FOCUSED
EDUCATION RESOURCES

Guidance for Completing the PIA

The below information provides guidance for the completion of each section of the PIA:

1. Identify the Purpose or Objective of the Initiative

The first requirement of the **PIA Directions** is that each PIA contains a statement that identifies the purposes or objectives of the initiative.

Each PIA should begin by providing the reader with a clear, plain-language description of the initiative that is under review and its purposes and objectives. If an initiative is critical or an important priority for the school district then this should clearly be set out in the PIA description. Part of the PIA analysis includes weighing the importance and benefits of certain initiatives against the privacy risks that may be posed. Making this assessment requires that the PIA articulate and reflect that consideration was given to the nature and relative importance of the initiative.

2. Identify the Information Elements

The second requirement of the **PIA Directions** is that each PIA contains a statement that identifies the information elements involved. This includes any personal information that will be collected, used or disclosed in connection with the initiative under consideration.

An “information element” refers to specific categories of information that will be collected, used and disclosed in connection with the initiative. The information elements are often reflected in a list or table form, and the specific fields or categories of information should be broken down and listed clearly.

A list of information elements could include, but are not limited to:

- Name.
- Residential mailing address (residential street address, city, postal code).
- Personal contact information (email and phone).
- Personal information number.
- Age and date of birth.
- Grade.
- Name of school student currently attending.
- Date of enrollment.
- Personal education number.

The PIA must also contain a statement or explanation confirming that all of the listed personal information elements are needed for the purposes of the initiative. If information is being collected, used or disclosed in connection with an initiative and it does not bear a rational connection to the initiative and/or there is not a pressing reason for processing that information, then the school district should re-consider whether it should be included.

Section 26 of FIPPA authorizes the collection of personal information when it is “necessary” to do so. While the term “necessary” does not require that the collection of the information be indispensable to the success of an initiative, previous decisions of the Privacy Commissioner have confirmed that there must be a rational connection between the initiative and the personal information collected. Extraneous personal information that is gathered simply because it is “nice to have” will not satisfy this test, and its collection and use may not be authorized under FIPPA.

3. Identify How Personal Information Will Be Collected, Used and Disclosed

The third component of the **PIA Directions** requires that the PIA set out the "how, what, where and when" of the personal information that will be collected in connection with the initiative under review. This description should set out information including:

- How the information will be collected.
- Who it will be collected from.
- How it will be used.
- Who it will be shared with and who will have access to it.
- Where it will be stored, and whether it will be stored outside of Canada.

The specific details of how data will flow in connection with the initiative should be included. In some cases, it may be helpful to include a diagram or flow chart. This description should be clear about where the personal information is collected from, who will have access to it internally, and who it will be shared with outside of the organization. If personal information is being linked or collected through interfaces from different data management systems, then this should also be identified in the PIA.

If the initiative involves third-party service providers, then this description may require input from those third parties in order to identify details, such as where the data will be stored and how it will be used or whether it may be further disclosed by such service providers.

4. Identify Legal Authorities

Personal information may only be collected, used and disclosed if the school district is authorized to do so under FIPPA. Sections **26**, **27**, **32**, **33** and **34** of FIPPA set out the circumstances in which public bodies may collect, use and disclose personal information.

When completing a PIA, it is necessary for the school district to clearly indicate the specific sections of the Act that authorize it to collect, use and disclose personal information including:

- Identifying the section of FIPPA that authorizes the school district to collect personal information. The authorities for collecting personal information appear in **section 26** of the Act.
- If personal information is being collected indirectly (i.e. from a source other than the individual to whom it pertains), then the authority to collect the personal information must also be cited. Those authorities appear in **section 27** of the Act.
- Once collected, personal information may only be used by the public body as authorized in sections **32** and **34** of the Act.
- The legal authorities for disclosing personal information are set out in section 33 of the Act. Again, if an initiative involves disclosing personal information to third parties, then the PIA should indicate the part of **section 33** that authorizes that disclosure.

5. Identify Privacy Risks and Proportionate Risk Response

Risk identification and mitigation are key purposes of every PIA. It is essential that every PIA therefore includes details of the privacy risks that may arise from the initiative and the mitigation strategies that will be put into place to protect against such risks. Risks that should be considered as part of this analysis include:

- The potential for unauthorized access and use of personal information.
- Harms that would flow from unauthorized user or disclosure in light of the volume and/or **sensitivity of the personal information**.
- Risks posed through the involvement of service providers and other third parties.
- Risks arising from the storage of personal information outside of Canada.
- The potential for human error.
- The likelihood and potential for electronic or online risks, such as cyber-attacks or ransomware attacks.

The mitigation strategies must be proportionate to the degree of the risk and the anticipated harms that would arise from unauthorized use. The greater the harms and risks at stake, the more robust the mitigation efforts should be.

6. Identify Reasonable Security Arrangements

The PIA should include details about the physical, organizational, electronic and contractual security measures that the school district has put into place to protect the personal information being used in connection with the initiative under review.

If the initiative involves a third-party service provider or the use of cloud services, then the PIA should also discuss the security measures that the service provider has in place to protect personal information. This analysis should be done before a school district makes a decision about contracting with third-party service providers.

7. PIAs and Foreign Access and Storage

Under FIPPA, a public body may not store personal information outside of Canada unless:

a. It has conducted a PIA;

b. The PIA includes a "supplemental assessment" of the foreign disclosure and storage risks; and

c. The PIA has been approved by the Head of the public body.

These requirements appear in section 33.1 of FIPPA:

> **FIPPA, section 33.1**
>
> *33.1 A public body may disclose personal information outside of Canada only if the disclosure is in accordance with the regulations, if any, made by the minister responsible for this Act.*

A PIA, including a careful analysis of the risks posed by storing or disclosing information outside of Canada, is mandatory under FIPPA. The PIA should, in particular, address the contractual controls that the school district has in place with any service providers that are storing personal information outside of Canada.

8. How to Document and Implement PIA Processes

It is recommended that the school district have a Privacy Impact Assessment Policy/Procedure detailing when PIAs are required, how they should be completed, and who has the authority to approve them.

Under the **PIA Directions**, a PIA must be documented. The Ministry of Citizens Services provides a **PIA template** that can be used for this purpose.

School districts may also create their own customized form, provided that the PIA addresses all of the required elements set out in the PIA Directions.

9. Designate Accountability

School districts must designate the appropriate level of position that holds accountability for each PIA. The level of responsibility should vary in proportion to the **sensitivity of the personal information** involved and the risks of the initiative. It is good practice to have the person responsible for the initiative "sign off" on the PIA to ensure that they have read, agreed with and accepted the risks and mitigation strategies.Where operationally possible, the PIA should also be reviewed and approved by the Privacy Officer and/or Head of the public body.

RESOURCES

The provincial government website provides additional **Guidance for PIAs**.

- Learn when and how to use **Security Threat and Risk Assessments (STRA)** for new or significantly modified information systems.