

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 the Privacy Officer, CIO or IT Security Officer when filling out this section.

11. Please describe the <u>physical</u> security measures related to the initiative (if applicable).

The solution is hosted entirely on cloud infrastructure provided by Microsoft. Microsoft employs a number of complex physical security mechanisms around a layered security approach.

https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

EMPLOYEE DATA CENTER ACCESS

Access to physical datacenter facilities is tightly controlled by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, integrated alarm systems, around-the-clock video surveillance by the operations center, and multi-factor access control. Only required personnel are authorized to access Microsoft datacenters. Logical access to Microsoft 365 infrastructure, including customer data, is prohibited from within Microsoft datacenters.

MS Security Operations Centers use video surveillance along with integrated electronic access control systems to monitor datacenter sites and facilities. Cameras are strategically positioned for effective coverage of the facility perimeter, entrances, shipping bays, server cages, interior aisles, and other sensitive security points of interest. As part of our multi-layered security posture, any unauthorized entry attempts detected by the integrated security systems generate alerts to security personnel for immediate response and remediation.

12. Please describe the <u>technical</u> security measures related to the initiative (if applicable).

The entire solution runs within a tightly controlled, managed, and partitioned Microsoft environment. All aspects of Microsoft physical and infrastructure-level security are outlined on:

https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

TechnoPro/ClockWork Enterprise has also completed a separate HECVAT assessment.

13. Does your department rely on any security policies? If so, indicate here:

VCC IT Security Policies:

Information Technology General Policy (B.5.1, B.5.2, B.5.4, B.5.5)
https://www.vcc.ca/about/governance--policies/policies/administration-policies/

Other IT Policies:

IT Administrative Rights Application and Policy
https://employee.vcc.ca/media/myvcc/content-assets/documents/departments/information-technology/forms/it-Administrative-Rights-Policy.pdf

Vulnerability Management
https://employee.vcc.ca/media/myvcc/content-assets/documents/departments/information-technology/other/Vulnerability-Management-IT-Standard.pdf

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.

ClockWork utilizes a role-based permission system. 'No access', 'read-only access', or 'read/write access' permissions are available for all form data (including disability and accommodation data). Also, access to student records can be restricted based on custom rules such as 'part-time students', or other custom rules such as 'student is a relative of a staff member'. Various functions, such as modifying data form definitions, running reports, sending emails, can also be restricted based on user roles.

No end-user has access to delete or modify any submitted data. Clockwork records specific user, date/time, and originating IP for login attempts (failed and success) and changes in the data (records).

Departments are only able to access the records related to their department, ensuring that there is no unauthorized access or exchange of personal information between departments.

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

    Access control will be granted through active directory with all access requests will go through our Helpdesk system.

    ClockWork supports Active Directory and Ldap integration for staff logins. For student and faculty logins ClockWork supports Active Directory, ADFS, Ldap, Portal Guard, Shibboleth, CAS, as well as custom authentication. Plus the following logging features:

    a) all security/authorization changes and user and admin security events are logged
    b) no requirements are necessary, logging is built-in and working out-of-the-box. Some logs are stored in the database and some logs are stored in Azure storage. Logs in the database will include sensitive information where logs in Azure storage will not.
    c) logging reports are available that provide access to logs that are in the database. Data can be searched, sorted and filtered.

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 information will not be disclosed to public but individuals defined within the business processes. VCC Disability Services, Counselling, and Arbiter of Student Issues teams will handle all questions and requests in regard to data update or discrepancies, depending on who receives the request for correction.

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

Yes. Personal information that is collected from students (including their medical documentation) is by the 3 department areas to provide individualized services to students: the PI is used to execute intake processes into the respective offices; make decisions about students' eligibility for accommodations; generate accommodation letters; provide them access to booking portals for test and other accommodations; refer them to appropriate services as needed; and provide the appropriate assistance in navigating issues within the College.

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.

Personal information is collected directly from the students with consent, or otherwise pulled from Banner, where students have the ability to correct and update their own personal information.

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. Personal information is kept for at least one year after it is used to make a decision that directly affects an individual and is kept in accordance with VCC's Records Retention Schedule.

Part 5 – Further Information

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

No.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact the Privacy Officer.	

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 the Privacy Officer.

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. See below.

A personal information bank of students will be created. VCC is able to provide the descriptors required as part of this initiative.

As per section 69 (6) of FOIPPA:

> *(6) The head of a public body that is not a ministry must make available for inspection and copying by the public a directory that lists the public body's personal information banks and includes the following information with respect to each personal information bank:*
>
> *(a) its title and location;*
>
> **ClockWork database – records are a shared responsibility between Disability Services, Counselling, and Arbiter of Student Issues**
>
> *(b) a description of the kind of personal information and the categories of individuals whose personal information is included;*
>
> **Personal information is collected from and about students. Personal information includes (depending on department): name, student number, contact information, age, sex, gender identification, sexual orientation, disability, marital and family status, medical history, psychological history, educational history, financial history, third party opinions about the individual, and the individual's own views or opinions.**
>
> *(c) the authority for collecting the personal information;*
>
> **College and Institute Act (RSBC 1996, c. 52)**
>
> **Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165) - s. 26(c)**

VCC Policy 327, Students with Disabilities

(d) the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed;

Personal information is collected by the College because it relates directly to and is necessary for the operation of Disability Services, Counselling, and Arbiter of Student Issues departments/office. Personal information is used to provide students with individualized services, accommodations, and assistance in navigating issues within the College as needed. Personal information is only disclosed for the purpose for which it was obtained or compiled or for a use consistent with that purpose (such as delivering services such as test accommodations), or with the student's explicit and informed consent.

(e) the categories of persons who use the personal information or to whom it is disclosed;

Individuals and College departments (Counselling, Disability Services, ASI) who require the personal information to deliver the required services (e.g. accommodation letters); third parties upon authorization from students (referral to other services or institutions)

Part 6 – Privacy Comments

This PIA is based on a review of the material provided 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.

Surinder Aulakh

Privacy Officer

19/06/2024

Signature   Date

Part 7 – Program Area Signatures

Nigel Scott		07/03/2024
Associate Director, Student Accessibility	Signature	Date

Robert Ruddell		July 8, 2024
Department Head, Counselling Services	Signature	Date

Tanny Marks		06/28/2024
Arbiter of Student Issues	Signature	Date
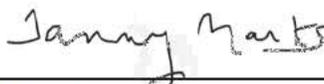
Norman Chang		6/25/2024
Director IT and Enterprise Architecture	Signature	Date