Privacy Impact Assessment for Non-Ministry Public Bodies

Use of MyEducation BC

Why do I need to do a PIA?
Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?
Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of School District:			
PIA Drafter:			
Email:		Phone:	
Program Manager:			
Email:		Phone:	

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

1. Description of the Initiative

The Ministry of Education, Boards of Education and Independent School authorities have collaborated to procure a common student information service for use by schools in British Columbia. The Ministry, on behalf of these parties, entered into a contract with **Fujitsu Consulting (Canada)** to provide MyEducation BC, a hosted, web-based service built upon the Follett Aspen SIS software.

MyEducation BC supports the operational needs of schools and school districts and is an important tool for delivering education services and monitoring student and school

performance. More specifically, MyEducation BC is a comprehensive student information service designed to:

- manage school and student information across the entire province;
- streamline the administrative processes used by schools;
- maintain a provincial student registry and electronic permanent student record; and
- prepare reports and data submissions for the Ministry.

The core functions of MyEducation BC include the management of student demographics, enrolment and attendance, programs and courses, student achievement, individual education and learning plans, and reports. A single record is maintained for each student which is available only to schools providing educational services to the student. In addition, students and parents will have the ability to access relevant student records and collaborate with teachers through a web-based portal. MyEducation BC is a strategic component of the BC Education Plan.

MyEducation BC replaces BCeSIS and participation in MyEducation BC is open to boards of education, independent schools and band schools in British Columbia (collectively referred to as "Districts") that have entered into a Memorandum of Understanding with the Ministry of Education. The service is also available to public schools in the Yukon under an inter-provincial agreement. Each member organization is represented on a Service Management Council that approves common business standards, protocols, and practices.

The service and data are housed in secure data centres in Kelowna and Regina. School staff, teachers, parents and students access MyEducation BC via a web browser using a server-side 128-bit SSL connection. Scope of record access is determined by user roles that are managed by districts.

Responsibility for privacy is jointly-held by the Ministry and the Districts. The Ministry, through a contract with its service provider, provides the shared application software and the infrastructure. The Districts are responsible for the collection, use, disclosure, accuracy and correction of personal student information. Audit logging is a service provided by Fujitsu and audit logs are available to the school districts. Established processes for monitoring access were established for BCeSIS and will be continued under MyEducation. School districts are responsible for monitoring access to their information and reporting breaches as set out in their own information management policies. Access requests for information contained in MyEducation are the responsibility of the school district under which the student is primarily enrolled.

2. Scope of this PIA

This PIA addresses the District's responsibilities for the information entered into the MyEducation system.

3. Related Privacy Impact Assessments

The Ministry of Education has completed a PIA regarding its own responsibilities pertaining to the MyEducation system. It is filed in the personal information directory as EDUC14025.

4. Elements of Information or Data

Schools and school districts collect personal information on students for the purpose of administering the delivery of education in schools, managing student safety, administering of the education system, complying with laws and regulations, conducting research and compiling statistics. The major information classes stored in MyEducation BC include:

- Student data including:
  - District and provincial ID numbers
  - Address
  - Emergency information
  - Birthday
  - Custody information
  - Release information
  - Physical and health information
  - Eligibility information
  - Field trip information
  - Photograph
  - Time table
  - Demographic information
  - Achievement and grading data
  - Languages
  - First Nation status
  - Citizenship status
  - Special Education/Individual Education Plans

- Student Learning Plans

- Class data including:
  - Roster
  - Teacher
- School data including:
  - Accident and injury data
  - Locker lists and assignments including lock combinations
  - Course information
  - Pupil-teacher contact data
  - Room and room assignment data
  - Home Room roster data
  - Transfer requests
  - Student roster data
  - Counselor roster
  - Sports team rosters
  - Family interview reports
- District data including:
  - Out of boundary data
  - Bus routes
  - Municipalities
  - Fees data
  - Meal program data
  - Enrollment data
  - Diploma and credit data
  - Attendance data
  - Co-op program data

The sensitivity of the personal information varies from very low to high.

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

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of 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

No student data is being stored outside of Canada. Production data for MyEducation BC is stored in a secure data centre in Kelowna and managed by the service provider, Fujitsu Consulting (Canada). A secondary data centre is maintained by Fujitsu Consulting (Canada) in Regina which is used for hosting training and support databases and is a backup site for disaster recovery purposes.

MyEducation BC is accessed via a web browser using server-side 128-bit SSL encryption. Public schools are connected to data centres through the Provincial Learning Network (SPANBC) and the Next Generation Network (NGN), managed by the province. Connections between data centres and service centres use dedicated circuits that are routed entirely through Canada.

School employees working from home, parents and students access MyEducation BC over the internet. All network traffic uses 128-bit SSL encryption.

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;	no
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 your privacy office(r) 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);	no
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.	

**** Please note: If your initiative involves a "data-linking initiative" or a "common or integrated program or activity", advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body's privacy office(r) to determine how to proceed with this notification and consultation.***

For future reference, public bodies are required to notify the OIPC of a" data-linking initiative" or a "common or integrated program or activity" in the early stages of developing the initiative, program or activity. Contact your public body's privacy office(r) to determine how to proceed with this notification.

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

Please complete the table below. Examples can be removed and additional lines added as needed. You may include a flow diagram as well for ease of explanation.

Privacy Impact Assessment for Non-Ministry Public Bodies

Use of MyEducation BC

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Information is collected directly from students and guardians for enrollment and the management of the student throughout their time in school.*	*Collection*	*26(c)*
2.	*Information is collected from students during their years in school for the purposes of providing educational services.*	*Collection*	*26(c)*
3.	*Information is collected from students during their years in school for the purposes of providing academic or personal counselling or other services necessary for the student.*	*Collection*	*26(c)*
4.	*Information is collected from a school from whom the student is transferring.*	*Collection*	*26(c); 27(1)(b)*
5.	*Information is used by educators, counsellors, administrative staff, and other professionals in the school system for the purposes for which the information was collected, or for a purpose that is consistent with the original purpose.*	*Use*	*32(a)*
6.	*Student information is disclosed to the Ministry of Education for funding, accountability and public reporting as per the School Act or Independent School Act*	*Disclosure*	*33.1(1)(c); 33.2(a)*
7.	*Student information is disclosed to educators, counsellors, administrative staff, and other professionals within the school system when the information is necessary to perform their duties*	*Disclosure*	*33.2(c)*
8.	*Student information is disclosed to the necessary individuals when a student is ill or injured*	*Disclosure*	*33.1(1)(n); 33.2(a)*
9.	*Information may be disclosed if the head of the public body determines that compelling circumstances exist that would affect anyone's health or safety*	*Disclosure*	*33.1(1)(m)*
10.	*Information in the MyEducation system can be disclosed to Fujitsu Consulting (Canada) in order to install, implement, maintain, repair, troubleshoot or upgrade the MyEducation system*	*Disclosure*	*33.1(1)(p)*

9. Risk Mitigation Table

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Employees could access personal information and use or disclose it for unauthorized purposes.*	*District privacy training and refresher training courses on responsibilities for personal information.* *All employees are required to sign-off on the computer use policy as a condition of employment.*	*Medium*	*Medium*
2.	*Employees have unauthorized access to personal information.*	*Accounts are assigned to users by School District staff on a need-to-know basis. Access by staff and teachers is limited to the minimum functionality and student records required to perform their duties.*	*Low*	*Medium*
3.	*Unauthorized individuals (including students) gain access the system.*	*All authorized users are issued individual accounts by the District and receive training regarding appropriate use. Passwords must have a degree of complexity that is compliant with provincial requirements. Sessions terminate automatically after xx minutes of inactivity.*	*Medium*	*Low*
4.				

10. Collection Notice

Requirements for the collection, storage, use, disposal and retention of student records are described in the *School Act* ss 79 Student Records and the Permanent Student Record Order.

When 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.*

This could be done in the registration package that parents first fill out, for example. Please include your proposed wording for a collection 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. For further help with collection notices please see the "Collection Notice Tip Sheet" located on the OCIO's website.

Part 3 – Security of Personal Information

Please fill out this security section with your local security controls.

11. **Please describe the physical security measures related to the initiative (if applicable).**

For example: locked cabinets, securely stored laptops, or key card access to the building.

12. Please describe the technical security measures related to the initiative (if applicable).

For example: use of firewalls, document encryption, password management or user access profiles assigned on a need-to-know basis.

13. Does your branch/department rely on any security policies?

Please describe any specific policies and procedures and provide contact details for someone who could answer further questions regarding these policies and procedures.

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.

For example: role-based access.

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

For example: regular review of account allocation, audit trails or physical sign-in and sign-out of files.

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?

Personal information is entered, updated and corrected by school staff, based upon information provided by students and their parents/guardians.

Teachers enter attendance and assessment information for students within their courses.

School staff, counsellors and/or special education practitioners enter special education information and Individual Education Plans for students.

Through the parent and student portals requests can be made to update personal information and select courses. This information is stored in MyEducation BC only after it has been reviewed by school staff and/or counsellors.

Changes to personal information are tracked in an audit log, which is available for review.

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

Yes

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.

For example: check to see that the information was obtained from a reputable source such as a parent, legal guardian or another government agency.

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?

Requirements for the retention of student records are described in the *School Act* ss 79 Student Records and the Permanent Student Record Order.

If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please describe retention schedules that apply where retention exceeds the one year requirement of FOIPPA. Please contact your public body's privacy office(r) and/or records office(r) if you require assistance.

Part 5 – Further Information

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

n/a

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

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

n/a

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	

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.

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

Please ensure Parts 6 and 7 are attached to your PIA.

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) 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 and submit it to Privacy Office(r).

Part 7 – School District Signatures

School District Contact Responsible for Protection of Privacy	Signature	Date

School District Privacy Officer/Privacy Office Representative	Signature	Date

School District Contact Responsible for Systems Maintenance and/or Security	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.