LOG ENTRIES IN STUDENT INFORMATION SYSTEM

Background

Greater St. Albert Catholic Schools is committed to ensuring that our students learn in safe and caring environments. An important aspect of ensuring student safety is retaining a history of incidents in which the student was involved where the student was potentially at risk or put another individual or individuals at risk. Such incidents are recorded in a factual manner with "need-to-know" information as provided by authorized users.

The collection and retention of Student Support Information is intended to serve as an important tool in communicating, on a need to know basis, with appropriate personnel, and where appropriate, parents/guardians/caregivers, community agency support services, school administration and central office personnel. This administrative procedure defines standards that govern how such log entries are to be made, but this administrative procedure is not intended to replace or serve as a substitute for the *Student Record Regulation*.

Definitions *Note: All bold-faced type refers to these definitions.*

Student Information System (SIS) is a web-based or computer-based system that contains day-to-day school information such as academic achievement, attendance, student services supports, student demographic, incident management, and student schedules. It works as a structured and accurate information exchange environment for integrating students, parents, teachers, principals, Division office staff, and Alberta Education. The current SIS used by Greater St. Albert Catholic Schools is PowerSchool but this could change from time-to-time at the discretion of the Division.

Student Support Information is personal student information including personal student-related information as defined in the *Freedom of Information and Protection of Privacy Act,* health information as defined in the *Health Information Act*, as well as any other information of a sensitive or confidential nature in a PowerSchool Log entry location to keep a record of student behaviour and where applicable, to track and identify patterns in student behavior, to modify and/or adjust prevention and/or intervention strategies, and to evaluate the success of preventative and/or intervention programming.

PowerSchool Log Entry is a record of a student's behaviour or harm-related circumstance (evidence of the medium to high risk of harm) in PowerSchool as a written record within the Log Entry section (set as a menu) that requires staff to be authorized to create a new entry or edit an existing entry as a record as per this AP 320.

Editing log entries access is the capacity to create, see, and edit current and previous log entries in PowerSchool for a student to whom a user is permitted access as an authorized user as per this AP 320.

Viewing log entries access is the capacity to see log entries for a student to whom the user is permitted access.

Authorized user is a person who is defined in this administrative procedure as having editing or viewing access to PowerSchool Log Entries for students whom they have been granted access. The authorized user must also agree to the disclaimer clause that permits access to view or create a log entry as a student record.

There are two categories of authorized users:

- **School level authorized personnel** or users are the school principal, vice-principal, current classroom teacher, and the counsellor;
- **Division level authorized personnel or users** are determined by the Assistant Superintendent of Learning Services in collaboration with the Division FOIP Coordinator based on who "needs-to-know" information about a student or students to work with school level authorized users to ensure the integrity of **Student Support Information** and to ensure students' safety and well-being.

Unauthorized user is a person who is not employed by the Division or who is not an authorized user and is not authorized to collect, access, store, retain, disclose, or dispose of student **PowerSchool log entries**.

Guidelines

1. Only **authorized users** may collect, access, use, store, retain, disclose, or dispose of the **Student Support Information** in the **PowerSchool Log Entry** for the purpose of this administrative procedure. The collection, access, use, storage, retention, disclosure, and disposal of the **Student Support Information** in the **Power School Log Entry** is restricted to authorized users on a strict "need-to-know" basis.

2. **School level authorized personnel** or users have **editing log entries access** to **PowerSchool Log Entries** for students registered in his/her school.

3. **Division level authorized personnel** or users have **viewing log entries access** to PowerSchool Log Entries for students registered in his/her Division unless the **Division level authorized user** is the PowerSchool Manager, Administrative Coordinator, PowerSchool; Data or Records Management Coordinator, Assistant Superintendent, Learning Services, and Inclusive Education Consultant- Counselling Lead, who have **editing log entries access** by necessity of their positions to address technical issues that could compromise the integrity of student support information.

4. The vice-principal, and the counsellor have "delegated authority editing access" for

students registered in his/her school. This means that the school principal, who is ultimately responsible for student programming (Section 20 of the *Education Act*) are delegating authority to an identified few staff members within the school to assist with programming responsibilities. These users are granted these privileges, but such privileges may be removed if the school principal deems that access to the student record(s) is not needed.

5. Teachers have access to record log entries for students in their current classes. These are accessed and edited on a need-to-know basis. Teacher access does not include viewing of all historical log entries, but is limited to their own log entries in the current year.

6. At no time shall personnel provide their login or email password to anyone, not even family members. Personnel who wish to collect, access, use, store, retain, disclose, or dispose of the **Student Support Information** in **PowerSchool Log Entry** must handle said information in confidence and on a "need-to-know" basis including, but not limited to, as required under the *Education Act*, the *Freedom of Information and Protection of Privacy Act*, and the *Child, Youth and Family Enhancement Act*. No personnel shall keep any **Student Support Information** that is sensitive or confidential on desks or in places where unauthorized persons or members of the public may see or have access to them.

7. Log-entries entered through PowerTeacher Pro should send a notification email to the school principal. Principals are responsible to review log entries to ensure that they meet the standards outlined in this Administrative Procedure.

8. Prior to any access into the **PowerSchool Log Entry** of the **Student Support Information** in the **PowerSchool Log Entry**, personnel must each consent to the following disclaimer:

> In clicking on the button below, I confirm that:
> a) I have read and understand Administrative Procedure 320;
> b) I hereby seek access to the PowerSchool Log Entry in relation to a Division student for work-related purposes on a need-to-know basis only;
> c) The information which I will hereby collect, access, use, store, retain, disclose, or dispose of may relate to a personal, sensitive, confidential, and/or risk-related student matter;
> d) I will not access any information in the PowerSchool Log Entry which I am not required to access in the execution of my work-related duties.

9. Log entries may contain the following information:
   - Incident in factual terms: state what happened, what and who said what; what was posted/streamed in descriptive terms and/or provide images or links to what was posted;
   - Time and location: state/provide the time(s), date (s), location(s) of the offence;
   - Student involvement: Involvement of the named student as limited to what specifically was said, done, and/or posted/streamed;

- Others involved: Involvement of other students using student initials for the first and last name and facts (what was said, done, posted/streamed);
- Names of investigators;
- Names of those notified of the incident;
- Time, date, location/media used for notification;
- Interventions: behavior plans, assessments, programs, counselling (i.e., provide need-to-know information about the plans, strategies, assessments and counselling).

10. Log entries must ***not*** contain the following information:
    - Inferences: inferences about why the student did, said, posted/streamed information;
    - Full names of students: involved other than the student named in the record;
    - Unnecessary details: that do not assist those reviewing the log entry to understand what happened, when an incident happened, or how the incident was causing harm or risk of harm (i.e., limit the information to the facts.).

Responsibilities

The superintendent and/or designate will:

- annually review user access to provide authorized users with "need-to-know" access and editing privileges and remove users who are not required access or limit users' privileges who require less than editing access;
- remove user access to PowerSchool log entries if a person was found to be an **unauthorized user** or someone who does need access or who has not followed this administrative procedure;
- provide **authorized users** with training and awareness materials as necessary to ensure that they understand their security obligations under this administrative procedure. Such training should include reference to but not be limited to the following risk management and security protocols:
    - restrict physical access to workstations to only authorized personnel;
    - secure workstations (screen lock or logout) prior to leaving area to prevent unauthorized access;
    - enable a password-protected screen saver with a short timeout period to ensure that workstations that are left unsecured will be protected;
    - comply with all applicable password policies and procedures; as per AP 140 and AP 149;
    - shall only install authorized software on workstations;
    - comply with all applicable encryption requirements;
    - ensure that anti-virus and anti-malware programs are running and up-to-date;
    - ensure that monitors are positioned away from public view;

- ensure that, where possible, the Student Support Information collected, accessed, used, stored, retained, disclosed, or disposed of under this administrative procedure should be not be stored on personal devices;
- ensure that all Student Support Information collected, accessed, used, stored, retained, disclosed, or disposed of under this administrative procedure will be maintained in accordance with the Division's general record retention practices in accordance with FOIP, and in accordance with AP 318 and AP 319;
- ensure that the Student Support Information stored in a PowerSchool Log Entry for the purpose of this administrative procedure should only be stored in PowerSchool on the Division server. Google services should **not** be used as a storage location for such information.
- ensure that any information that is no longer required for the purpose of this administrative procedure, and the retention of which is not regulated by any provincial or federal law, may be destroyed in accordance with Division's records management procedures and practices;
- provide a means for reporting privacy complaints to the Division Freedom of Information and Protection of Privacy Coordinator as per AP 170;
- conduct risk assessments which may include threat/risk assessments, privacy impact assessments or other assessments as necessary in relation to the implementation of this administrative procedure. Any risks identified by the risk assessment shall be mitigated by reasonable means.

References:

Violent Threat and Risk Assessment Protocol
Administrative Procedure 140 Use of Technology
Administrative Procedure 149 Social Media
Administrative Procedure 170 Freedom of Information
Administrative Procedure 310 Student Safety
Administrative Procedure 319 Mandated Student Records
Administrative Procedure 318 Secondary Student Records
Administrative Procedure 350 Student Conduct
Administrative Procedure 355 Use of Alcohol, Cannabis or Restricted and Illicit Drugs
Administrative Procedure 357 Vandalism by Students
Administrative Procedure 358 Harassment (Students)
Administrative Procedure 359 Safe and Caring Learning Environment for Students
Administrative Procedure 412 Occupational Health and Safety
Administrative Procedure 460 Harassment (Employees)
Freedom of Information and Protection of Privacy Act
Health Information Act,
Student Record Regulation

Implemented: October 15, 2018