Administrative Procedure 141 PROTECTION OF PRIVACY

The *Protection of Privacy Act* (POPA) establishes mandatory requirements for all Alberta public bodies, including school divisions, regarding the management, protection, and authorized use of personal information, data derived from personal information, and non-personal data. The Division is committed to ensuring full compliance with POPA and maintaining the trust of students, families, staff, and the public.

This administrative procedure outlines the Division's responsibilities and processes for meeting the requirements of POPA, including:

- Authorizing and limiting the collection, use, and disclosure of personal information
- Ensuring secure handling of all information
- Establishing and maintaining a Privacy Management Program
- Managing privacy breaches and reporting obligations
- Conducting Privacy Impact Assessments
- Managing non-personal and derived data
- Ensuring transparency and accountability in all data practices

Definitions
Key terms from the Act used in this procedure include:

Personal Information – recorded information about an identifiable individual (e.g., contact, demographic, health, education, biometric, or financial information).

Data Derived from Personal Information – identifiable data created through data matching.

Non-Personal Data – data that has been modified, anonymized, or synthesized so it no longer identifies an individual.

Head of the Public Body – the Superintendent or designate, as defined under the Access to Information Act.

Employee – includes contractors, volunteers, appointees, and students on **placement**.

1. Roles and Responsibilities

1.1. Head of the Public Body (Superintendent)

Under POPA, the Superintendent is legally designated as the Head of the Public Body. Through this Administrative Procedure, the Superintendent formally delegates all day-to-day powers, duties, and functions under POPA to the Secretary-Treasurer, except the power to further delegate.

The Superintendent

- Approves this procedure and amendments
- Provides oversight of privacy compliance
- Receives periodic status reports
- Retains authority to assume any POPA responsibility

1.2. Delegated Head of the Public Body – Secretary-Treasurer
The Secretary-Treasurer is responsible for:

- Administering all duties as Head under POPA
- Overseeing compliance
- Approving data matching, non-personal data creation, disclosures, PIAS, and vendor agreements
- Ensuring timely breach notifications
- Maintaining the Privacy Management Program and the Directory of Personal Information Banks

1.3. Privacy Officer
The Privacy Officer:

- Develops, implements, and maintains the Privacy Management Plan
- Leads breach intake, assessment and reporting
- Conducts privacy training
- Supports compliance monitoring

1.4. Employees and Contractors
All employees must:

- Comply with POPA and this procedure
- Report Privacy Breaches Immediately
- Complete mandatory privacy training
- Handle Information securely

2. Collection of Personal Information

The collection of personal information by the Division is limited to what is necessary for:

- Educational programming and student services
- Division operations and administration
- Student and staff safety
- Compliance with statutory obligations

2.1. Direct Collection Requirement
Personal information must be collected **directly from the individual** unless an exception in S.5 applies (e.g. safety emergencies, eligibility verification, debt collection).

2.2. Notification Requirement
At the time of direct collection, the Division must inform individuals of:

- Purpose of collection
- Legal authority
- Contact information for questions
- Whether information will be input into automated systems

3. Use of Personal Information

The Division may use personal information only:

- For the purpose it was collected;
- For a consistent purpose (s.14); or
- With the individual's consent (as prescribed).

Use must be limited to what is **necessary**.

4. Disclosure of Personal Information

Disclosure is allowed only under circumstances in s.13, including:

- Where the disclosure is not an unreasonable invasion of privacy;
- To carry out the purpose for which the information was collected;
- With consent;
- Required by law, court order, or law enforcement;
- For common or integrated programs;
- To protect health or safety of a minor or avert imminent danger.

Disclosure must be **limited to the minimum necessary**.

The **sale of personal information is strictly prohibited**.

5. Correction of Personal Information

Individuals may request correction if they believe their personal information is inaccurate using the Correction of Personal Information Request Form (Appendix B).

The Division must:

- Correct or annotate the record within 30 business days.
- Notify other public bodies or third parties who received the information in the preceding year.

Opinions, including a professional or expert opinion, must not be corrected.

6. Protection and Security of Information

The Division must protect personal information and data derived from non-personal data which is in the custody of the Division by implementing:

- Reasonable security arrangements against unauthorized access, collection, use, disclosure, or destruction.
- Security must include:
  - Administrative safeguards (policies, procedures, training)
  - Technical safeguards (encryption, MFA, access controls)
  - Physical safeguards (secure offices, controlled access)
  - Information & Data Classification Levels (the classification level assigned to personal information must reflect the sensitivity of the personal information)

7. Privacy Incidents and Breach Reporting

A four stage-protocol applies:

7.1. Immediate Reporting – Any suspected or actual loss or breach of personal information must be reported immediately to the employee's supervisor and the Secretary-Treasurer.

7.2. Preservation of Evidence – No action may be taken that could impede an investigation including deleting or altering data, unless directed by the Superintendent or designate.

7.3. Notification – The Division is responsible for assessing risk and notifying affected individuals where a breach presents a reasonable risk of harm. Notification of the

incident is to be sent to the Commissioner and the Minister as well.

7.4. Mitigation and Prevention – Root cause analysis, corrective actions and documentation are to be completed.

8. Privacy Management Program

The Division must establish and maintain a Privacy Management Program (PMP) that:

- Contains documented policies and procedures.
- Is proportional to the volume of sensitivity of personal information.
- Meets all prescribed regulatory requirements

Any person may request a copy of the PMP, which must be provided within 30 business days.

9. Privacy Impact Assessments

Privacy Impact Assessment are completed when the Division is implementing a new program or if there is a significant change to a current program that collects, uses and discloses personal information. The Assessment is to include the identification and review of risks and mitigation strategies.

- Copies of any Privacy Impact Assessments are to be provided to the Commissioner.

10. Data Matching and Derived Data

Data matching is allowed only for the purposes of research and analysis or program administration/evaluation. Derived data must be protected using reasonable security measures and be destroyed or transformed into non-personal data when no longer required.

The Division must implement human oversight, auditing and validation measures for systems used for creating data derived from personal information or non-personal data to ensure the accuracy and reliability of the data.

- The Secretary-Treasurer must provide notice to an individual when the Division intends the personal information to be used by an automated system.
- The Division may disclose information to another public body to carry out data-matching (when two sources of personal information are linked into a single data set) when planning, administering, delivering, managing, monitoring or evaluating a program or service.
- When creating non-personal data, the Division must establish a Data quality assurance process.

11. Directory of Personal Information Banks

The Division must maintain and publish a directory of all personal information banks (PIBs). The directory is to be updated as new PIBs are created or purposes change.

12. Employee Protections & Offences

A person who knowingly collects, uses or discloses personal information or who creates or discloses non-personal data in contravention of this Act will be guilty of an offense and may be subject to fines as stipulated in the Act, ranging from $125,000 to $1, 000, 000.

13. Review and Revision

This administrative procedure will be reviewed:

- Annually

- When legislation changes
- When new systems or programs involving personal information are introduced
- After privacy incidents

References: Sections 52, 53, 65, 68, 222 Education Act
Protection of Privacy Act
Protection of Privacy Regulation
Protection of Privacy (Ministerial) Regulation

Created May 2026