



Education Practicum Tracking Privacy Impact Assessment

| | |
|------------------------|---|
| Project Code | PC0667 |
| Submission Date | February 20, 2017 |
| Organization | University of Victoria |
| Unit and Service Owner | Dr. Leslee Francis-Pelton, Chair of the Department of Curriculum and Instruction, Faculty of Education |
| Contact | Jennifer Cara <i>Project Coordinator - University Systems</i> 250-721-6380 jcara@uvic.ca |
| Reviewed By | Garry Sagert, Director, UVON |
| Review Date | [[Date of review – can be filled in by PMO or Reviewer]] |

1.0 Privacy Context

1.1 Description of Systems and Linkage to Legislation

This project aims to adapt the HSD Practicum Tracking platform, to assist the Faculty of Education with practicum data tracking and storage, while improving information security by leveraging existing knowledge bases, such as Banner, to reduce data input errors and duplication. This system, a variation of which is currently in use by HSD, will be used to enter contact and other information about schools, mentors, Practicums, Students, and Supervisors, in order to coordinate the assignment of student teachers to schools for practicums.

FIPPA implications include collection and storage of personal information about practicum students, potentially sensitive information, who has access to that information, and what that information is used for.

1.2 Use of System

This system, a variation of which is currently in use by HSD, will be used to enter information about schools, mentors, Practicums, Students, and Supervisors, in order to coordinate the assignment of student teachers to schools for practicums. Currently this information is stored in

Sec. 15 [REDACTED] which is cumbersome and prone to human error. Practicum Coordinators in the Faculty of Education will enter information in an Apex Application

- Student Information
- Practicum Placements
- Placement Information
- Schools Information
- Mentors (Create, Edit)
- Supervisors
- Ability to view One Card photos of students (when photos exist) in their profiles in the database, automatically pulled from Banner

1.3 Custody and Control

The records below will be accessed by the application. All data is stored at the UVic datacentre. Only the Practicum coordinators at UVic have access to the platform. Access to the Practicum Application is set up by an Administrator, is unique to each coordinator and not shared, and access will be removed immediately when it is determined that an individual no longer requires access. All practicum coordinators have access to all data.

For Manual entry fields, the Administrative Authority is creating a policy to determine what information may or may not be entered into these fields, to avoid unnecessary privacy intrusion (for example no medical information in the case of a withdrawal for medical reasons).

For document uploads, there is a criminal record check document required to be attached to a student record, because a student is required to provide one in order to work in the education system. This document is highly confidential. Only Practicum coordinators have access to this data. There is no set retention period currently in place.



Education Practicum Tracking Privacy Impact Assessment

| | |
|------------------------|---|
| Project Code | PC0667 |
| Submission Date | February 20, 2017 |
| Organization | University of Victoria |
| Unit and Service Owner | Dr. Leslee Francis-Pelton, Chair of the Department of Curriculum and Instruction, Faculty of Education |
| Contact | Jennifer Cara <i>Project Coordinator - University Systems</i> 250-721-6380 jcara@uvic.ca |
| Reviewed By | Garry Sagert, Director, UVON |
| Review Date | [[Date of review – can be filled in by PMO or Reviewer]] |

1.0 Privacy Context

1.1 Description of Systems and Linkage to Legislation

This project aims to adapt the HSD Practicum Tracking platform, to assist the Faculty of Education with practicum data tracking and storage, while improving information security by leveraging existing knowledge bases, such as Banner, to reduce data input errors and duplication. This system, a variation of which is currently in use by HSD, will be used to enter contact and other information about schools, mentors, Practicums, Students, and Supervisors, in order to coordinate the assignment of student teachers to schools for practicums.

FIPPA implications include collection and storage of personal information about practicum students, potentially sensitive information, who has access to that information, and what that information is used for.

1.2 Use of System

This system, a variation of which is currently in use by HSD, will be used to enter information about schools, mentors, Practicums, Students, and Supervisors, in order to coordinate the assignment of student teachers to schools for practicums. Currently this information is stored in

Sec. 15 [REDACTED] which is cumbersome and prone to human error. Practicum Coordinators in the Faculty of Education will enter information in an Apex Application

- Student Information
- Practicum Placements
- Placement Information
- Schools Information
- Mentors (Create, Edit)
- Supervisors
- Ability to view One Card photos of students (when photos exist) in their profiles in the database, automatically pulled from Banner

1.3 Custody and Control

The records below will be accessed by the application. All data is stored at the UVic datacentre. Only the Practicum coordinators at UVic have access to the platform. Access to the Practicum Application is set up by an Administrator, is unique to each coordinator and not shared, and access will be removed immediately when it is determined that an individual no longer requires access. All practicum coordinators have access to all data.

For Manual entry fields, the Administrative Authority is creating a policy to determine what information may or may not be entered into these fields, to avoid unnecessary privacy intrusion (for example no medical information in the case of a withdrawal for medical reasons).

For document uploads, there is a criminal record check document required to be attached to a student record, because a student is required to provide one in order to work in the education system. This document is highly confidential. Only Practicum coordinators have access to this data. There is no set retention period currently in place.

1.4 Personally identifiable information Data Types and Information Flows
Information collected and accessed in the Practicum Application by Tab:

| | |
|-------------------------------------|---------------------|
| Student – Pulled From Banner | |
| First/Last Name | Confidential |
| V# | Confidential |
| Address | Confidential |
| Email | Confidential |
| Phone | Confidential |
| Netlink ID | Confidential |
| Date of Birth | Confidential |
| Year of Study | Confidential |
| Entry Term | Confidential |
| Academic Standing | Confidential |
| OneCard Photo | Confidential |
| DOCUMENTS: | |
| Criminal Record check Upload | Highly Confidential |
| Practicum Report | |
| Appeals documents | |

Manual Input:

| | |
|--------------------|----------|
| Schools | |
| District | Public |
| Name | Public |
| Level | Public |
| Address | Public |
| Website | Public |
| Contact names | Public |
| Contact phone | Public |
| Contact email | Public |
| Contact role | Public |
| Placements | Internal |
| Students | Internal |
| Affiliation status | Internal |
| Affiliation Expiry | Internal |
| Submission Date | Internal |

| | |
|----------------------|----------|
| Mentors | Internal |
| Notes - MANUAL ENTRY | Internal |

| | |
|----------------------|----------|
| Mentor | |
| Name | Internal |
| Email | Internal |
| Role | Internal |
| Phone | Internal |
| Status | Internal |
| Status Date | Internal |
| Associated School | Internal |
| Placements | Internal |
| Supervised Students | Internal |
| Notes - MANUAL Entry | |

| | |
|---------------------------|--------------|
| Practicum: INPUT | |
| School Name | Internal |
| Level of School | Internal |
| Year/Term dates | Internal |
| Students in placement | Internal |
| Student Mentor | Internal |
| Placement Status | Confidential |
| Number of visits required | Confidential |
| Notes - MANUAL ENTRY | Confidential |

| | |
|-------------------------|--------------|
| Input | |
| Status | Confidential |
| Status Dates | Confidential |
| Teaching Area | Internal |
| Active term/course/year | Internal |
| Cohort | Internal |
| Coordinator | Internal |
| CRC Status | Confidential |
| CRC Expiry | Confidential |
| Waiver Complete | Internal |
| TFI Scores | Confidential |
| | |
| Flags: | |

| | |
|---------------------------------------|--------------|
| Complete Course Work Y/N | Confidential |
| Practicum Denied | Confidential |
| Required/voluntary/medical/withdrawal | Confidential |
| Extenuating Circumstance | Confidential |
| Other Notes - MANUAL Entry | |
| Notes - MANUAL Entry | |
| Practicums Taken | Internal |

| | |
|-------------------|--------------|
| Supervisor | |
| Report download | Confidential |
| Name | Internal |
| Email | Internal |
| Role | Internal |
| Phone | Internal |

When a student requires a practicum, the Practicum Coordinators look at what schools, mentors, supervisors, etc are available, and assign a student to whatever combination is the best fit. The Coordinators coordinate with students, Supervisors, schools and mentors via telephone and/or email, outside of this application. Only the Practicum coordinators have access to the platform. Various reports can be run as part of this application, and exported to .csv or excel. Notes can be manually entered and documents manually attached to various tabs as noted above.

The Students Tab is populated with information pulled from Banner, including OneCard photo if available.

2.0 Privacy Threshold Analysis

| | | | | | | | | | | |
|---------------------|---|---|---|--------------|--|----------|--|------------|--|--|
| 1 | Has a Privacy Impact Assessment ever been performed for this project or program? | N | | | | | | | | |
| 2 | <p>What is the information classification level of information collected, maintained, or shared in any identifiable form as part of this project or service? Select all classification levels that apply. See University Policy IM7800 for detailed definitions.</p> <p><input checked="" type="checkbox"/> Highly Confidential <input checked="" type="checkbox"/> Confidential <input checked="" type="checkbox"/> Internal <input type="checkbox"/> Public <input type="checkbox"/> Don't Know <input type="checkbox"/> Information is not collected, maintained, or shared in any identifiable form as part of this project or service</p> | | | | | | | | | |
| 3 | <p>What are the type(s) of personal, critical, or sensitive information collected, maintained, or shared by this project? Please be specific about the data elements.</p> <p><i>Examples include, but are not limited to information about students, employees, donors, alumni, credit cards, health information, etc. See Appendix A of University Policy IM7800 for more examples.</i></p> <table border="1" data-bbox="293 1066 1414 1381"> <tr> <td data-bbox="293 1066 532 1129">Highly Confidential</td> <td data-bbox="532 1066 1414 1129"> <ul style="list-style-type: none"> Criminal record Check </td> </tr> <tr> <td data-bbox="293 1129 532 1203">Confidential</td> <td data-bbox="532 1129 1414 1203">Photo, Biographical student data (name, address, phone number, email),</td> </tr> <tr> <td data-bbox="293 1203 532 1350">Internal</td> <td data-bbox="532 1203 1414 1350">Practicum registration and success information (pass/fail), will all be pulled from Banner. Practicum placement information (agency, supervisor, mentor, position, skills required) will be maintained in this system.</td> </tr> <tr> <td data-bbox="293 1350 532 1381">Don't Know</td> <td data-bbox="532 1350 1414 1381"> <ul style="list-style-type: none"> </td> </tr> </table> | Highly Confidential | <ul style="list-style-type: none"> Criminal record Check | Confidential | Photo, Biographical student data (name, address, phone number, email), | Internal | Practicum registration and success information (pass/fail), will all be pulled from Banner. Practicum placement information (agency, supervisor, mentor, position, skills required) will be maintained in this system. | Don't Know | <ul style="list-style-type: none"> | |
| Highly Confidential | <ul style="list-style-type: none"> Criminal record Check | | | | | | | | | |
| Confidential | Photo, Biographical student data (name, address, phone number, email), | | | | | | | | | |
| Internal | Practicum registration and success information (pass/fail), will all be pulled from Banner. Practicum placement information (agency, supervisor, mentor, position, skills required) will be maintained in this system. | | | | | | | | | |
| Don't Know | <ul style="list-style-type: none"> | | | | | | | | | |
| 4 | Does this project or program involve the implementation of a new electronic system or use of a new application/ software to support the creation, collection, storing, backing-up or disposition of personal, sensitive, or critical information? | [Existing] , existing PII from Banner will be used within this system with additional internal information (placement details) stored against a student's record. | | | | | | | | |

| | | |
|----|--|---|
| 5 | <p>Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?</p> <p>[[If so, what are those technologies? Examples include, but are not limited to, cloud platforms Sec. 15 social media, mobile applications, smart cards, RFID, biometrics, locator technologies, visual surveillance, video recording, profiling, data mining, etc.]]</p> | N |
| 6 | <p>Will the project involve the collection or creation of new information about individuals?</p> <p>[[If so, what information?]]</p> | N (information currently tracked using Sec. 15) |
| 7 | <p>Will personal information about individuals or sensitive/critical information be disclosed to organizations, programs, processes or people who have not previously had routine access to the information?</p> <p>[[If so, which organizations, processes or people?]]</p> | N |
| 8 | <p>Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?</p> <p>[[If so, how?]]</p> | N (information currently tracked using Sec. 15) |
| 9 | <p>Will the project collect, use, or disclose PII or sensitive/critical information for research purposes?</p> <p>[[If so, do you have appropriate research approvals (e.g. ethics)?]]</p> | N |
| 10 | <p>Will the project require that individuals are contacted in ways that they may perceive to be intrusive?</p> <p>[[If so, how may they perceive it to be intrusive?]]</p> | N |
| 11 | <p>Is any of the information owned by another organization?</p> <p>[[If so, which organization(s)?]]</p> | N |
| 12 | <p>Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?</p> <p>[[If so, which ones?]]</p> | N |
| 13 | <p>Does this project collect, access or use Social Insurance Numbers (SIN)?</p> | N |
| 14 | <p>How many user records containing PII or sensitive/critical information will be stored, accessed or used? [1-1000],[1001-5000],[5,001-50,000],[50,001-100,000],[100,000+]</p> | Sec. 15 |
| 15 | <p>Where will the information be stored?</p> <p>UVic Data Centre</p> | |
| 16 | <p>Will a third party (e.g. vendor or service provider) have access to the information?</p> | N |

| | | |
|-----------|--|------------|
| | [[If so, which third parties?]] | |
| 17 | Is any of the information being accessed from outside of Canada? <input type="text" value="[[If so, by whom and from where?]]"/> | N |
| 18 | Does the IT system connect, receive, or share information in identifiable form, or PII or sensitive/critical information with any other IT systems? <input type="text" value="[[If so, which ones?]]"/> Examples include, but are not limited to: <ol style="list-style-type: none"> 1. Personal information is used in a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled). 2. Personal information is used in a system that has connections to at least one other system. 3. Personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed. 4. Personal information is transmitted using wireless technologies.]] | 1 |
| 19 | If there is external sharing, is it pursuant to new or existing information sharing agreements? <input type="text" value="[[List these agreements]]"/> | N/A |

3.0 Privacy & Security Risks

| ID | Risk Description | Probability (1-5) | Impact (1-5) | Risk Mitigation Measures (reduce probability and/or impact) |
|----|--|----------------------|-----------------|---|
| 1 | Lack of legal authority to collection, use or disclose PII | 1 | 4 | <p>Data is collected for the sole purpose of setting up practicums and communicating with participants. Participants agree to disclosure of data for this purpose. Existing system has been performing this function for several years.</p> <p>GV0235 Protection of Privacy Policy, section(s) 18.00, 19.00</p> |
| 2 | Unauthorized collection of PII by authorized individuals/processes/systems | 1 | 3 | <p>Data is collected for the sole purpose of setting up practicums and communicating with participants.</p> <p>AP-2 Purpose Specification</p> <p>The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 16.00, 17.00</p> <p>AC-21 Information Sharing</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required and Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. <p>Response:</p> <ul style="list-style-type: none"> See AC-20 |
| 3 | Excessive collection of PII by authorized individuals/processes/systems | 1 | 2 | <p>Only information required for administration of practicums is collected and stored.</p> <p>DM-1 Minimization of Personally Identifiable Information</p> |

| | | | | |
|---|--|---|---|--|
| | | | <p>Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;</p> <p>Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 19.00</p> <p>AC-21 Information Sharing</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required and Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. <p>Response:</p> <ul style="list-style-type: none"> See AC-20 | |
| 4 | Inappropriate or unauthorized use of PII by authorized individuals/processes/systems | 1 | 4 | <p>EDEC agrees to set policies regarding what highly sensitive personal data can be entered in Notes fields. Data will only be used for Practicum administration and communication thereof.</p> <p>UL-1 Internal Use</p> <p>The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00</p> <p>PL-4 Rules of Behavior</p> <p>Control:</p> <ul style="list-style-type: none"> Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; Reviews and updates the rules of behavior; and |

| | | | | |
|---|--|---|---|---|
| | | | | <ul style="list-style-type: none"> Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated <p>Response:</p> <ul style="list-style-type: none"> See AC-8, CM-10 <p>AC-21 Information Sharing</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required and Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. <p>Response:</p> <ul style="list-style-type: none"> See AC-20 |
| 5 | Unauthorized disclosure by individuals/processes/systems | 1 | 4 | <p>Data is collected for the sole purpose of setting up practicums and communicating with participants. Participants agree to the collection of data for this purpose. Only authorized users have access to the application, controlled by an administrator will de-provision users in a timely manner.</p> <p>UL-1 Internal Use</p> <p>The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00</p> <p>AC-4 Information Flow Enforcement</p> <p>Control:</p> <p>The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.</p> <p>Response:</p> <ul style="list-style-type: none"> See SC-7 <p>IA-2 Identification and Authentication (organizational Users)</p> |

| | | | | |
|---|---|---|---|--|
| | | | | <p>Control:</p> <ul style="list-style-type: none"> The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). <p>Response:</p> <ul style="list-style-type: none"> See SC-8 <p>AC-21 Information Sharing</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required and Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. <p>Response:</p> <ul style="list-style-type: none"> See AC-20 |
| 6 | Creation of new PII by data matching | 1 | 3 | No new PII or data matching is created within this project. |
| 7 | Unauthorized tracking of individuals through transaction monitoring | 1 | 1 | No unauthorized tracking of individuals occurs as a result of this project. The current process is not changing, no new data is being collected. Participants agree to collection of data to participate in a practicum. |
| 8 | Data stored outside of Canada and in the public cloud | 1 | 1 | All Data is stored at the Uvic Data centre |
| 9 | Data retention beyond prescribed timeline | 4 | 1 | <p>There is currently no prescribed timeline for data retention. EDUC will set timelines if required.</p> <p>SI-12 Information Handling and Retention</p> <p>Control:</p> <ul style="list-style-type: none"> The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements <p>Response:</p> <ul style="list-style-type: none"> Use policy slates that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines |

| | | | | |
|----|--|---|---|---|
| | | | | http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf |
| 10 | Risk of increased surveillance | 1 | 1 | There is no surveillance as part of this functionality, monitoring only occurs as part of the existing practicum process – Participants attend practicums, and the administrators are advised if the practicum is successfully completed. |
| 11 | Unauthorized use as a records repository | 4 | 1 | <p>There is currently no prescribed timeline for data retention. EDUC will set timelines if required.</p> <p>SI-12 Information Handling and Retention</p> <p>Control:</p> <ul style="list-style-type: none"> The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements <p>Response:</p> <ul style="list-style-type: none"> Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf |
| 12 | Public perception | 1 | 1 | The implementation of the new system will only be visible to Practicum Administrators, no external parties will have access to it. Practicum tracking and administration will continue to the campus the same as it does today, but more securely. |
| 13 | Use of existing PII data in a new system or business process | 5 | 1 | <p>A new application is being implemented, but will maintain existing work and dataflows, and will not be utilized by any users who do not use the existing system/process. The system does not connect to any external process, just Banner.</p> <p>PL-4 Rules of Behavior</p> <p>Control:</p> <ul style="list-style-type: none"> Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; Reviews and updates the rules of behavior; and Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated |

| | | | |
|--|--|--|---|
| | | | <p>Response:</p> <ul style="list-style-type: none"> • See AC-8, CM-10 <p>UL-1 Internal Use</p> <p>The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00</p> <p>AC-4 Information Flow Enforcement</p> <p>Control:</p> <p>The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.</p> <p>Response:</p> <ul style="list-style-type: none"> • See SC-7 <p>IA-2 Identification and Authentication (organizational Users)</p> <p>Control:</p> <ul style="list-style-type: none"> • The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). <p>Response:</p> <ul style="list-style-type: none"> • See SC-8 <p>System Interconnections</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> • Authorizes connections from the information system to other information systems through the use of interconnection Security Agreements; • Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and • Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]. |
|--|--|--|---|

Consultation Checklist

IT Projects

The following leaders in each functional area can refer you to an appropriate subject matter expert to help develop the technical elements of your project plan and ensure it is complete.

| Service Area | Impact? (Y/N) | Leader | Expert Consulted | Date of Consultation |
|----------------------------------|------------------|---------------------|------------------|----------------------|
| Office of the CIO | Y | Wency Lum | | |
| Systems General Office | | Trish Kearley | | |
| Client Technologies | | Lance Grant | | |
| Desktop Support Services | | David Street | | |
| Computer Help Desk | | Marcus Greenshields | | |
| Academic & Admin Services | | Nav Bassi | | |
| Client Account Managers | | Garry Sagert | | |
| Production and Technical Support | | Scott Thompson | | |
| Development Services | | Dave Wolowicz | | |
| Identity Services | | Corey Scholefield | | |
| UVic Online | Y | Garry Sagert | | |
| Data Centre Services | | Kim Lewall | | |
| Network Services | | Jane Godfrey | | |
| Infrastructure Services | | Ron Kozsan | | |
| Information Security Office | | Lance Grant | | |
| Project Management Office | | Chandra Beaveridge | | |

Sponsor

The project sponsor or system owner must be consulted in the creation of the Privacy Impact Assessment. Use this table to document consultation with the project sponsor or service owner.

| Name | Comments | Date of Consultation |
|---|--|----------------------|
| Leslee Francis-Pelton – EDUC Administrative Authority | Meeting to discuss data elements and privacy level | Dec 12/2016 |
| Kerry Robertson - EDUC | Meeting to discuss data elements and privacy level | Dec12/2016 |

Other Projects

[[Please include a table like the above for any other subject matter experts that you believe should provide input for this PIA.]]

| Department/Unit | Leader | Expert Consulted | Date of Consultation |
|-----------------|--------|------------------|----------------------|
| | | | |

Revision History

[[As the PIA is distributed between the sponsor, stakeholders, and SMEs, update this table to indicate changes between document versions.]]

| Version | Date | Author | Comments |
|---------|------|--------|----------|
| | | | |

Appendix A – Privacy Controls

| ID | PRIVACY CONTROLS |
|------|---|
| AP | Authority and Purpose |
| AP-1 | <p>Authority to Collect</p> <p>The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.</p> <p>Response:</p> <p>GV0235 Protection of Privacy Policy, section(s) 18.00, 19.00</p> |
| AP-2 | <p>Purpose Specification</p> <p>The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 16.00, 17.00</p> |
| DM | Data Minimization and Retention |
| DM-1 | <p>Minimization of Personally Identifiable Information</p> <p>Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 19.00</p> |
| DM-2 | <p>Data Retention and Disposal</p> <p>Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 20.00, 25.00</p> |
| DM-3 | <p>Minimization of PII Used in Testing, Training, and Research</p> <p>Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and Implements controls to protect PII used for testing, training, and research</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 20.00, 21.00, 22.00</p> |
| IP | Individual Participation and Redress |

| ID | PRIVACY CONTROLS |
|------|---|
| IP-1 | <p>Consent</p> <p>Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 18.00</p> |
| IP-2 | <p>Individual Access</p> <p>Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 29.00, 32.00</p> |
| IP-3 | <p>Redress</p> <p>Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 30.00, 31.00, 33.00</p> |
| IP-4 | <p>Complaint Management</p> <p>The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 34.00</p> |
| SE | <p>Security</p> |
| SE-1 | <p>Inventory of Personally Identifiable Information</p> <p>Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.</p> |

| ID | PRIVACY CONTROLS |
|------|---|
| SE-2 | <p>Privacy Incident Response</p> <p>Develops and implements a Privacy Incident Response Plan; and Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, Procedures for responding to a Privacy Incident or Privacy Breach</p> |
| UL | Use Limitation |
| UL-1 | <p>Internal Use</p> <p>The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00</p> |
| UL-2 | <p>Information Sharing with Third Parties</p> <p>Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.</p> <p>Control(s) / Compliance:</p> <p>GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00,</p> |

Appendix B – Security Controls

| ID | SECURITY CONTROLS |
|------|---|
| AC-2 | <p>Account Management</p> <p>Control:</p> <ul style="list-style-type: none"> • Identifies and selects the following types of information system accounts to support organizational missions/business functions: organization-defined information system account types; • Assigns account managers for information system accounts; • Establishes conditions for group and role membership; • Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; • Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; • Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions; • Monitors the use of information system accounts; • Notifies account managers: <ul style="list-style-type: none"> • When accounts are no longer required; • When users are terminated or transferred; and • When individual information system usage or need-to-know changes; • Authorizes access to the information system based on: <ul style="list-style-type: none"> • A valid access authorization; • Intended system usage; and • Other attributes as required by the organization or associated missions/business functions; • Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and • Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. <p>Response:</p> <ul style="list-style-type: none"> • Account Management is governed by the following institutional policies and procedures: <ul style="list-style-type: none"> • IM7200 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf • Account Management is subject to the operating procedures and processes of the University. <p>[[Add additional relevant information as required.]]</p> |
| AC-3 | <p>Access Enforcement</p> <p>Control:</p> <ul style="list-style-type: none"> • The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. <p>Response:</p> <ul style="list-style-type: none"> • See AC-4, SC-7 <p>[[Add additional relevant information as required.]]</p> |

| ID | SECURITY CONTROLS |
|-------|--|
| AC-4 | <p>Information Flow Enforcement</p> <p>Control:</p> <p>The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies.</p> <p>Response:</p> <ul style="list-style-type: none"> • See SC-7 <p>[[Add additional relevant information as required.]]</p> |
| AC-8 | <p>System Use Notification</p> <p>Control:</p> <p>Displays to users an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.</p> <p>Response:</p> <ul style="list-style-type: none"> • Organization-defined systems use policy will: <ul style="list-style-type: none"> • Primarily positive and explanatory (and not just a list of “don’ts”). • Encourage usage by providing positive examples and suggestions. • Require that content be office-appropriate. • Require that personally identifiable information is not used. • Include links to University of Victoria policies and training resources • Organization-defined systems use policy will include reference to and compliance with: <ul style="list-style-type: none"> • IM700 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf • GV0235 – Protection of Privacy http://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf • IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf • Canadian Copyright Act http://www.canlii.org/en/ca/laws/slat/rsc-1985-c-c-42/latest/rsc-1985-c-c-42.html <p>[[Add additional relevant information as required.]]</p> |
| AC-19 | <p>Access Control for Mobile Devices</p> <p>Control:</p> <ul style="list-style-type: none"> • Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and • Authorizes the connection of mobile devices to organizational information systems <p>Response:</p> <ul style="list-style-type: none"> • University of Victoria recommends for all users and requires for Exchange users the use of: <ul style="list-style-type: none"> • Sec. 15 • [Redacted] • [Redacted] <p>[[Add additional relevant information as required.]]</p> |

| ID | SECURITY CONTROLS |
|-------|---|
| AC-20 | <p>Use of External Information Systems</p> <p>Control:</p> <ul style="list-style-type: none"> The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: <ul style="list-style-type: none"> Access the information system from external information systems; and Process, store, or transmit organization-controlled information using external information systems. <p>Response:</p> <ul style="list-style-type: none"> See CP-9, PE-3, SC-7, SI-8 <p>[[Add additional relevant information as required.]]</p> |
| AC-21 | <p>Information Sharing</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required and Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. <p>Response:</p> <ul style="list-style-type: none"> See AC-20 <p>[[Add additional relevant information as required.]]</p> |
| AC-22 | <p>Publicly Accessible Content</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Designates individuals authorized to post information onto a publicly accessible information system; Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered. <p>Response:</p> <ul style="list-style-type: none"> See AC-4, AC-21, IA-2, IA-8 <p>[[Add additional relevant information as required.]]</p> |
| AT-2 | <p>Security Awareness Training</p> <p>Control:</p> <ul style="list-style-type: none"> The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): <ul style="list-style-type: none"> As part of initial training for new users; When required by information system changes; and |

| ID | SECURITY CONTROLS |
|------|---|
| | <ul style="list-style-type: none"> Organization-defined frequency thereafter. <p>Response:</p> <ul style="list-style-type: none"> Privacy training will be required for new users to ensure compliance with FIPPA. <p>[[Add additional relevant information as required.]]</p> |
| AU-6 | <p>Audit Review, Analysis, and Reporting</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Reviews and analyzes information system audit records for indications of defined inappropriate or unusual activity. Reports findings to the Chief Privacy Officer and Chief Information Officer <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| CA-3 | <p>System Interconnections</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Authorizes connections from the information system to other information systems through the use of interconnection Security Agreements; Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]. <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| CM-3 | <p>Configuration Change Control</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> Determines the types of changes to the information system that are configuration-controlled; Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; Documents configuration change decisions associated with the information system; Implements approved configuration-controlled changes to the information system; Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; Audits and reviews activities associated with configuration-controlled changes to the information system; and Coordinates and provides oversight for configuration change control activities through the: organization-defined configuration change control that convenes organization-defined configuration change conditions. <p>Response:</p> <ul style="list-style-type: none"> System configuration settings and changes are managed using the University systems Change Management processes and Change Advisory Board (CAB). <p>[[Add additional relevant information as required.]]</p> |

| ID | SECURITY CONTROLS |
|-------|---|
| CM-8 | <p>Information System Component Inventory</p> <p>Control:</p> <ul style="list-style-type: none"> • Develops and documents an inventory of information system components that: <ul style="list-style-type: none"> • Accurately reflects the current information system; • Includes all components within the authorization boundary of the information system; • Is at the level of granularity deemed necessary for tracking and reporting; and • Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and • Reviews and updates the information system component inventory. <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| CM-10 | <p>Software Usage Restrictions</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> • Uses software and associated documentation in accordance with contract agreements and copyright laws; • Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and • Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| CP-2 | <p>Contingency Plan</p> <p>Control:</p> <p>The organization develops a contingency plan for the information system.</p> <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| CP-9 | <p>Information System Backup</p> <p>Control:</p> <p>Conducts backups of user-level information contained in the information system. Conducts backups of system-level information contained in the information system. Conducts backups of information system documentation including security-related documentation; and Protects the confidentiality, integrity, and availability of backup information at storage locations.</p> <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| IA-2 | <p>Identification and Authentication (organizational Users)</p> <p>Control:</p> <ul style="list-style-type: none"> • The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). |

| ID | SECURITY CONTROLS |
|------|--|
| | <p>Response:</p> <ul style="list-style-type: none"> • See SC-8 <p>[[Add additional relevant information as required.]]</p> |
| IA-8 | <p>Identification and Authentication (non-organizational users)</p> <p>Control:</p> <ul style="list-style-type: none"> • The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). <p>Response:</p> <ul style="list-style-type: none"> • See SC-8 <p>[[Add additional relevant information as required.]]</p> |
| MP-2 | <p>Media Access</p> <p>Control:</p> <ul style="list-style-type: none"> • The organization restricts access to organization-defined types of digital and/or non-digital media] to personnel or roles. <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| PE-3 | <p>Physical Access Control</p> <p>Control:</p> <ul style="list-style-type: none"> • Enforces physical access authorizations, controls and audits exist. <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| PL-4 | <p>Rules of Behavior</p> <p>Control:</p> <ul style="list-style-type: none"> • Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; • Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; • Reviews and updates the rules of behavior; and • Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated <p>Response:</p> <ul style="list-style-type: none"> • See AC-8, CM-10 <p>[[Add additional relevant information as required.]]</p> |

| ID | SECURITY CONTROLS |
|-------|---|
| RA-3 | <p>Risk Assessment</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> • Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; • Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; • Reviews risk assessment results [Assignment: organization-defined frequency]; • Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and • Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. <p>Response:</p> <ul style="list-style-type: none"> • See sections 1.4 and 3.0 of this document. <p>[[Add additional relevant information as required.]]</p> |
| SC-7 | <p>Boundary Protection</p> <p>Control:</p> <ul style="list-style-type: none"> • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; • Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| SC-8 | <p>Transmission Confidentially and Integrity</p> <p>Control:</p> <ul style="list-style-type: none"> • The information system protects the confidentiality and; integrity of transmitted information. <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| SI-8 | <p>SPAM Protection</p> <p>Control:</p> <p>The organization:</p> <ul style="list-style-type: none"> • Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and • Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures <p>Response:</p> <p>[[Add additional relevant information as required.]]</p> |
| SI-12 | <p>Information Handling and Retention</p> <p>Control:</p> |

| ID | SECURITY CONTROLS |
|----|--|
| | <ul style="list-style-type: none"> The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements <p>Response:</p> <ul style="list-style-type: none"> Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf <p>[[Add additional relevant information as required.]]</p> |