Lloydminster Catholic School Division – Administrative Procedures

AP 321 – Student Data System

Related LCSD AP's	AP 145 – Network Services: MAN/Internet Access
Form(s)	
References:	*The Education Act, 1995* sections 85, 87 Saskatchewan Education Information Security and Acceptable Use Policy for Student Data
Received by the Board: August, 2020	Update: August, 2020

Background

The Division believes in the protection of the personal information of students as well as the confidentiality, integrity and availability of the Division's information technology assets (software and information stored on the Student Data System).

This Administrative Procedure is provided in compliance with Saskatchewan Ministry of Education direction.

Definitions

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.

The Division believes all end-users must be aware of potential security threats, their responsibilities in regard to those threats, and rules related to the acceptable use of the information.

These procedures are based on Saskatchewan Education's "Information Security and Acceptable Use Policy" manual.

All staff designated with access to the "Student Data System" will follow the user guidelines defined in Administrative Procedure 145 – Network Services: MAN/Internet Access.

Student Data System access accounts which are no longer required, or which will not be used for an extended period, will be disabled.

End-users are expected to exercise good judgment in determining whether or not a particular activity is an acceptable use of the Student Tracking Protocol of the Saskatchewan Ministry of Education Student Data System.

If any end-user or agency is found negligent, access to the department's system may be denied.

Any violation shall be subject to appropriate consequences, including a full range of disciplinary actions according to the relevant governing association as well as the potential enforcement of applicable Federal and Provincial Laws.

Procedures

1. End-User Responsibilities

    1.1 All staff shall protect network password security and Student Data System access codes.

    1.2 Staff workstations shall be protected by either logging off or locking the workstation before leaving unattended.

    1.3 Staff responsible for student data shall protect information that is held outside of the system.

        1.3.1 Digital media (CD, Diskette, back-ups, etc) containing sensitive information shall be stored in a physically secure location when not in use.

        1.3.2 Paper output containing sensitive information shall be 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).

        1.3.3 Sensitive information shall be destroyed when no longer required. Paper documents containing sensitive information should be shredded. Information on digital media should be erased.

    1.4 All security-related incidents shall be reported to the Director or designate, who will immediately report to the Registrar:

        1.4.1 Any violation of Information Security and Acceptable Use Policy (all suspicious activity must be reported);

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

        1.4.3 Computer virus infections.

2. The Director or designate, is responsible for promptly notifying the Registrar when an individual is terminated, moves to another school, or when that individual will be taking a leave (definite/indefinite) of greater than forty-five (45) calendar days. A Student Tracking Security Authorization for SDS, SGSE, NIPA (Delete Account) form will be used to communicate all changes in employee status.

3. Acceptable Use

3.1 Acceptable use of student data includes:

3.1.1 Enrolling students attending your school;

3.1.2 Withdrawing students from your school;

3.1.3 Updating student information; and

3.1.4 Printing or producing reports as required by an authorized entity.

3.2 Unacceptable use of student data includes:

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

3.2.2 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);

3.2.3 Reading another user's information files from a display terminal, as printed output or from magnetic media without that user's explicit permission;

3.2.4 Requesting or attempting to learn another individual's password;

3.2.5 Using or attempting to use another individual's account;

3.2.6 Using department computer systems as a conduit for unauthorized access attempts on remote computer systems;

3.2.7 Attempting to intercept, block, de-crypt or eavesdrop on any electronic message addressed to another individual; and

3.2.8 Developing, downloading or using programs that attempt to bypass security mechanisms or uncover security weaknesses.

4. Monitoring and Enforcement

4.1 The Division recognizes that:

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

4.1.2 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.

4.2 Every effort will be made to protect the privacy of the individual if they are monitored. Monitoring activities will be restricted to those necessary to prove or disprove allegations of inappropriate use. Knowledge of monitoring activities and results will be restricted to

Information Technology and Audit staff responsible for conducting the monitoring and those charged with making a decision based upon the findings.