

Purpose

RVS is responsible to protect and secure any Personal Information it obtains. This Administrative Procedure outlines what Personal Information must be protected and the procedures in place that must be followed by RVS Staff, Volunteers, Contractors, Students, and Third Parties to protecting the privacy of all individuals.

Background

The Freedom of Information and Protection of Privacy (FOIP) Act controls the manner in which a local public body collects, uses, discloses and disposes of personal information. It also outlines the duty of the public body to protect personal information.

Definitions

Head of the Division: The Superintendent, is the Head of the Division for the purposes of the Freedom of Information and Protection of Privacy Act.

FOIP Coordinator: The Associate Superintendent of Business and Operations, as FOIP Coordinator, is responsible for ensuring that the Division complies with all provisions of the Act and for establishing procedures and practices to ensure appropriate implementation and management of this legislation.

Site Coordinator: The Principal of each school shall be the site coordinator for the purposes of the FOIP Act. Site Coordinators are responsible to ensure the protection of personal information at their schools and direct inquiries about disclosure of information to the FOIP Coordinator.

Custodian: The individual, usually the Division's Records Management Assistant or Principal, responsible for managing the information in accordance with the decisions made by the document owner and the Division (Records Retention Schedule).

PASI: The Provincial Approach to Student Information database and application maintained by Alberta Education.

Personal Information: Recorded information about an identifiable individual including:

- name;
- home or business address or;
- home or business telephone number;
- race, national or ethnic origin, colour;
- religious or political beliefs or associations;
- age, sex, marital status or family status;
- identifying number (i.e. Student Number, Staff ID);
- symbol or other particular assigned identifier;
- fingerprints, biometric information, blood type, genetic information or inheritable characteristics;
- individual's health and health care history, including information about a physical or mental disability;
- information about the individuals' education, financial employment or criminal history;

- opinions about the individual;
- the individual's personal view or opinions except if they are about someone else (may be expressed through art, images or other works).

Personal Information Banks (PIB):

Required by the FOIP Act, the school division must retain a list of all PIB's that includes:

- the title or name of the information bank
- the location of the information bank
- what kind of personal information is contained in the information bank
- what categories of individuals the information pertains to
- why the information was collected and how it is used or disclosed
- the legal authority for the collection of the information

Record(s):

Any paper, microform, electronic or physical object regarded as an official record, a document upon which a decision is based, where information is stored and made/or acquired by an employee of RVS. These records are subject to the FOIP Act.

Procedures

1. Information Collection

- 1.1 All information collection is to be in accordance with the FOIP Act. If relevant, it will also be in accordance with the Health Information Act.
- 1.2 Personal Information is collected from a variety of Stakeholders including students, employees, contractors, visitors, volunteers and third parties.
- 1.3 Only information that directly relates to, and is necessary for, operation of the programs and/or activities of the School Division is to be collected. Information may also be collected that is expressly authorized by an enactment of Alberta or Canada or as otherwise outlined in the FOIP Act. This includes collection and sharing of student information through the PASI system.
- 1.4 Information is to be collected directly from the individual it pertains to (if over 18 and mentally/physically able), or otherwise from the parent, guardian, custodian, or emergency contact for the individual. In extenuating circumstances information may be collected from other sources if:
 - 1.4.1 Authorized by that individual;
 - 1.4.2 Provided for in another Act, or regulation under another Act;
 - 1.4.3 Directed by the Privacy Commissioner;
 - 1.4.4 Used to determine suitability for an honor or award information;
 - 1.4.5 Referenced for the purpose of fund-raising (any published or public source may be used);

- 1.4.6 Collected for use in the provision of legal services to the Government of Alberta or a public body.
- 1.5 When collecting information, specific information (as outlined below) must be included in the disclaimer that clearly outlines the reason, use and retention of the information. Appendix "A" shows a template disclaimer that to be included on all Division forms. The Privacy Notice to be located on Rocky View Schools Website will be available through AP140.
 - 1.5.1 The purpose for which the information is collected;
 - 1.5.2 The specific legal authority for the collection;
 - 1.5.3 The title, business address and business telephone number of the officer or employee of the public body who can answer the individuals' questions about the collection;
 - 1.5.4 A statement that consent is voluntary and may be revoked at any time, except where the information gathering is required by law and collected by a legislated body;
 - 1.5.5 To the extent possible, identification of any consequences that may result from refusal;
 - 1.5.6 The period of time during which consent remains valid (retention of information); and
 - 1.5.7 Provisions for a tracking mechanism for consent.
- 1.6 If the information collected directly affects the individual the public body must make every reasonable effort to ensure the information is accurate and complete. In addition, the information must be retained to allow opportunity for the individual to correct inaccurate information. AP180 outlines these procedures in more detail.
- 1.7 Personal information can be recorded in **many** formats. In a school setting, this may include:
 - 1.7.1 Paper records (i.e. class lists, printed assessment records);
 - 1.7.2 Electronic records (i.e. Electronic student attendance records, emails);
 - 1.7.3 Photographs (i.e. Yearbook images, artwork, student participation in activities);
 - 1.7.4 Video footage (ie. Surveillance cameras, or video collected for promotion of RVS event).

2. Use of Information

- 2.1 Information is only to be used for the reason provided when the information was collected (outlined in 1.4 and 1.5).
- 2.2 Information is used only as necessary for the public body to perform a service or program.
- 2.3 Information may be used to verify the eligibility of an individual to access a program or service.



3. Protection of Personal Information

The Division is required to ensure all Personal Information collected is protected from unauthorized access, unauthorized collection, unauthorized use, unauthorized disclosure or unauthorized destruction. The Division is required to evaluate risks and put safeguards in place to protect personal data.

3.1 Responsibility to Protect

- 3.1.1 The Superintendent will ensure that a record is kept of all personnel who have been authorized to access Records and Source Systems that contain Personal Information (also known as Personal Information Banks (PIB)).
 - 3.1.1.1 RVS must provide authorization before persons may have access to Personal Information Banks (i.e. PowerSchool access). This is often reflected through an employees' job description.
- 3.1.2 Every staff member, contractor, volunteer and student is responsible to protect personal information.
 - 3.1.2.1 All volunteers, contractors and staff must sign confidentiality agreements if working with students, or in classroom spaces with exposure to student or staff personal information.
 - 3.1.2.2 The Principal is responsible to inform volunteers and have them complete form [AF491-A](#).
- 3.1.3 Each staff member or custodian, authorized to have access to records and source systems that contain personal information, is responsible to be informed and fully understand their role specific to the proper handling and protection of information in their custody of control. If unaware they should review this with their direct supervisors. Specific handling and protection measures include those outlined in AP140 for responsible use of technology as well as:
 - 3.1.3.1 Taking precautions, consistent with the sensitivity of data in one's custody.
 - 3.1.3.2 Keeping confidential or sensitive material, including portable devices with access to confidential or sensitive material, **in a secure location or in their direct possession**. This includes secured portable technology. **Please note that a vehicle is not considered a secure location.**
 - 3.1.3.3 Collecting or using information ONLY as outlined in this procedure.
 - 3.1.3.4 Storing personal information only in designated locations and for the time period outlined within the Record Retention Schedule.
 - 3.1.3.5 Sharing of personal information may only occur in accordance with 2.1, 2.2, and 2.3, and only if the appropriate consent forms are in place.
 - 3.1.3.6 Confirming, when sending e-mail or digital communications, that the recipients e-mail address corresponds to the address of the recipient.

- 3.1.3.7 Protecting data is the responsibility of the sender, including the responsibility to make sure that information reaches the destination intact without unauthorized access, change or disclosure.
 - 3.1.3.7.1 Using the BCC (Blind Copy) feature when sending external e-mail to more than one party, or using alternate methods as outlined in AP146.
 - 3.1.3.7.2 Updating, on a regular basis, pre-programed or pre-populating contact lists to ensure they are correct.
 - 3.1.3.7.3 Verifying an individual is legally authorized to have access to the information before sharing it with them.
- 3.1.3.8 Limiting information accessed to only contain that which is needed for specific tasks.
- 3.1.3.9 Maintaining an inventory of the paper files containing Personal Information that may be temporarily stored at an offsite secure location (including those stored at an employees' home).
- 3.1.3.10 Retaining a Master Copy of all records, in RVS' centralized paper files or digital files (Enterprise Corporate Management (ECM) system).
- 3.1.4 The Principal is responsible for ensuring that staff training and awareness activities are completed, and that staff are familiar with the Divisions:
 - 3.1.4.1 Requirements for Technology Use including e-mail use (AP146, AP140, AP143);
 - 3.1.4.2 Guidelines for use of existing software programs;
 - 3.1.4.3 Processes to request use of new/unauthorized software programs;
 - 3.1.4.4 Familiarity and awareness of what is Personal Information (see definitions);
 - 3.1.4.5 Constraints and prerequisites for use of student images, work (AP144);
 - 3.1.4.6 Consequences to an individual, and the Division, when a privacy breach occurs.
- 3.1.5 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 (AP185).
- 3.1.6 It is the responsibility of the Superintendent to ensure proper security measures are in place.
 - 3.1.6.1 The Division's Technology for Learning Branch oversees the management and security of Divisional Digital PIB's in accordance with article 3.2.

3.2 Assessing the Impact of Systems and Processes on Privacy

- 3.2.1 Major software, programs, apps and other data storage systems used by the division, that can access Personal Information, are to be reviewed through a Privacy Impact Assessment (PIA).
- 3.2.2 Changes to systems used for, and methods of, information collection, retention, storage or disposal must also be reviewed through a privacy impact assessment and signed off by the Associate Superintendent of Business and Operations. This rule directly addresses the FOIP Regulation (section 7(5)) for electronic forms and data collection.
- 3.2.3 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. Records of third-party access will be maintained by the Technology for Learning branch.

4. Reporting Loss of Information / Breaches

- 4.1 Notice of any loss of Personal Information, whether lost, stolen, shared incorrectly or disclosed improperly, must be sent to the Associate Superintendent of Business and Operations (busops@rockyview.ab.ca).
- 4.2 Lost or stolen RVS owned devices must be reported in the ITSM (Information Technology Service Management) [system](#). In addition, individuals must complete form [AF5317-A](#).
- 4.3 The Associate Superintendent of Business and Operations or designate is responsible for reporting breaches, on behalf of the Superintendent, to the Office of the Privacy Commissioner.
- 4.4 Any party whose information has been breached will be notified.

Date Issued: August 31, 2020

Version: I

References

- i. External Legislation:
 - The Education Act Section 33, 52, 53, 65, 68, 197, 222
 - [Freedom of Information and Protection of Privacy Act](#)
 - [FOIP Regulation](#) AR186/2008
- ii. RVS Policies and Procedures:
 - AP140 – Responsible Use of Technology
 - AP143 – Teachers’ Digital Presence
 - AP144 – Public Use of Student Images/Work
 - AP146 – Standardized E-mail Signature Block & Best Practice for Corporate E-mail
 - AP147 – Use of RVS Computer Devices
 - AP180 – FOIP Requests for Information or Correction to Personal Information
 - AP185 – Records Management



August 31, 2020

- iii. RVS Forms:
 - [AF144-A – Consent for Public Use of Student Images/Work](#)
 - [AF144-E – Consent for Third Party Promotional Events](#)
 - [AF144-B – Student Artwork Showcase Application \(RVS Education Centre\)](#)
- iv. RVS Handbooks and Manuals
 - FOIP Disclaimer (Appendix A)
 - [FOIP FAQ Guide](#)
 - FOIP/Privacy Notice/Terms of Service
- v. Contact/Branch
 - Business and Operations (busops@rockyview.ab.ca)



August 31, 2020

APPENDIX A
FOIP DISCLAIMER - Forms

The information on this form is being collected pursuant to the Education Act and the Freedom of Information and Protection of Privacy Act. Questions concerning its collection or use can be directed to Rocky View Schools FOIP Coordinator, the Associate Superintendent of Business and Operations, by calling 403.945.4000 or by e-mail (busops@rockyview.ab.ca).

This information will be retained in accordance with Rocky View Schools procedures for _____. (*retention period of the form*)