Administrative Procedure

Mission Public Schools

Section:	**District Administration**
Title:	**Privacy Impact Assessment**

Purpose
To outline procedures for reviewing and assessing the potential impact of a proposed policy, procedure system, project, program or activity, to ensure the school district complies with the Freedom of Information and Protection of Privacy Act (the Act), Part 3 – Protection of Privacy.

Guidelines
A privacy impact assessment (PIA) is a step-by-step review process to ensure personal information collected or used in a project or initiative, is protected. Before implementing a new initiative, or making significant changes to an existing initiative, including a change to the location where personal information is stored when stored outside of Canada, a PIA is required.

General Procedures
1. Identify the purpose or objective of the initiative.

2. Identify the information elements, including personal information, to be collected, used, disclosed, or stored, and confirm that the personal information elements are necessary for the purpose of the initiative.

3. Where applicable identify:

    a. how and from whom the personal information will be collected;
    b. how the personal information will be used;
    c. how and to whom personal information will be disclosed; and
    d. if a supplementary assessment or disclosure is required for the storage of personal information outside of Canada. See supplemental procedures for more information.

4. Identify the relevant legal authority for the collection, use, or disclosure of personal information, as applicable.

5. If the initiative involves personal information, identify privacy risks and privacy risk responses that are proportionate to the identified risk.

6. Identify reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made.

7. An employee wanting to initiate a new program or initiative must review the program with their Principal, District Principal, Director or Manager.

8. The PIA process must be:
    a. submitted on the approved template.
    b. initiated by the Principal, District Principal, Director, or Manager overseeing the department or program area.
    c. determine if a supplementary assessment is needed for the storage of personal information outside of Canada, by determining;
        i. whether the initiative involves personal information that is sensitive, and
        ii. whether the personal information that is sensitive is disclosed that it will be stored outside of Canada.

    d. reviewed by the Information Technology Department, identifying any technology security concerns, and any additional measures that would be needed to protect personal information.

9. If the PIA determines that the information collected is highly sensitivity, additional information may be required prior to approval.

10. Prior to implementation, if the program or initiative is to be used for educational purposes, the PIA must be approved by the Assistant Superintendent confirming the program or initiative meets the school district's objectives regarding education.

11. Prior to implementation, the PIA must be approved by the Education Lead/Assistant Superintendent and the FIPPA Officer (Secretary-Treasurer), confirming adherence to the following requirements:
    a. that notice of collection will be given to individuals per section 27 (2) of the Act, or confirm that notice of collection is not required, per section 27 (3) of the Act; 11.
    b. where personal information is used to make a decision that directly affects an individual, confirm that reasonable efforts will be made to ensure the accuracy and completeness of personal information per section 28 of the Act;
    c. confirm that a process is in place, per section 29 of the Act, to correct individuals' personal information upon request, or to annotate their personal information if it is not corrected per the individual's request;
    d. where personal information is used to make a decision that directly affects an individual, confirm that the personal information will be retained for at least one year after use, per section 31 of the Act

Supplemental Assessment

12. If the disclosure of information outside of Canada is made in accordance with section 33 (2) (f) *if the information is made available to the public under an enactment that authorizes or requires the information to be made public;* of the Act, an assessment of disclosure for storage of personal information outside of Canada is not required.

13. A supplemental assessment is required if the initiative involves personal information that is sensitive; and, if the sensitive personal information is disclosed to be stored outside of Canada.

14. The school district must identify the privacy risk(s) as well as the level of the privacy risk(s) associated with the disclosure by examining factors which include but are not limited to the following:
    a. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;
    b. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;
    c. whether the personal information is stored by a service provider; and,
    d. where the personal information is stored.

15. For each privacy risk, identify a privacy risk response that is proportionate to the level of risk posed. These may include technical, security, administrative or contractual measures (e.g. ways to manage and review access to personal information).

16. The outcome of the assessment of disclosure for storage of personal information outside Canada will be a risk-based decision made by the school district on whether to proceed with the initiative

Determining if Personal Information is Sensitive

Some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is improperly collected, used or disclosed. Personal information may be considered sensitive depending on:

- The type of information
- The context in which it is collected, used, disclosed or stored

Context is a key factor in determining whether personal information is sensitive. Information that, on its own, may seem harmless in one context can become more sensitive when connected to services that may expose the personal activities or preferences of its users. For example, a home address may not be considered sensitive on its own. However, in some situations, a home address paired with an individual's name may be considered sensitive because of the potential negative impact on the individual if the home address is disclosed to the wrong person (e.g., in situations that may impact an individual's personal safety).

The following is a non-exhaustive list of types of personal information that are commonly considered sensitive. Note: the collection, use and disclosure of personal information should still be limited to what is necessary for the project, program or system:

- Personal health information
- Genetic and biometric data
- Personal financial information
- Geolocation data
- Criminal records
- Racial or ethnic origin
- Sexual orientation
- Religious, philosophical or political beliefs

Understanding the sensitivity of the personal information will help inform if the additional assessment is required, and the completion of the additional assessment**.**

Privacy Risks

The following list indicates risks that need to be considered. It is not an exhaustive list. There may be other relevant factors that need to be considered.

- Whether the sensitive personal information is stored by a service provider
- Where and how the sensitive personal information is stored
- The likelihood that unauthorized collection, use, disclosure or storage of sensitive personal information will occur
- The impact to an individual(s) if unauthorized collection, use, disclosure or storage of their sensitive personal information occurs

Privacy Risk Response

For each privacy risk identified, include a risk response that is proportionate to the level of risk. The higher the risk, the more robust the risk responses should be.

Risk responses can include measures that are contractual, technical, administrative and/or policy-based to manage access to sensitive personal information.

Date Approved: January 2023
Legal Reference: *Access to Information and Protection of Privacy Act*

Cross Reference: *Access to Information and Protection of Privacy and Personal Information Policy*
Privacy Management Program (includes procedures: Collection of Personal Information, Requesting Access to Information, Privacy Impact Assessment, Privacy Breach Management, and Privacy Complaints)
Forms *Privacy Impact Assessment General*
Privacy Impact Assessment – Education App