DDSB Ignite Learning

PROCEDURE

Governance (GOV)

PR GOV 06-06

Title: **Privacy Impact Assessment Procedure**
Adopted: October 20, 2026
Effective: November 2, 2026
Amended/Reviewed: N/A

This procedure must be interpreted, applied, and implemented in ways that uphold Indigenous and human rights and responsibilities, promote accessibility, and prevent and address (and do not reinforce) discrimination/discriminatory barriers.

1.0 RATIONALE

The Privacy Impact Assessment (PIA) procedure serves as a proactive mechanism to assess how the Board's programs and services impact individual privacy. Beyond risk mitigation, the PIA process is a core component of the Board's governance framework, promoting transparency, reinforcing institutional accountability, and maintaining public confidence in the Board's handling of personal information.

2.0 DEFINITIONS

2.1 MFIPPA means *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56,* as amended.

2.2 Personal Information (PI) means recorded information about an identifiable individual, including,

a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
c) any identifying number, symbol or other particular assigned to the individual,
d) the address, telephone number, fingerprints or blood type of the individual,
e) the personal opinions or views of that individual except if they relate to another person,
f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
g) the views or opinions of another person about the individual, and

h) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

2.3 Personal Health Information means identifying information about an individual in oral or recorded form if the information:

a) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family.
b) Relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual.
c) Is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019.
d) Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual.
e) Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance.
f) Is the individual's health number.
g) Identifies an individual's substitute decision-maker.
h) Is the individual's digital health identifier or other identifying information related to the creation of the digital health identifier.

2.4 Privacy Impact Assessment (PIA) is a systematic risk-assessment process used to identify, evaluate, and mitigate potential privacy and data protection risks associated with the collection, use, disclosure, storage, or destruction of Personal Information (PI) or Personal Health Information (PHI).

2.5 Privacy Impact Assessment Questionnaire is a diagnostic tool containing structured questions regarding the collection, use, retention, disclosure, and security of Personal Information (PI) and Personal Health Information (PHI). It is used to evaluate privacy risks and assist the Board in completing a full Privacy Impact Assessment.

2.6 Projects include any new or significantly modified program, service, process, technology, data integration or third-party agreement involving the collection, use, disclosure, processing, retention or destruction of personal information or personal health information.

2.7 Sensitive Personal Information (Sensitive PI) means PI that, due to its nature, context, or the circumstances in which it is collected, used, disclosed or otherwise handled, could create a heightened risk of significant harm to an individual if it is lost, stolen, accessed, used or disclosed without authorization. Sensitive PI may include health, financial, biometric or genetic information, government-issued identifiers, ethnic or racial origin, gender identity, gender expression, sex,

pregnancy, age, citizenship, place of origin, marital or family status, criminal record history, religious or philosophical beliefs, sexual orientation, geolocation information, disciplinary information, or other Personal Information that is sensitive in the circumstances.

2.8 Technology Approval Process (TAP) Review Committee is an operational governance body responsible for assessing privacy and security risks associated with Board technologies, systems, and vendors.

3.0 RESPONSIBILITY

3.1 This Procedure establishes DDSB's operational process for identifying when a Privacy Impact Assessment is required and for completing, reviewing, approving, retaining and updating PIAs. PIAs support compliance with applicable privacy obligations, including MFIPPA, PHIPA where applicable, the DDSB Privacy Policy, and any applicable provincial requirements governing school board privacy impact assessments.

3.2 Nothing in this Procedure alters the governance structure established under the DDSB Privacy Policy, including the Board of Trustees' role as head of the institution under MFIPPA and its delegation of MFIPPA powers and duties to the Director of Education.

3.3 The Business Owner (the DDSB staff member who is leading the initiative regarding the project) is responsible for:

a) Submitting a request to the Head of IT through the Technology Approval Process (TAP) Portal which may be found here.
b) Providing complete and accurate information to the Head of IT, including a completed PIA Initial Questionnaire.
c) Facilitating vendor cooperation with the Head of IT and Legal.

3.4 IT Services is responsible for:

a) Liaising with the Vendor on technical and security documentation.
b) Reviewing the intake documents provided by the Business Owner, including the PIA Initial Questionnaire, to determine if a PIA is required.
c) Completing the PIA template when an assessment is triggered (with input from the Privacy Officer/General Counsel or their designate).
d) Analyzing privacy/security risks and documenting findings, and providing risk mitigation recommendations to the TAP Review Committee for projects where it is determined that a PIA is required.

3.5 Legal Services is responsible for:

a) Working with IT Services to conduct the PIA and address contractual terms.
b) Analyzing legal and privacy risks and documenting findings.

c) Providing risk mitigation recommendations to the TAP Review Committee for projects where it is determined that a PIA is required.
d) Sitting on the TAP Review Committee (represented by the Privacy Officer/General Counsel or their designate) and formally signing off on the TAP-approved PIA.
e) Escalating PIA reviews and the go/no-go decisions to the Executive Team when necessary.
f) Maintaining a centralized PIA registry and associated documentation.

3.6 The TAP Review Committee is responsible for:

a) Reviewing the completed PIA templates and non-PI security assessments.
b) Making formal go/no-go decisions and establishing documented Risk Mitigation Plans when required.
c) Maintaining official minutes of all decisions and determinations.
d) Overseeing the implementation of and ongoing compliance with the Risk Mitigation Plans.

3.7 The Executive Team is responsible for:

a) Reviewing escalated PIAs, and for such PIAs, making go/no-go decisions and developing a documented risk mitigation plan.

3.8 Also note that the Corporate Records Office provides guidance where retention or disposition requirements are unclear, records are being migrated, a system is being replaced or retired, or the proposed arrangements may not meet the Board's records management requirements.

3.9 The Business Owner provides the operational information needed to answer the records questions, with IT confirming system capabilities and the Corporate Records Office consulted as needed.

4.0 APPLICATION AND SCOPE

4.1 This procedure applies to all DDSB staff, trustees, third-party service providers, and vendors involved in initiating, procuring, developing, or managing Board projects, technologies, or programs.

4.2 It applies to any new or significantly modified initiative involving the collection, use, disclosure, processing, or retention of Personal Information (PI) or Personal Health Information (PHI), including software adoptions, third-party vendor agreements, data integrations, and automated technologies.

4.3 All new initiatives involving personal information, including technology and non-technology initiatives such as forms, surveys, programs, pilots, and trials, must be assessed in accordance with this Procedure. An initiative is not exempt from assessment solely because it is free, provided under a trial or pilot, or intended for

limited use, including use in a single classroom.

4.4 Existing systems and initiatives involving personal information will also be reviewed, as required, to identify and address any outstanding PIA requirements.

4.5 This procedure does not apply to non-PI initiatives (which require standard IT security clearance and records management clearance), or to mandatory Ministry initiatives with fixed statutory parameters.

5.0 ASSESSMENT PROCEDURES

5.1 The Business Owner submits a project request to IT Services via the TAP Portal.

5.2 The Business Owner provides the Head of IT with relevant intake documentation, including the following:

5.2.1 A completed PIA Initial Questionnaire,

5.2.2 A 2-page project summary that provides:

i. A concise description of the project and its business/academic objectives.
ii. Confirmation of whether the Board has an existing relationship with the vendor.
iii. The identity and contact details of all external vendors hosting or processing personal information.
iv. Project status (planning, procurement, implementation) and target completion dates.
v. For technology adoptions, preliminary analysis of alternative products available to meet the same objectives, including a review of existing Board-approved software.

5.2.3 Vendor PIAs (if available),

5.2.4 Security assessments and privacy policies, and

5.2.5 All draft contractual documentation (including order forms, Master Services Agreements, and Data Protection Addenda).

5.3 Security Assessment and Initial Contract Review

Upon receiving the intake documentation, IT Services and Legal Services shall conduct a preliminary evaluation:

5.3.1 Security Assessment: IT Services conducts a security review using the HECVAT form. IT Services will determine whether to complete the full or abridged HECVAT based on initial risk, documenting this rationale in the assessment. IT Services may rely on vendor representations but should

obtain reasonable supporting documentation and seek clarification where required.

5.3.2 Initial Contract Review: Legal Services conducts a preliminary review of vendor contractual terms (including terms of service, order forms, and data protection addenda) to identify legal and privacy risks.

5.4 PIA Determination and Completion

IT Services and Legal Services shall evaluate the completed PIA Initial Questionnaire, alongside the preliminary findings from 5.3 to determine the appropriate path.

5.4.1 Where a PIA is required: Any project involving the collection or processing of PI automatically mandates a PIA. IT Services completes the comprehensive PIA Template with the active support from Legal Services (for contractual and regulatory compliance) and the Business Owner (for operational and functional details).

i. The PIA identifies and describes all privacy and security risks, characterizing them as “low,” “medium,” or “high” based on context, probability, and impact. It includes clearly defined mitigation recommendations, each assigned an importance level of “low,” “medium,” or “high.” Upon completion, the PIA Template is submitted to the TAP Review Committee for formal review under Section 5.5.

5.4.2 Where a PIA is Not Required: For projects that do not process or engage PI (e.g., non-PI software), IT Services completes a standard security assessment before submitting the project to the TAP Review Committee.

5.5 TAP Review Committee Approval (Tiered Approach)

The TAP Review Committee makes the formal go/no-go decision. The Head of IT and the Privacy Officer/General Counsel (or designate) must both be present at any meeting where a go/no-go decision is made.

5.5.1 Projects Not Requiring a PIA: If it was determined under Section 5.4 that no PIA is required, the TAP Review Committee reviews the project for technical and IT security clearance, formally recording in the official minutes that no PI is involved and no PIA is required.

5.5.2 Projects Requiring a PIA: If a PIA was required and completed under Section 5.4, the TAP Review Committee reviews the completed PIA Template alongside all intake and assessment documentation and makes a go/no-go decision.

(a) Risk Mitigation Plan: The Committee establishes a documented Risk Mitigation Plan based on the PIA and contract review recommendations. This

plan details specific risk controls and target completion dates based on risk severity, mitigation importance, and available resources. The Risk Mitigation Plan is recorded in the PIA template.

(b) Decision and Implementation Timelines for Projects Involving Sensitive PI:

(i) Pre-Approval Conditions: Where a project involves sensitive PI and requires specific mitigation steps prior to project authorization (such as mandatory contract amendments or critical technical controls), the TAP Review Committee will reconvene upon the target completion date to verify success before issuing a final go/no-go decision.

(ii) Post-Launch Remediation: Projects may be approved and implemented before all lower-priority mitigation measures are completed, provided that any mitigation measures required to be in place before the collection of Personal Information have been implemented and the TAP Review Committee has formally accepted the remaining residual risk. Only mitigation measures that can appropriately be completed after implementation may be deferred to post-launch remediation.

(c) Ongoing Compliance: The TAP Review Committee remains responsible for overseeing ongoing implementation and compliance with the Risk Mitigation Plan and will reconvene as needed to verify full completion.

5.5.3 Escalation to the Executive Team: If the TAP Review Committee has concerns about approving a project under this Section 5.5, but the Head of IT and/or the Privacy Officer/General Counsel consider that the project might be crucial to Board operations, the issue may be escalated to the Executive Team.

5.5.4 The Executive Team makes the final go/no-go decision and confirms the Risk Mitigation Plan to be implemented by the TAP Review Committee. Upon Executive approval, the complete PIA will consist of the documents outlined in Section 5.5.2 and the Executive Team meeting minutes for this item. The final PIA shall be indexed and signed as approved by the Privacy Officer/General Counsel.

5.6 Ad Hoc TAP Committee

In urgent circumstances, an Ad Hoc TAP Committee may be convened, consisting of the Head of IT, the Privacy Officer/General Counsel (or their designates), and the Business Owner, to expedite review.

5.7 PIA Registry

The Privacy Officer/General Counsel is responsible for maintaining a PIA registry and related documentation. The documentation retained for each PIA include the following:

5.7.1 The completed PIA Initial Questionnaire and PIA template (including appended security assessment).

5.7.2 Any key vendor documentation relied upon to complete the PIA.

5.7.3 The risk mitigation plan.

Final determinations are communicated to the relevant business unit and noted in the PIA Template. For projects with outstanding conditions, the TAP Review Committee reconvenes on the scheduled follow-up date to verify completion before final clearance, while unapproved or discontinued initiatives are noted as unapproved on the PIA template and filed in the registry.

5.8 PIA Review and Updates

An approved PIA must be re-evaluated and updated prior to implementing any material changes (i.e., changes that significantly alter privacy risks, data flows, or compliance requirements) to a project or its data handling practices. The Business Owner is responsible for notifying Legal Services/Privacy Office and IT Services of any proposed changes, including new uses of Personal Information, changes to collected data elements or sources, new system integrations, or the activation of Artificial Intelligence features (including vendor-introduced AI functionality). Changes to data hosting locations, vendor ownership, sub-processors, retention schedules, or security safeguards, as well as contract renewals, material amendments, or privacy breaches, will similarly trigger a re-evaluation.

Upon notification, Legal Services/Privacy Office and IT Services will determine whether the change warrants a formal update to the assessment. In addition to event-driven triggers, each approved PIA will undergo a routine review every three (3) years to confirm its continued validity. All review outcomes, whether resulting in a full update or confirming the existing assessment remains current, along with any revised documentation, are formally recorded in the PIA registry with the next scheduled review date.

5.9 Communication

Policies and procedures are posted online in accessible formats.

6.0 APPENDICES

Appendix A – Privacy Impact Assessment (PIA) Template

Appendix B – PIA Initial Questionnaire

7.0 REFERENCE DOCUMENTS

- DDSB P GOV 06 Privacy Policy

- DDSB PR GOV 06-03 Technology Approval Process Procedure
- DDSB PR GOV 06-04 Technology Approval Process (Cloud Services): Privacy and Security Assessment Guide
- *Education Act,* R.S.O. 1990, c. E.2, as amended
- *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended (MFIPPA)
- *Personal Health Information Protection Act,* 2004, S.O. 2004, c. 3, Sched. A, as amended (PHIPA)
- IPC, *Planning for Success: Privacy Impact Assessment Guide for Ontario's Public Institutions* — importantly, the IPC released an updated guide in August 2026 specifically reflecting the MFIPPA requirements coming into force January 2027.
- *Enhancing Digital Security and Trust Act*, 2024, S.O. 2024, c. 24, Sched. 1, as amended (EDSTA)
- O. Reg. 52/26: Digital Technology Affecting Individuals Under Age 18