

ASL translation: <https://vimeo.com/698155832/6ebec58691>

Chapter 4 Human Resources Management

4.12 Protection of Privacy Policy

Policy Statement

The Atlantic Provinces Special Education Authority (“APSEA”) collects, uses, retains, and discloses personal information in order to deliver educational services in the Atlantic Provinces. APSEA is responsible for custodianship and accountability when collecting, using, storing, and disclosing personal information, and for protecting personal information in accordance with applicable laws and privacy best practices.

Definitions

The following definitions relate to the protection of privacy by APSEA, but not all terms are used in this Policy:

Consent – Is obtained when it is reasonable to expect that the individual providing the consent understands the nature, purpose, and consequences of the collection, use or disclosure of their personal information to which they are consenting.

Digital Resource Assessment – The review and assessment of digital resources completed before such resource is used in an educational setting.

Employee - A person who has entered into a contractual agreement of employment with APSEA, as well as other direct employees performing work for APSEA.

FOI Laws - The following provincial public sector freedom of information and protection of privacy laws, together, are referred to herein as the FOI Laws: The [Access to Information and Protection of Privacy Act \(ATIPPA\)](#) and of Newfoundland and Labrador; the [Right to Information and Protection of Privacy Act \(RTIPPA\)](#) and regulations of New Brunswick; the [Freedom of Information and Protection of Privacy Act \(FOIPOP\)](#) and regulations of Nova Scotia (as well as Nova Scotia’s [Personal Information International Disclosure Protection Act \(PIIDPA\)](#) which restricts disclosure of or access to information from, outside of Canada); and the [Freedom of Information and Protection of Privacy Act \(FOIPOP\)](#) and regulations of Prince Edward Island.

Personal Information – Under the FOI Laws (defined below), “personal information” means recorded information about an identifiable individual, and can include;

- the individual’s name, address, or telephone number;
- the individual’s race, national or ethnic origin, colour, or religious or political beliefs or associations;
- the individual’s age, gender identity, sexual orientation, marital status, or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual’s fingerprints, blood type or inheritable characteristics;
- information about the individual’s health-care status or history, including a disability;
- information about the individual’s educational, financial, criminal or employment status or history,
- the opinions of a person about the individual; and
- the individual’s personal views or opinions, except where they are about someone else.

Privacy – The right of an individual to control the collection, use, and disclosure of personal information. Privacy of personal information is a right of every citizen.

Privacy Breach – An incident where personal information is collected, used, retained, or disclosed without appropriate authorization or in error.

Privacy Impact Assessment – A process that a public body may require before adoption of a new practice or procedure relating to personal information and privacy (and that may include participation by APSEA) that identifies, addresses, and documents potential privacy risks that may occur in the course of collecting, using, or disclosing personal information.

Privacy Program – A program that encompasses privacy controls and processes, mechanisms for monitoring, tools for fulfilling privacy obligations, and provides education of privacy best practices through training.

Video Image Collection – Video surveillance and video images collected within APSEA buildings. This information constitutes personal information and as such is subject to this policy.

Policy Objectives

Privacy of personal information is a right of every citizen. The objective of this policy is to outline APSEA’s responsibility for the collection of personal information for the purposes of delivering educational services, as well as its legal obligation to ensure information within its custody and control is secured and protected from unauthorized access, use, disclosure, and disposal.

This policy addresses the following regarding the protection of personal information.

- The collection, use, disclosure, and protection of personal information.
- Access to, and the right to challenge, personal information in the custody and control of APSEA and third-party providers.
- The process to report a Privacy Breach.

APSEA recognizes the importance of providing guidance and direction for the protection of personal information and the development of a Privacy Program. This policy provides a framework under which all parties can fulfill their role and responsibilities and ensure compliance with privacy best practices and relevant FOI Laws, as well as APSEA policies and procedures.

Application

This policy applies to all APSEA employees, volunteers and Committee members and any individual in a contractual relationship with APSEA.

Policy Directives

1. APSEA will only collect, use, retain and disclose information in the delivery of educational services to students and in accordance with applicable FOI Laws and privacy best practices.
2. APSEA will take reasonable measures and implement safeguards to ensure:
 - a) the protection of personal information in its custody and control against unauthorized access, collection, use, disclosure, or disposal and in adherence with retention schedules.
 - b) that those authorized to access such information do so only within the performance of their employment duties.
 - c) individual rights to access to their own personal information is provided as per legislative requirements, including an individual's right to challenge the accuracy and completeness of the information and request amendments as appropriate. However, employees with access to APSEA information are to follow protocols as set up by APSEA to access their own personal information.
3. This policy is applicable to:
 - a) all records in the custody or under the control of APSEA including records relating to APSEA operations, and all records created or receiving in the day-to-day business operations of APSEA, regardless of the medium in which those records are created, stored, and maintained.
 - b) all administrative and educational applications and information technology systems used to create, store, and manage records and information including, but not limited to, email, database applications and website.

- c) all employees and any third-party or agents who collect or receive records and information on behalf of APSEA or for the day-to-day operations of APSEA.

The Superintendent or their designate is responsible to ensure compliance with this policy and to delegate administration of legislative requirements to designated staff.

4. The FOI Laws require that public bodies (including school boards):
 - a) provide the public with the right of access to records.
 - b) protect the privacy of individuals whose personal information is collected, used, and disclosed by public bodies.
5. Any individual who accesses, uses, or discloses personal information without authority and in contravention of FOI Laws or this Policy may be subject to the penalties under such laws, and action being taken by APSEA. Such action by APSEA may include disciplinary action, up to and including termination of employment; and/or referral for criminal investigation/prosecution.
6. APSEA will ensure third-party service providers, who have access to and/or custody of personal information on its behalf, are held accountable for protection of that information. Third party service providers are obligated to abide by applicable legislation (including applicable FOI Laws), and APSEA's privacy policy, procedure, and protocols.
7. APSEA will take reasonable measures to establish a privacy program, including privacy requirements within programs, contracts, agreements, and information technology systems.
8. APSEA will implement a privacy breach protocol for investigating and mitigating any incidents where personal information is accessed, collected, used, and or disclosed by an individual unauthorized to do so, or where there has otherwise been a privacy breach.
9. If an individual has a concern or complaint regarding the handling of their personal information, they should contact the Manager of Human Resources.

Accountability

All APSEA Employees are responsible for understanding and following this operational policy and any documents related to protection of privacy.

Monitoring

- The Superintendent of APSEA or their designate will review this policy annually.

References

The [Access to Information and Protection of Privacy Act \(ATIPPA\)](#) and regulations is the principal legislation governing the protection of information within Newfoundland and Labrador.

The [Right to Information and Protection of Privacy Act \(RTIPPA\)](#) and regulations is the principal legislation governing the protection of information within New Brunswick.

The [Freedom of Information and Protection of Privacy Act \(FOIPOP\)](#) and regulations is the principal legislation governing the protection of information within Nova Scotia.

The [Freedom of Information and Protection of Privacy Act \(FOIPOP\)](#) and regulations is the principal legislation governing the protection of information within Prince Edward Island.

The [Personal Information International Disclosure Protection Act \(PIIDPA\)](#) and regulations governs transfers/disclosures of personal information by public bodies to jurisdictions outside of Canada.

Privacy Breach Protocol

Digital Resource Assessment Process

Approval Dates

Approved: February 2022

Revised: