INFORMATION SECURITY

Background

The Division supports the use of digital environments to enhance teaching, learning, and business processes, including information and records management. As a result, protected information may be collected, created, and stored in electronic form. All staff have a statutory and ethical responsibility to ensure appropriate care of this information when using technology and cloud-based services and must comply with Alberta's Education Act, the Protection of Privacy Act (POPA, as amended by Bill 33), the Freedom of Information and Protection of Privacy Act (FOIP) where applicable, Board policy, and Division administrative procedures.

Definitions

For the purposes of this Administrative Procedure:

Cloud-Based Services

Applications or services externally available while outside of the Division's facilities. These may include contracted services hosted by third parties or those made available by Technology Services.

Digital Citizenship

The generally accepted behavior of responsible citizenship carried over to online environments. This includes, but is not limited to:

- Treating others with dignity and respect
- Respecting the privacy of others
- Refraining from sharing information about others without their knowledge or consent
- Avoiding profane, abusive, threatening, or offensive language or content
- Protecting personal information from unknown individuals or agencies
- Using secure means when engaging in online financial transactions
- Respecting copyright and applicable laws (Canadian and international)
- Ensuring proper authorization prior to accessing resources
- Refraining from malicious actions that disrupt systems or networks

Portable Storage Device

Any mobile device that can store, process, or transmit information digitally, including but not limited to laptops, tablets, smartphones, thumb/portable drives, and CD/DVDs.

Protected Information

All information assets collected or stored that, if compromised, could cause harm to an individual or the Division. This includes personal information as defined under FOIP and POPA.

Personal Information

Recorded information about an identifiable individual, including but not limited to:

- Name, home or business address, or telephone number
- Race, ethnic origin, colour, religion, or political beliefs
- Age, sex, marital or family status
- Identifying numbers or symbols
- Biometric data, genetic information, or photo likeness
- Health, educational, financial, employment, or criminal history
- Opinions about the individual or their personal views

Information Steward

The person(s) or delegate(s) responsible for determining how protected information may be used and disclosed.

Privileged Access

Special access or abilities beyond that of a standard user. Granted only when necessary to perform assigned duties and must be logged and auditable.

Core Applications

Digital tools or systems required for division operations and educational service delivery, used broadly across PRSD (e.g., PowerSchool, Google Workspace for Education, Microsoft 365). Core applications are endorsed by the head of the relevant Central Operations department and do not require parent/guardian opt-in consent.

Low-Risk Applications

Optional digital tools that collect only basic personal information (e.g., student name, PRSD email address) and have been assessed through a Privacy Impact Assessment (PIA) as posing minimal privacy risk. General consent for these applications is obtained via PRSD's registration form or website.

Applications Requiring Explicit Consent

Any optional application that collects more than basic personal information, stores data outside Canada without adequate safeguards, involves sensitive data, or uses Artificial Intelligence (AI) or automated decision-making. Explicit parent/guardian consent must be obtained prior to use.

Privacy Impact Assessment (PIA)

A documented review of how personal information is collected, used, disclosed, stored, and safeguarded within an application or service. A PIA is required for all core, low-risk, and optional applications before approval.

Artificial Intelligence (AI) and Automated Decision-Making

Technologies or systems that analyze data and generate outputs with limited or no human intervention. PRSD will not use AI for decisions that significantly affect students without human review and prior notification.

Procedures

The Peace River School Division (PRSD) collects, uses, and discloses personal information under the authority of the Education Act (s.11, 31, 33, 52, 53, 196–197, 222) and Alberta's Protection of Privacy Act (POPA, as amended by Bill 33). Collection is limited to what is necessary for educational programming, school operations, and to maintain a safe and respectful learning and working environment.

1. Collection, Use, and Disclosure

    1.1. Staff may collect and use personal information to:

    - Deliver educational programming and supports
    - Communicate with parents/guardians and respond to emergencies
    - Publish internal communications such as class lists, calendars, newsletters, or yearbooks
    - Display student work or photos in schools and division facilities
    - Recognize students for awards, honor rolls, or event programs
    - Create and manage network IDs and technology accounts
    - Access approved educational technology tools
    - Meet reporting obligations to Alberta Education and other authorized bodies

    1.2. Collection must always be limited to the minimum information necessary for the stated purpose.

2. Privacy Impact Assessments (PIA)

    2.1. A PIA must be completed and approved by the Superintendent or delegate before use of any new cloud-based service, software application, tool, or process that collects, uses, or discloses personal information.

    2.2. PIAs must document:

    - App/system description, purpose, and scope
    - Specific personal information collected
    - Legal authority (Education Act + POPA ss.33–35)
    - Data flows, hosting country, and third-party disclosures

- Safeguards (administrative, technical, and physical)
- Retention and secure disposal plan
- Privacy risks and mitigation strategies

2.3. PIAs are required for all core, low-risk, and optional applications and are prioritized for division-wide systems.

3. Consent Requirements

3.1. General Consent

- Applies to core applications and low-risk applications that have undergone a PIA and are deemed to collect only limited personal information.
- Obtained through PRSD's student registration process and website statement.
- Parents/guardians cannot opt out of core applications as they are required for educational service delivery.

3.2. Explicit Consent

- Required for any optional application that:
  - Collects sensitive personal information
  - Stores data outside Canada without adequate contractual safeguards
  - Involves higher privacy risks or automated decision-making
- Obtained using PRSD's official explicit consent form before use.
- Parents/guardians may withdraw consent at any time by notifying the school.

4. Artificial Intelligence (AI) and Automated Decision-Making

4.1. PRSD will clearly disclose when an application uses AI or automated decision-making.

4.2. AI will not be used for decisions that significantly affect students (e.g., grades, discipline, eligibility for services) without human review and prior notice, in accordance with Bill 33.

4.3. PIAs for AI-enabled applications must include AI-specific risk and bias assessments.

5. Information Security and Access Control

5.1. All protected information shall be stored securely and guarded against unauthorized access.

5.2. Access Control

- Granted only to those who require information to perform their duties.

5.3. Privileged Access

- Granted only when justified by job function or temporarily approved by the Information Steward.
- Subject to a privileged access audit by the Superintendent or delegate.

6. Portable Storage Devices

6.1. Use prohibited for protected information unless authorized by the Superintendent or designate.

6.2. When approved, data must be encrypted, password-protected, and removed after task completion.

7. User Accounts and Authentication

7.1. Each user must have a unique account and password; account sharing is prohibited.

7.2. Multi-factor authentication (MFA) must be used by staff accessing cloud-based services and remote access systems where available.

7.3. Remote access to on-premise systems is to be treated as temporary and used only when required.

8. Breach Reporting and Incident Response

8.1. Suspected or actual information security breaches must be reported immediately to a supervisor.

8.2. Supervisors must notify the Superintendent or designate.

8.3. No action may be taken that could impede an investigation, and no accounts or data may be deleted until directed.

8.4. Parents, students, or staff will only be notified of a breach when authorized by the Superintendent or designate.

9. Backup, Monitoring, and Compliance

9.1. Technology Services maintains system backups, endpoint detection and response (EDR), and security logging.

9.2. Annual information security and privacy training is mandatory for all employees.

9.3. The Superintendent or delegate will ensure compliance through privileged access audits and other reviews as necessary.

9.4. Failure to comply with this procedure may result in disciplinary action.

Adopted/Revised/Reviewed: JUN 2016/JUN 2019/NOV 2019/OCT 2024/SEP 2025