This form is used by VIU to determine if a proposed new initiative or significant changes to an existing initiative (policy, system, project, program or activity) meets or will meet the protection of privacy requirements under Part 3, Section 69 (5.3) of the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA). The Act makes it a legal requirement that VIU conduct a PIA in accordance with the directions of the minister responsbile for the Act. The PIA is a risk management tool to identify potential privacy issues and impacts, allowing correction and mitigation, thus avoiding costly system, program, service, or process redesign; privacy complaints or breaches; and harm to personal, professional, and institutional reputation.

# PART 1 - GENERAL INFORMATION

## 1.1. Unit and Program Area

Identify the Department and Program submitting this PIA.

|  |  |
| --- | --- |
| Department: |  |
| Program: |  |

## 1.2. Contact Information

Identify the individuals best positioned to speak to the contents of this PIA.

|  |  |  |  |
| --- | --- | --- | --- |
| Name of PIA drafter: |  |  |  |
| Position Title: |  |  |  |
| Phone: |  | Email: |  |
| Name of Program Manager: |  |  |  |
| Position Title: |  |  |  |
| Phone: |  | Email: |  |

## 1.3. Overview of the Initiative

Provide as background a general description of the initiative and the context in which it functions. Describe what you are doing, how it works, who is involved and when or how long the initiative runs. This could include the purpose of the initiative and its benefits, what larger process it is part of, how it aggregates and stores together information that was previously maintained separately, how it converges different record keeping systems, the parties involved, how it will automate or otherwise change the existing business workflow, etc. If this is a change to an existing program or system, describe the current system or program and the proposed changes.

|  |
| --- |
|  |

## 1.4. Specific Actors Involved

Thinking back to how you described the background in the previous section, provide specific details with respect to the individual actors involved in the process, focusing on how personal information will be collected, accessed, used, disclosed and retained.

### 1.4.a. Student Information

|  |  |
| --- | --- |
| Collection: |  |
| Access: |  |
| Use: |  |
| Disclosure: |  |
| Retention: |  |

### 1.4.b. Employee Information

|  |  |
| --- | --- |
| Collection: |  |
| Access: |  |
| Use: |  |
| Disclosure: |  |
| Retention: |  |

### 1.4.c. Other Parties’ Information

|  |  |
| --- | --- |
| Collection: |  |
| Access: |  |
| Use: |  |
| Disclosure: |  |
| Retention: |  |

## 1.5. Scope of this PIA

Where applicable, explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

|  |
| --- |
|  |

## 1.6. Related Privacy Impact Assessments

Identify PIAs for other parts of the initiative or any PIAs that were previously completed for this initiative.

|  |
| --- |
|  |

## 1.7. Elements of Information or Data

List the types of personal information involved in the initiative, if applicable. This could include the individual’s name, age, address, work/home email, work/home phone number, educational history, employment history, work status, health information, financial information, photos, comments, or opinions about third parties. See Schedule A for a partial list of types of personal information.

If the initiative does not involve personal information, go ahead to Part 8 Signatures.

### 1.7.a. Student data elements:

|  |
| --- |
|  |

### 1.7.b. Employee data elements:

|  |
| --- |
|  |

### 1.7.c. Other Parties’ data elements:

|  |
| --- |
|  |

## 1.8. Storage of Access Outside of Canada

 Provide a brief description of whether the personal information can be accessed from outside Canada. For example, by a service provider that is repairing a system, or if the information is being stored outside Canada, for example, in the “cloud”. If the data is stored within Canada and only accessible within Canada, please indicate this and describe with whom and where it is stored.

|  |
| --- |
|  |

## 1.9. Data-linking Initiative

|  |
| --- |
| In FIPPA, “data-linking” and a “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 three questions, your initiative may be a data-linking initiative. If so, you must comply with requirements under the Act for a data-linking initiative. |
| 1. Personal information from one database is linked or combined with personal information from another database.
 | * Yes
* No
 |
| 1. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled.
 | * Yes
* No
 |
| 1. 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
 | * Yes
* No
 |
| If you answered ‘yes’ to all three questions, please contact the Information and Privacy Coordinator or Privacy Officer to discuss the requirements of a data-linking initiative. |

## 1.10. 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 three 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 services or services
 | * Yes
* No
 |
| 1. Those services are provided through: 1) a public body and at least one other public body or agency working collaboratively to provide that service; or 2) one public body working on behalf of one or more other public bodies or agencies.
 | * Yes
* No
 |
| 1. The common or integrated program or activity is confirmed by a written agreement that meets the requirements set out in section 12 of the FIPPA Regulation.
 | * Yes
* No
 |
| If you answered ‘yes’ to all three questions, please contact the Information and Privacy Coordinator or Privacy Officer to discuss the requirements of a common or integrated program or activity. |

## 1.11. Data Flow

Provide a description (either a narrative, flow chart, or table) of the linkages and flows of personal information collected, used, and/or disclosed.

|  |
| --- |
|  |

# PART 2 – COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

## 2.1. Personal Information Flow Diagram/Table

Complete the table(s) below, if applicable. Include a personal information data flow diagram (if one exists) as well as completing the table(s).

### 2.1.a. Student Personal Information Data Flow

|  |
| --- |
| **Personal Information Flow Table** |
|  | **Description /Purpose of Activity** | **Privacy Rule** | **Legal Authority** |
| 1. |  | Collection |  |
| 2. |  | Use |  |
| 3. |  | Disclosure |  |

### 2.1.b. Employee Personal Information Data Flow

|  |
| --- |
| **Personal Information Flow Table** |
|  | **Description /Purpose of Activity** | **Privacy Rule** | **Legal Authority** |
| 1. |  | Collection |  |
| 2. |  | Use |  |
| 3. |  | Disclosure |  |

### 2.1.c. Other Parties’ Information Data Flow

|  |
| --- |
| **Personal Information Flow Table** |
|  | **Description /Purpose of Activity** | **Privacy Rule** | **Legal Authority** |
| 1. |  | Collection |  |
| 2. |  | Use |  |
| 3. |  | Disclosure |  |

## 2.2. Risk Mitigation Table

Complete the table(s) below. Describe the risk and the mitigation strategy. Use the terms ‘High’, ‘Med’ or ‘Low’ to rate the “Likelihood” and “Impact” of each risk. In cases where the risks are substantially different for the individuals whose personal information is in VIU’s custody or under its control, complete a table for each group. In cases where the risks are substantially similar or the same, complete only one table.

### 2.2.a. Risks to Student Personal Information Data

|  |
| --- |
| Risk Mitigation Table |
|  | Risk | Mitigation Strategy | Likelihood | Impact |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4. |  |  |  |  |
| 5. |  |  |  |  |
| 6. |  |  |  |  |
| 7. |  |  |  |  |

### 2.2.b. Risks to Employee Personal Information Data

|  |
| --- |
| Risk Mitigation Table |
|  | Risk | Mitigation Strategy | Likelihood | Impact |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4. |  |  |  |  |
| 5. |  |  |  |  |
| 6. |  |  |  |  |
| 7. |  |  |  |  |
| 8. |  |  |  |  |

### 2.2.c. Risks to Other Parties’ Personal Information Data

|  |
| --- |
| Risk Mitigation Table |
|  | Risk | Mitigation Strategy | Likelihood | Impact |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4. |  |  |  |  |
| 5. |  |  |  |  |
| 6. |  |  |  |  |
| 7. |  |  |  |  |
| 8. |  |  |  |  |

## 2.3. Collection Notice

In order to allow individuals the ability to exercise their information rights with knowledge of how their information will be used, they must be notified at or prior to the time of collection. Section 27(2) of the Act requires that the individual from whom personal information is collect be told: a) the purpose for collecting it, b) the legal authority for collecting it, and c) the title, business address and business telephone number of an officer or employee of VIU who can answer the individual’s questions about the collection.

Describe below how and when notice will be given to individuals. Include the specific collection notice(s) that will be used.

### 2.3.a. Student Personal Information Collection Notice

|  |
| --- |
|  |

### 2.3.b. Employee Personal Information Collection Notice

|  |
| --- |
|  |

### 2.3.c. Other Parties’ Personal Information Collection Notice

|  |
| --- |
|  |

# PART 3 – SECURITY OF PERSONAL INFORMATION

Describe below the specific measures that will be used to protect the personal information from unauthorized collection, access, use, disclosure, retention and disposal. See Schedule C for a list of common types of security measures.

## 3.1. Security Measures

### 3.1.a. Physical Security Measures

|  |
| --- |
|  |

### 3.1.b. Technical Security Measures

|  |
| --- |
|  |

### 3.1.c. Security Policies, Procedures and Standards

|  |
| --- |
|  |

# PART 4 – ACCURACY, CORRECTION AND RETENTION OF PERSONAL INFORMATION

## 4.1. Updating and Correcting Personal Information

Describe here, if applicable, the procedure to allow individuals to routinely update or correct their personal information using regular channels (e.g., a student uses the SRS to update a home address or telephone number, an employee uses the HIS system to update emergency contact information, etc.)

|  |
| --- |
|  |

## 4.2. Decisions That Directly Affect an Individual

Describe here, if applicable, how the information will be used to make decisions that directly affect an individual.

|  |
| --- |
|  |

# PART 5 – FURTHER INFORMATION

## 5.1. Systematic Disclosures of Personal Information

Describe here, if applicable, any usual disclosures inside the University between the office with primary responsibility for the personal information and other VIU departments and programs. Also, describe any usual disclosures outside the University between VIU and another public or private body (e.g., provincial, territorial or federal government ministry, department or agency; university or college, transit authority; law enforcement agency).

If VIU and one or more other parties have signed an Information Sharing Agreement, include a copy with this completed PIA. An Information Sharing Agreement sets terms and conditions on the collection, use, disclosure and protection of personal information by the parties to the agreement.

|  |
| --- |
|  |

Access for Research or Statistical Purposes

Describe here, if applicable, any usual disclosures of the personal information made by your department for a research purpose, including statistical research, and how you comply with Section 35 of the Act.

|  |
| --- |
|  |

# PART 6 – INFORMATION AND PRIVACY COMMENTS

## 6.1. Information or Materials Reviewed

The Privacy Officer will describe here any additional resources and authorities consulted when reviewing and commenting on the completed PIA.

|  |
| --- |
| I have reviewed and considered: |

## 6.2. Conditions of Approval

The Information and Privacy Coordinator will describe here any recommended conditions to be considered by the Privacy Officer with delegated decision-making authority under the Act, who approves the completed PIA.

|  |
| --- |
| Recommended Conditions: |
| 1. |  |
| 2. |  |
| 3. |  |
| 4. |  |

# PART 7 – APPROVAL AND SIGNATURES

The undersigned confirm that they have taken reasonable steps to confirm the contents of the PIA are accurate and complete.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Bill Boyte*  |  |  |  |  |
| *VIU Privacy Officer*  |  | Signature |  | Date |
| *Insert Name* |  |  |  |  |
| *Insert position title* of Program Manager (if applicable) |  | Signature |  | Date |
| *Insert Name* |  |  |  |  |
| *Insert position title* of Project Manager, Information Technology Services (if applicable) |  | Signature |  | Date |

SCHEDULE A

**Definition of Terms**

|  |  |
| --- | --- |
| **Access** | Disclosure of personal information by the provision of access to personal information. |
| **Anonymize** | Present the results of a process in such a way that individuals whose personal information is contained in the records cannot be identified, and no linkages can be made between any personal information found in the records and personal information that is publicly available from other sources.  |
| **Authorized access** | Occurs when a person has access to personal information in the custody or control of the University that is authorized by the Act. |
| **Consistent purpose** | A use of personal information is consistent with the purpose for which the information was obtained or compiled if the use:1. has a reasonable and direct connection to that purpose, and
2. is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.
 |
| **Contact information** | Information that enables an individual at a place of business to be contacted; includes name, position title, business telephone number, business address, business email or business fax number of the individual. |
| **Data linking** | **T**he linking or combining of personal information in one source with personal information in one or more other sources if the purpose of the linking or combining is different from:1. the purpose for which the information in each database was originally obtained or compiled, and
2. every purpose that is consistent with each purpose referred to in paragraph (a).
 |
| **Disclose** | Reveal, show, expose, provide copies of, sell, give or tell.VIU may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3 of the Act. |
| **Employee** | A person employed for wages or salary by the University. In relation to VIU, includes: (a) a volunteer and (b) a service provider (see also the definitions for each of the latter terms). |
| **Individual identifier** | Information that would enable a third party to deduce the identity of the person concerned; examples include a person’s name, Social Insurance Number, student number, employee number, address, date of birth (usually used in combination with other identifiers). |

|  |  |
| --- | --- |
| **Instructor** | Individuals responsible for the teaching of credit and non-credit courses including professors, associate professors, assistant professors, professors emeritus, adjunct professors, visiting faculty, practitioner faculty, post-retirement appointees, lecturers, instructors, teaching assistants, tutors and markers, faculty associates, in-service associates, associate members and program coordinators. |
| **Personal information** | Recorded information about an identifiable individual, other than business contact information, including but not limited to:1. names, home addresses and telephone numbers;
2. age;
3. sex;
4. marital or family status;
5. identifying number;
6. race, national or ethnic origin;
7. colour;
8. religious or political beliefs or associations;
9. educational history;
10. medical history;
11. disabilities;
12. blood type;
13. employment history;
14. financial history;
15. criminal history;
16. images;
17. anyone else's opinions about an individual;
18. an individual's personal views or opinions; and,
19. name, address and phone number of parent, guardian, spouse or next of kin.
 |
| **Record** | Includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records. |
| **Service provider** | A person retained under contract to perform services for VIU or a person with whom an employee automatically enters into an agreement by virtue of using their product or service and in so doing accepts the service provider’s terms of use. |
| **Unauthorized collection, use, disclosure and disposal** | Occurs when a person who has access, whether authorized or unauthorized, to personal information in the custody or control of the University, collects, uses, discloses and disposes of that information and it is not authorized by the Act. |
| **Use** | Employ information to accomplish a specific purpose.  |
| **Volunteer** | A person who provides a service to the University without being paid. |