Lloydminster Catholic School Division – Administrative Procedures

AP 321 – Student Information Systems

Related LCSD AP's	AP 144 – Information Security AP 145 – Network Services: MAN/Internet Access
Form(s)	Form 4.6 – Security Authorization for SDS (Schools using MySchoolSask) Form 4 - Saskatchewan Ministry of Education's *Student Tracking Security Authorization for SDS, NIPA* (General Form)
References:	*The Education Act, 1995* sections 85, 87 Saskatchewan Education Registrar's Handbook, Appendix B: "Information Security and Acceptable Use Policy".
Received by the Board: December, 2020	Update: December, 2020

Background

The Division understands the critical and legal responsibility for the protection of student information as well as the confidentiality, integrity and availability of the Division's information technology assets, software, and information. The protection of student data and student data systems will apply to each of the Division's authorized student data services as defined below.

This Administrative Procedure was developed to meet the administrative and reporting requirements regarding student information in compliance with both Alberta and Saskatchewan Ministerial regulations. The following procedures are also compliant to AP 144 Information Security.

Definitions

Student Data or Student Information Systems

For the purpose of this Administrative Procedure, "student data" refers to all information stored in each of the following:

- the Saskatchewan Student Data System (SDS);
- the Saskatchewan MySchoolSask (MSS) system;
- the Alberta Provincial Approach to Student Information (PASI);
- Follett Destiny;
- School Messenger; and,
- Bus Planner.

Confidentiality Refers to ensuring that information is accessible only to those individuals who are explicitly authorised to view it.

Integrity Refers to ensuring that information is protected from unauthorized or inadvertent modification so that it remains accurate and complete and can therefore be relied upon for use in making educational business decisions.

Availability Refers to ensuring that systems and the information that they contain are available when the end-user requires them.

These procedures are based on Saskatchewan Education's Registrar's Handbook, Appendix B: "Information Security and Acceptable Use Policy".
All personnel designated with access to Division student data are required to follow user guidelines defined in Administrative Procedure 145 – Network Services: MAN/Internet Access.

Procedures

1. Responsibilities for Division Authorized User with Access to Student Data
   - 1.1 The Chief Financial Officer, in consultation with the Division's supervisory coordinators and supervisors, will ensure Division authorized personnel with access to Division student data are annually informed regarding the potential security threats, their responsibilities in regard to those threats, and rules related to the acceptable use of the information.
   - 1.2 The following Division supervisory coordinators and supervisors include:
     - 1.2.1 Data Coordinator: Saskatchewan Student Data System (SDS);
     - 1.2.2 Data Coordinator: Saskatchewan MySchoolSask (MSS) system;
     - 1.2.3 Data Coordinator: Alberta Provincial Approach to Student Information (PASI);
     - 1.2.4 Learning Resource Coordinator: Follett Destiny;
     - 1.2.5 Division Communications Coordinator: School Messenger; and,
     - 1.2.6 Transportation Supervisor: Bus Planner.
   - 1.3 All authorized users of Division student data systems shall protect their personal access ID and password.
   - 1.4 Personnel workstations shall be protected by either logging off or locking the workstation before leaving unattended.
   - 1.5 Personnel responsible for student data shall protect information that is held outside of the system.
     - 1.5.1 The IT Department shall:
       - 1.5.1.1 Store all Network System Services 'master' passwords in a secured location in the Division Office.
       - 1.5.1.2 Store physical digital media (back-ups, etc.) containing sensitive information stored on the Division's Network System Services in a physically secure location when not in use.
     - 1.5.2 School and Division administration shall ensure paper output containing sensitive information is protected from unauthorized access (e.g. sensitive documents should not be left unattended on desktops or printers or in any other location where individuals who are unauthorized to view the contents might gain access to it).
     - 1.5.3 Sensitive information shall be destroyed when no longer required. Paper documents containing sensitive information should be shredded. Information on digital media should be permanently deleted.
   - 1.6 All Student Data System security-related incidents shall be reported to the Division's Data Coordinator who will report directly to the Director or designate. The Director, or designate, will immediately report the violation to the Registrar, including:
     - 1.6.1 Any violation of Information Security and Acceptable Use Policy (all suspicious activity must be reported);

1.6.2 Any security flaws or weaknesses discovered while accessing information stored on Saskatchewan Ministry of Education's Student Data System; and,

1.6.3 Computer virus infections.

2. The Director or designate, is responsible for promptly notifying the Saskatchewan Ministry's System Administrator when an individual authorized with Student Data System (SDS) credentials is terminated, moves to another school, or when that individual will be taking a leave (definite/indefinite). The Saskatchewan Ministry of Education's *Security Authorization for SDS (Schools using MySchoolSask/Mon Ecole Sask) (Form4.6)* will be used to communicate all changes in employee status.

3. Acceptable use of Student Data:

3.1 The **"use"** of personal information refers to the ability of school division personnel or contractors working directly with the school division to utilize the personal information the school division has collected or created. Section 27 of LAFOIP provides that personal information may be used by the Board of Education (Board) for the purpose for which it was obtained or compiled, or for a use that is consistent with that purpose. (Definition provided by: https://saskschoolsprivacy.com/central-adminstration/central-administration-summary/use-access-disclosure-of-information/)

4. Unacceptable use of Student Data includes:

4.1 Disclosing confidential information to individuals or organizations with no written or formal authority to possess that information;

4.2 Viewing or distributing data files belonging to another user unless specifically authorized to do so, regardless of whether a security weakness in the system might permit this (the ability to access information does not implicitly grant permission to view that information);

4.3 Reading another user's information files from a display terminal, as printed output or from a data storage device without that user's explicit permission.

5. Monitoring and Enforcement for the confidentiality, integrity, and Availability of Student Information.

5.1 The Division recognizes that:

5.1.1 Saskatchewan Ministry of Education has the ability to monitor individual system usage through the use of logs and other tracking tools.

5.1.2 In the interest of enforcing security and acceptable use policies, the Ministry reserves the right to employ any tool or activity necessary for monitoring, auditing and, where necessary, controlling end-users' access to the system. Monitoring and enforcement activities may include tracking of unauthorized resource access attempts.