Administrative Procedures Manual	**Administrative Procedure 142**
	Student Information System Security
	APPROVED: October 2020
Page 1 of 4	AMENDED/REVIEWED: October 2021
LEGAL REFERENCE:	Section 9, 18 52, 53, 56, 70, 222 Education Act Freedom of Information and Protection of Privacy Act Section 23 Canadian Charter of Rights and Freedoms Freedom of Information and Protection of Privacy Regulation 200/95 Student Record Regulation 97/2019 Alberta Education Information Security Management Directives (ISMD) V2.3 February 20,2020 PASI Usage Agreement

Background

It is a requirement from Alberta Education that all school authorities using either PASIprep or a PASI enabled Student Information Systems (SIS) to access student information in PASI must adhere to security controls as per the PASI Usage Agreement.

Grande Prairie Public School Division (GPPSD) maintains student information in the PowerSchool Student Information System, as well as several other ancillary database systems that connect to PowerSchool through Application Programming Interface (API).

The baseline standard for PASI security controls is derived from the Government of Alberta Information Security Management Directives.

Software Connecting to PASI

PowerSchool – PowerSchool has a live connection to PASI for student demographic data, student enrollment data and student marks and diploma credit.

Dossier – software supports creation of specialized documentation for individual student instructions as well as storage for specialized testing and assessment results. The software imports student data from PowerSchool and provides support for direct upload to the Digital Student Record on PASI.

School Engage - software allows for online student registration from parent accounts; uploading of student documentation, updates to student demographic information. Software reads from and writes to PowerSchool. Connection with PASI for document upload is under development.

Other Software connecting to PowerSchool (no impact to PASI)
Destiny - Library Management
School Messenger - Attendance Management/messaging system for broadcasts to parents
Peace Collaborative Services (PCS) Database – PCS reporting software that extracts demographic data from PowerSchool for use on student reports.

Procedures

1. Information security policies, procedures, and responsibilities - The SIS Coordinator will maintain the GPPSD Student Information System Manual, which outlines the Division's security policies, procedures, and responsibilities as they relate to the SIS and connections to PASI. (Section 1 and 2)

   The GPPSD SIS Manual will be reviewed annually and include the following:

   1.1. Outline of user hierarchy within the SIS, including levels of access to PowerSchool, Dossier, School Engage, and direct connection to PASI

   1.2. Outline of rules of access to the SIS for staff, parents, and students
   - 1.2.1. Staff - levels of access as defined by role; responsibilities of each role
   - 1.2.2. Parents - access to multiple students on public portal
   - 1.2.3. Students - access to individual student data on public portal (age/grade)

   1.3. Procedures for:
   - 1.3.1. Onboarding new staff
     - 1.3.1.1. responsibilities of staff with access to SIS
   - 1.3.2. Training of staff in a new role
     - 1.3.2.1. responsibilities of the role
   - 1.3.3. Annual Review of Account Management and Security
   - 1.3.4. Division response to SIS security breach.

2. Information security management - Any staff whose role requires access to the SIS or PASI will be provided with SIS security orientation/training:

   2.1. Training for new staff and staff changing roles within GPPSD will include a learning module specifically related to SIS data security. Changes and updates to security procedures will be communicated to all staff with SIS access. The learning module for security will be reviewed annually by the SIS Coordinator to ensure accuracy of training material.

2.2. Security roles for all SIS users will be defined and documented within the GPPSD SIS Manual Section 1-Security.

2.3. Security compliance and security incidents within the SIS will be monitored by the SIS Coordinator and reported to the Associate Superintendent of Business Services or designate as required.

3. External party security policies, standards and contracts relating to School Authority information and IT systems with contracts for software development that has impact on the SIS or any related system will include:

3.1. Requirements for the third party to adhere to Division policy for data security.

3.2. Requirements for the third party to adhere to Division policy for data confidentiality.

4. Email accounts and messages used to transmit and receive electronic communication within the SIS system shall conform to division policy for password security.

4.1. Current messaging services within the SIS:

4.1.1. School Messenger

4.1.2. School Engage

5. Authorized use of SIS:

5.1. Assignment and Removal of accounts along with monitoring

5.1.1. Changes to accounts will be limited to the Education Technology Department, based on requests from Division Administrators and the Human Resource Department.

5.1.2. Annual account reviews will be conducted.

6. A Division incident response plan for breaches of security or privacy – refer to the GPPSD SIS Manual.

7. Division policy and contracts with third party contactors that pertain to SIS, shall conform with Information Security and Privacy as required by Legislation.

8. User access logs are managed through the specific software being accessed. Access to the user access logs within PowerSchool is limited to the members of the System Administration security group.

Activity logs for the identified software are as follows:

PowerSchool – The software provides for logging of all the users access who access the software in a database table (refer to the GPPSD SIS Manual Section 3 – User Log Review)
PASI – User activity logging is maintained by the PASI site and also available to the Division level users.
Dossier and School Engage – These two systems currently do not provide for user logging.

9. Log Files
   - 9.1. Limited access: Log Files are available only to members of the System Administration Security Group.
   - 9.2. Review: Logging is tested by the SIS Coordinator or designate annually, (or following major software upgrade) to ensure correct log information is recorded
   - 9.3. Incident response: In the event of a breach or incident, the relevant log files will be examined to identify the unauthorized access to the breached system.