Appendix A – Privacy Impact Assessment (PIA) Template

Project/Product ("Project"):
Date:
Business Owner responsible for project:
Analyst responsible for this PIA:

All documents relied on for the completion of this PIA are listed in Part E.

PART A - BACKGROUND

Concise project description *(This includes an explanation of the goal of the Project)*:

External vendors:

Project status and implementation date:

Overall project pre-assessment risk rating (high, medium or low with a brief rationale):

PART B – PERSONAL INFORMATION INVENTORY

Complete a separate column for each unique group of impacted individuals (e.g., students, staff, parents), adding columns as required. IT Services completes this section using information supplied by the Business Owner and vendor, while Legal Services confirms the applicable legal authority and supplements the section with information contained in the vendor's contract. Under MFIPPA and IPC guidelines, Personal Information (PI) includes any recorded information about an identifiable individual—such as demographic details (e.g., name, address, email, phone, age, gender identity, race, equity status), educational records, health or financial data, biometrics, ID numbers (OEN, SIN), opinions, or correspondence. Use the table below to detail how information moves through the initiative, including who provides it, how the Board and vendor use and store it, position titles and roles with access, relevant integrations, third-party sub-processors, routine disclosures, retention periods, and secure disposal protocols when the service ends (a simple flow diagram or table may also be attached if helpful).

	Group 1 (Students)	**Group 2 (Staff)**
What personal information (PI) is being collected, used or disclosed? *List all data elements*		
What is the source of the PI? *Direct or indirect collection? Collections*		

	Group 1 (Students)	Group 2 (Staff)
from parents are direct collections in most cases. If indirect, from whom or from where is information being collected?		
What is the purpose of the collection and use of the PI?		
Is the collection of this PI necessary for the stated purpose?		
Are there any potential secondary uses of the PI that might not be in line with the original purpose (or a related, consistent purpose) for the collection or use of the PI? If yes, please describe:		
Legal authority for collection and use? *Refer to a provision of the Education Act.*	Section 283(2) *Education Act*	Section 283(2) *Education Act*
Indicate how individuals will be notified of the purposes for the collection, use and/or disclosure of the PI		
Who at the Board has access? *List the position titles of all officers, employees or agents of the Board who will have access and the purpose for access.*		
Is it routinely disclosed to any third parties? *A disclosure is when personal information is transferred to another person or organization for the person or organization's own purposes.*		
Why is it routinely disclosed?		
Legal authority for routine disclosure? *Identify the subjection of 32 of*		

	Group 1 (Students)	Group 2 (Staff)
MFIPPA that permits the disclosure.		
If applicable, who at the Third-Party organization has access? *List the position titles of all officers, employees or agents of the third-party organization who will have access and the purpose for access.*		
Limitations and restrictions? *List any limitations or restrictions on the collection, use or disclosure of personal information e.g. emails collected will only be used for authentication purposes, information collected will be used solely for determining eligibility for services.*		
Are there procedures in place to allow for the disclosure, correction, and deletion of personal information by users? If yes, describe:		

Records Retention and Disposition

	Group 1 (Students)	Group 2 (Staff)
What records will the initiative create or hold, and where will the official copy be kept?		
What retention periods apply to the PI, and what event starts each period? *Indicate the amount of time PI will be retained for. Bear in mind that personal information must ordinarily be retained at least one year from last use under MFIPPA. Also refer to the Board's RRCS and include the series where known.*		
How will records be retrieved, preserved when required, and securely disposed of? *Include how disposal is authorized and documented. IT Services and the vendor confirm system capabilities. Consult the Corporate Records Office where*		

requirements are unclear, and record any limitations in the mitigation plan.		

PART C – RISK ASESSSMENT

Outsourcing risk

Has a contract review been conducted (y/n)?	**[YES/NO]** by
Has a security review been conducted (y/n)?	**[YES/NO]** by
Is the project safe to proceed (y/n)?	**[YES/NO]**

NOTE: The IPC expects school boards to attempt to negotiate terms that are generally aligned with its outsourcing guidance. The contract review identifies significant deficiencies that ought to be the subject of negotiation, even if rated "low" risk.

(1) Contractual deficiencies (Please see the attached Contract Review to assess low risk contractual deficiencies)

	Contractual deficiency	**Risk assessment (H/M/L)**
1.		
2.		
3.		
4.		

(2) Security risks

Description of breach related risk *Summarize any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information – e.g. physical harm, embarrassment, reputational harm, identity fraud.*	
Description of safeguards and practices	
Indicate where the PI will reside? *E.g. Third party hosted, third-party's cloud provider (e.g. amazon), hosted*	

on premises (e.g. Board server)	
Indicate the geographic location where PI will reside	
If applicable, will third-party organization employees be trained in the requirements for protecting PI and made aware of the relevant notification procedures if PI is stolen, lost or accessed by unauthorized persons, including notifying Board of a breach? (Note that Board requires breach notification). If yes, describe:	
Does the proposed system involve the use of Artificial Intelligence (AI)?	
If you responded yes to the above AI question, provide a brief narrative description explaining how the AI functions within the solution, including its purpose, intended use, and core functionality:	<u>Decision-Making and Oversight</u> Solution involves automated decision making: ☐ Yes ☐ No ☐n/a Human oversight is in place, and explanations are available, for AI that supports decisions about individuals: ☐ Yes ☐ No ☐n/a Individuals are explicitly notified when AI materially affects a decision about them: ☐ Yes ☐ No ☐n/a <u>Data Privacy and Training Controls</u> Solution uses Board data for secondary purposes (e.g., model training, performance improvements): ☐ Yes ☐ No ☐n/a The Board can opt out of having its data used to train AI models: ☐ Yes ☐ No ☐n/a Technical controls are in place to prevent sensitive Board data from being ingested into the model: ☐ Yes ☐ No ☐n/a Board data can be permanently deleted from the AI system upon request: ☐ Yes ☐ No ☐n/a <u>Operation and Lifecycle Management</u> AI features can be switched off immediately by administrators during a security or operational incident: ☐ Yes ☐ No ☐n/a Clear retention and disposal schedules are established for all AI inputs and outputs: ☐ Yes ☐ No ☐n/a - How long are AI inputs and outputs kept, and how are they disposed of? _____ _____ A defined AI lifecycle management plan is in place, including formal decommissioning procedures: ☐ Yes ☐ No ☐n/a

Please identify the safeguards in place to protect the PI at the Board or third-party organization (select all that are known or apply):	*Technical/Security Safeguards* ☐ Encryption at rest and in transit ☐ Enforces strong passwords ☐ Appropriate role-based access controls available ☐ Multi-factor Authentication (either third party's or institution's MFA) ☐ Maintains up-to-date software and timely application of patches ☐ Use of security controls such as firewalls, intrusion detection and prevention, anti-virus and anti-spam ☐ Appropriate access/forensics/investigative logs/records are available (or can be provided) - If logs are kept, indicate what activities are logged, how are the logs kept and who can access the logs:_____ _____ _____ _____ _____ - Can the Board obtain copies of the logs if needed? ☐ Y ☐ N ☐ Periodic validation of implemented security controls by independent third parties ☐ Completion of a security audit or other assessment (e.g., SOC 2, ISO) ☐ Additional safeguards: Click or tap here to enter text. ☐ No technical safeguards in place ☐ Need help determining *Physical Safeguards* ☐ Controlled access to locations where PI is stored ☐ Locked cabinets ☐ Access cards or keys required to access secure areas ☐ Use of video surveillance to monitor premises ☐ Additional safeguards: Click or tap here to enter text. ☐ No physical safeguards in place ☐ Need help determining *Procedural Safeguards* ☐ Privacy Policy ☐ Security Policy ☐ Use of confidentiality agreements with employees or employment contracts include clauses confirming their obligations to protect PI/confidential data ☐ Privacy and Security training provided to employees ☐ Third Party Organization documentation (e.g., framework, program or process) includes content that demonstrates employees are informed of their privacy and security obligations

	☐ Privacy Impact Assessment or other privacy review completed/provided by Third Party organization ☐ Additional safeguards: Click or tap here to enter text. ☐ No procedural safeguards in place ☐ Need help determining *Evidence of Breach Notification Obligations of Third-Party* ☐ Stated in Privacy or Security Policies and Practices ☐ Stated in Terms of Use or Service/Agreement ☐ Not stated ☐ Need help determining
The third-party organization indicates they are compliant with the following privacy legislation/data privacy laws:	☐ Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) or *FIPPA* ☐ Personal Information Protection and Electronic Documents Act (PIPEDA) ☐ European Union General Data Protection Regulation ☐ Other Canadian Privacy Legislation ☐ Other International Privacy Legislation ☐ Not stated ☐ Need help determining
Please indicate if the following documentation is available and provide copies:	☐ Third-party privacy and security policies ☐ Third-party privacy and/or security audits, assessments, questionnaires (e.g., HECVAT, SOC 2, ISO) ☐ Third-party Agreement, Terms of Use or Service, or other contractual documents

Significant deficiencies identified in security review (if any):

	Security deficiency	**Risk assessment (H/M/L)**
1.		
2.		
3.		

(3) Privacy risks

Identify key privacy risks based on the fair information practice principles model, as reflected in the PIPEDA model code and other privacy statutes.

Risk assessment is based on considering each risk within a probability and impact matrix.

	Key privacy risk	**Assessment**
1.		

2.		
3.		
4.		
5.		

PART D – RISK MITIGATION RECOMMENDATIONS

	Mitigation	**Importance (High/Medium/Low)**	**Due Date of Completion**	**Status** **(Complete/Incomplete) as of [Date]**
1.				
2.				
3.				
4.				
5.				
6.				
7.				

Any outstanding action should have an assigned owner and due date. Actions required before collection begins should be completed and verified before collection proceeds.

Recommended date for reviewing this PIA: _____

PART E – DOCUMENTS RELIED ON FOR THE COMPLETION OF THIS PIA

Retain the version of each document relied on for the assessment, including relevant vendor policies and online terms. A link may be included for convenience but should not replace the copy reviewed where the content may change.

Document Name	**Version or Effective Date of Document**	**Date Reviewed**

Please Note: PIAs are living documents and must be reviewed and updated when significant changes to a program, system, technology, or the handling of Personal Information may affect previously identified privacy or security risks.