ADMINISTRATIVE PROCEDURE 180

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY

General Administration

July 2025

Purpose/Background

The Access to Information Act (ATIA) and Protection of Privacy Act (POPA) controls the manner in which a local public body collects, uses, discloses and disposes of personal information. The ATIA and POPA Acts also ensure access to information as a right and protects personal information.

The Division has historically provided many different types of information openly to the public through both routine disclosure and active dissemination and, where appropriate, will continue to do so. The ATIA and POPA Acts are considered to be a last resort for obtaining information from the Division that does not meet the criteria as either a discretionary or mandatory exception to disclosure.

Personal information banks will be secured. Personal information banks include but are not limited to employee files, student records, health records and emergency contact information.

Procedures

1. Access to information is a right of the general public. This right must be balanced by appropriate protection of the privacy of personal information. The Division will provide access to information in its custody and control in a manner consistent with this Administrative Procedure and with the three (3) fundamental principles upon which the ATIA Act was developed:

   1.1 To allow the right of access to records held by public bodies subject to limited and specific exceptions;

   1.2 To allow the right to access an individual's own personal information about themselves, subject to limited and specific exceptions;

   1.3 To provide the independent decision made by public bodies under the ATIA to the Office of the Information and Privacy Commissioner.

   The Division will also protect the privacy of all information in its custody and control in a manner consistent with this Administrative Procedure and with the five (5) fundamental principles upon with the POPA was developed:

   1.4 To provide guidance with the collection, use, and disclosure of personal information by public bodies;

   1.5 To allow individuals the right to request corrections to their personal information held by a public body;

   1.6 To enable public bodies to data match and allow the creation, use, and disclose of non-personal data and data derived from personal information;

   1.7 To require public bodies to protect personal information including when data matching, and creating, using, and disclosure of data derived from personal information and non-personal data; and

   1.8 To allow for independent review of decision made and resolution of complaints made against public bodies.

2. The Superintendent is the Head of the Division for the purposes of the Access to Information Act and Protection of Privacy Act.

3. As delegated by the Superintendent, The Access to Information (ATI) Coordinator, is responsible for ensuring that the Division complies with all provisions of the Acts and for establishing procedures and practices to ensure appropriate implementation and management of these legislations.

4. The Principal of each school shall be the site coordinator for the purposes of the Acts. Site Coordinators are responsible for ensuring the protection of personal information at their schools and direct inquiries about disclosure of information to the ATI Coordinator.

5. The Division reserves the right to edit personal identifiers that are deemed to be of a personal and /or of a sensitive nature from documents made public in order to protect the rights of the individual, in conformance with the Access to Information Act and Protection of Privacy Act.

6. The Associate Superintendent of Business and Operations will establish procedures to:
   - 6.1 Allow the right for any person to access the records in the Division's custody or control subject only to those limited and specific exceptions stated in the Acts and the payment of fees adopted by the Division.
   - 6.2 Control the manner in which the Division's agents collect personal information from an individual. When information is collected directly from individuals, notice will be provided to the individual relative to:
     - 6.2.1 The purpose for which the information will be used;
     - 6.2.2 The legal authority for collecting the information; and
     - 6.2.3 The name of a contact within the Division if they have questions.
   - 6.3 Control the manner in which the Division's agents use personal information. Information may be used:
     - 6.3.1 For the purpose for which the information was collected;
     - 6.3.2 For use consistent with the purpose for which the information was collected; or
     - 6.3.3 When the individual the information is concerning has identified the information and has consented in the prescribed manner to the use of the information.
   - 6.4 Control disclosure by the Division's agents of personal information. The use of personal information must:
     - 6.4.1 Have a reasonable and direct connection to the original purpose for which the information was collected; and
     - 6.4.2 Be necessary for performing the statutory duties of, or for operating a legally authorized program of, the Division.
   - 6.5 Ensure that written consent to use personal information is obtained. Consent shall include:
     - 6.5.1 To whom the information may be disclosed and how it may be used;
     - 6.5.2 The purpose of the collecting;

6.5.3 A statement that consent is voluntary and may be revoked at any time;

6.5.4 To the extent possible, identification of any consequences that may result from refusal;

6.5.5 The period of time during which consent remains valid; and

6.5.6 Provisions for a tracking mechanism for consent.

6.6 Allow individuals, subject to limited and specific exceptions, the right to have access to the information about them held by the Division.

6.7 Allow individuals the right to request corrections to information about them held by the Division.

6.8 Provide for an independent review of decisions made by the Division pursuant to the Acts.

Reference:

- RVS AF180-AATIA/POPA Request Access to Information - General
- RVS AF180-B Independent Student Consent for Release of Personal Information to Parent or Legal Guardian
- RVS AF180-C ATIA/POPA Request for Access to Student Information
- RVS AF180-D Consent for Use of Non-Supported RVS Technologies
- RVS AF180-E Student Information Correction
- RVS AF180-F Request for Information Law Enforcement
- RVS AF180-G Informed Consent Data Sharing Third Parties 2022
- RVS AF180-H Consent to Release Personal Information Council Society
- RVS AF180-G Consent to Release Personal Information Graduation Committee
- Education Act
- Access to Information Act
- Protection of Privacy Act
- Access to Information Act Regulations
- Protection of Privacy Act Regulations

Appendix A – PROTECTION OF STUDENT INFORMATION

Purpose/Background

The Division recognizes that a significant amount of information about students and their families is collected and also recognizes its responsibility to use this information for its intended purpose and to safeguard it.

The protection of student information on a province-wide student database is the responsibility of all authorized users.

Definitions

Information – refers to all information in the custody or under the control of the Division, whether in electronic or other recorded format, and includes administrative, financial, personal and student information, and information about those who interact or communicate with the Division.

Employee - has the meaning given in the Access to Information Act and includes employees, contractors, volunteers, and others providing services to, or on behalf of, the Division.

Student information - means personal information about a student, whether enrolled with the Division or not, including information about any student contained in PASI.

PASI - the Provincial Approach to Student Information database and application maintained by Alberta Education.

Risk - any factor that could be detrimental to the confidentiality, availability, integrity or privacy of information in the custody or control of the Division.

Procedures

1. All information must be maintained in confidence and disclosed only if authorized by regulation or law including, but not limited to, the Education Act, the Access to Information Act, the Protection of Privacy Act, the Child, Youth and Family Enhancement Act, and the Income Tax Act.

2. Only legally authorized people may access student information.

3. The Superintendent will ensure that a record is kept of all personnel who have been authorized to access student information.

4. Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and the Division's records management standards, procedures, and practices.

5. Each person using the students' information at a Division location or otherwise, is responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.

6. The nature of security measures must be adequate and appropriate for the sensitivity of the information to be protected.

7. Employees will be provided with training and awareness materials as necessary to ensure that they understand their security obligations.

8. Sensitive or confidential information must be stored in a secure location with restricted access, such as secure electronic storage, a locked room, or a locked filing cabinet. Security measures must be appropriate for the sensitivity of the information being stored regardless of the physical or electronic medium on which it is stored.

9. Care must be taken when transporting or transferring sensitive or confidential information so that it reaches its intended destination intact and without unauthorized access or disclosure.

10. Any information that is no longer required for either administrative, educational, financial, legal or historical purposes, and the retention of which is not regulated by any provincial or federal law, may only be destroyed in accordance with records management procedures and practices.

11. All privacy concerns are to be forwarded to the Division's Access to Information Coordinator

12. The Superintendent or designate may grant temporary remote access rights to third parties, ensuring the security of their network meets the standard of the Division.

13. The Superintendent or designate will ensure that a corporate record of third-party access is maintained.

14. Risk assessments, which may include threat/risk assessments, privacy impact assessments or other assessments as necessary, shall be conducted on any new business process, system, application or service, if it involves the collection, use or disclosure of personal or otherwise sensitive personal information.

15. Workstation security is critical in the realization of the intent of this Administrative Procedure and is the responsibility of the Superintendent to ensure proper security measures are in place.

16. Personal information

    16.1 Personal information must be exported to or stored on Division equipment only.

        16.1.1 All Division digital devices that have personal information on them must employ full disk encryption with an approved software encryption package. No Division data may exist on a laptop in clear text.

16.1.2 Persons who have the ability to export personal information must have a password on the screen saver of any device used. The screensaver must turn on within 3-5 minutes of inactivity.

16.2 Any computer logged into applications hosting personal information must be secured if walked away from. To secure a workstation, users must do one of the following: log-out of the application that hosts personal information or engage user-authentication on the device.

16.3 All persons that access personal information with a digital device must not save passwords in the authentication page of the application (i.e., a browser webpage or computer password management software).

16.4 If using a shared digital device from a school/department, users must ensure any personal information is cleaned off before returning the computing device for others to use.

16.5 Personal information can be emailed using only the Division corporate email system (Novell GroupWise). No other electronic transport technology can be used unless approved by the Superintendent. Personal information that is forwarded by email must only be shared with an authorized employee through a rockyview.ab.ca email address. Forwarding emails that contain personal information to other email systems is not permitted.

16.6 Personal information must be transported on Division devices only. If authorized personnel are working off-site, the school/department must provide a Division device for such use. Personal data must be stored or transported only on a fully encrypted USB drive, DVD, CD, external drive or mobile device. It may be accessed on non-Division mobile devices providing it is not stored there.

16.7 Only persons requiring exported personal information will be granted access to it. The Division Student Information System team will oversee the management and security of groups in the Division Student Information System.

16.8 Transitory reports extracted from applications that host personal information are restricted to the school/department that requires them and are not to be stored beyond the academic year in which they were produced. These files are to be stored on a network drive, not on individual computing devices, and are to be deleted after no longer useful, i.e., if a cumulative monthly report is done, the previous report is to be removed when running the current monthly report.

16.9 All exported personal information must adhere to defined record retention procedures as outlined by Administrative Procedure 185 - Records Management and Administrative Procedure 185 Appendix – Records Retention Schedule.

16.10 Authorized users will be identified each year by the Director of Technology for Learning. A detailed log will be kept of all temporary accesses granted.

16.11 The Associate Superintendent of Human Resources will ensure all staff complete confidentiality/non-disclosure agreements as per the ISO27001 standard and PASI operational guidelines.

16.12 Printed reports of staff exports are to be handled carefully, i.e., filed in a locked desk, file cabinet, secure area or locked office. Division document management procedures must be followed. Print copies are to be shredded when no longer needed.

16.13 Personal information is recorded information about an identifiable individual, and may include:

16.13.1 The individual's name, home or business address or home or business telephone number;

16.13.2 The individual's race, national or ethnic origin, colour or religious or political beliefs or associations;

16.13.3 The individual's age, gender, marital status or family status;

16.13.4 An identifying number, symbol or other particular assigned to the individual;

16.13.5 The individual's fingerprints, blood type or inheritable characteristics;

16.13.6 Information about the individual's health and health care history, including information about a physical or mental disability;

16.13.7 Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;

16.13.8 Anyone else's opinions about the individual;

16.13.9 The individual's personal views or opinions, except if they are about someone else;

16.13.10 Student records; and,

16.13.11 Student digital images.