	Lloydminster Catholic School Division – Administrative Procedures
	AP 144 – Information Security
Related LCSD AP's	AP145 – Network Services: MAN/Internet Access AP146 – Use of Personal Electronic Devices (PEDS) AP147 – Purchase and Use of Software AP148 – Technology Maintenance and Services AP149 – Social Media and Online Posting AP158 – Technology / Online Acceptable Use AP180 – Local Authority Freedom of Information and Protection of Privacy (LAFOIP) AP185 – Records Retention and Disposal AP321 – Student Data System
Form(s)	
References:	*The Education Act, 1995* sections 85, 87 *The Local Authority Freedom of Information and Protection of Privacy Act, 2018* sections 30, 40, 41: The Local Authority Freedom of Information and Protection of Privacy Regulations Saskatchewan Education Information Security and Acceptable Use Policy for Student Data Saskatchewan Cumulative Records Guidelines 2019: Appendix A *The Public Health Act, 1994:* Saskatchewan *Health Information Protection Act (HIPA):* Saskatchewan Alberta Education: Revised Security Controls for PASI Agreement - Schedule "A" Records Retention and Disposal Guide For Saskatchewan School Divisions: Saskatchewan School Boards Association
Received by the Board: December, 2020	Update: December, 2020

Background:

The purpose of this Administrative Procedure is to define standards for protecting the Division's information, especially sensitive and personal information, from unauthorized collection, use, disclosure, retention or destruction.

The Director, or designate, is accountable for the Division's compliance with this administrative procedure and for maintaining and updating the administrative procedure as necessary.

This Administrative Procedure applies to all the Division's employees, contractors, vendors and agents with a Division-owned device used to connect to the Division network. This Administrative Procedure applies to all matters related to employee and student access to the Division's network services, cloud storage, internet resources, and remote access connections used to do work on behalf of the Division.

A. Definitions:

- *Commercial Electronic Messages* (CEM): A CEM is defined as any message sent to an "electronic address" that has as its purpose, or one of its purposes, the encouragement of participation in a commercial activity.
- *Canadian Anti-Spam Legislation* (CASL): CASL applies specifically to "commercial electronic messages", which are defined as "any means of telecommunication, including a text, sound, voice or image message,"

B. Information Security Principles

1. Only authorized persons may have access to information held in local servers or cloud storage repositories.
2. All information must be maintained in confidence and disclosed only if authorized by either Alberta or Saskatchewan government regulation.
3. Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and the Saskatchewan School Boards Association's records management standards, procedures, and practices.
4. Each person using the Division's information services at a Division location or remotely, is responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.
5. The nature of security measures must be adequate and appropriate for the sensitivity of the information to be protected.
6. Employees will be provided with training and awareness materials as necessary to ensure that they understand their security obligations.

C. Procedures

1. The following information security procedures outline the role and responsibilities for all users related to information created and stored on both the Division's network system and cloud storage:
    - AP145 Network System Services – MAN / Internet Access
    - AP146 Use of Personal Electronic Devices (PEDS)
    - AP147 The Purchase and Use of Software
    - AP148 Technology Maintenance and Services
    - AP149 Social Media and Online Posting
    - AP158 Social Media and Online Posting
    - AP251 Digital Media Instructional Resources
    - AP321 Student Data System

2. The Chief Financial Officer will ensure all administrative personnel are annually updated regarding the Division's information security administrative procedures.
   2.1. Security controls implemented shall be supplemented by appropriate training, exercise, and user awareness materials.
   2.2. The IT Manager shall be responsible, in consultation with the Chief Financial Officer, for the network system plan, security, maintenance, and performance monitoring for all information and IT systems.
   2.3. All Division users of information and IT systems shall take responsibility for and accept the duty to actively protect school authority information and technology assets, and report IT security events and incidents.
   2.4. The Division's Data Coordinator is accountable for monitoring; and, reporting security compliance and security incidents to the Chief Financial Officer as required.

3. Employee and Student Access Credentials (username / password)
   3.1. All Division employees and students shall be provided access only to the Division's network systems they have been authorized to use. (Appendix 1)
   3.2. Access to Division's network systems shall require a secure logon process.
   3.3. Formal user registration and the registration process shall be in place for granting access to all Division network systems. The issuance of authentication credentials (username/password) shall be controlled by the IT Manager with a formal management process.
   3.4. All users shall be issued a unique username and password for their use only. The user shall protect their identification credentials issued to them from unauthorized use.
   3.5. The allocation and use of elevated privilege and special accounts for all Division network services shall be restricted and controlled by the IT Manager.
   3.6. The IT Manager shall formally review user access rates at least annually. The IT Manager shall ensure access changes are documented.

4. External business vendors and agencies shall adhere to security policies and standards established for the Division's information and IT services systems. Those requirements shall be established through contract or agreement and must include:
   4.1. Division authority security requirements shall be communicated with external business vendors and agencies prior to commencement of service delivery agreement.
   4.2. Confidentiality agreements for protecting information shall be established and reviewed regularly by the Chief Financial Officer, in consultation with the IT Manager.
   4.3. Security requirements shall be identified and addressed by the Chief Financial Officer, in consultation with the IT Manager, prior to granting external business vendors and agencies access to school authority information or IT systems.
   4.4. Information exchange procedures and controls shall be determined and implemented by contract or agreement by the Chief Financial Officer, in consultation with the IT Manager, to

protect the exchange of information between organizational entities through all types of communication services.

4.5. Information exchange agreements between the school authority and other external organizations shall be documented by the Chief Financial Officer.

5. Information transmitted by electronic messaging shall be appropriately protected by:
   5.1. Using Division devices and services to create, store, and transmit Division information to outside partners and agencies.
   5.2. Using Division network services via remote access protocols to transmit Division information to outside partners and agencies.
   5.3. Contractor or partner agencies shall not sublet any services within their contract / agreement without authorization by the Chief Financial Officer.

6. Access to IT systems and services shall be consistent with business needs and based on security requirements.

7. The IT Manager shall identify and investigate breaches of security or privacy on Division Network System Services and, in consultation with the Chief Financial Officer, shall manage the breach of security or privacy. Post-incident review shall be conducted by the Chief Financial Officer, in consultation with the IT Manager, to assess and improve the incident response plan and mitigate future information security incidents.
   7.1. All Division Administrative Procedures related to technology and information services shall be followed to determine the criticality of information and security incidents, identify appropriate responses including stakeholder communication, and manage remediation activities.
   7.2. Division Administrative Procedures have been developed to assist and guide the detection, prevention and recovery controls by the IT Manager to protect IT systems against malicious code and intrusions.

8. The IT Manager shall ensure the integrity of Division information security and privacy as required by provincial legislation, in the Division's Administrative Procedures, and, if applicable, contractual clauses, in so far as they may affect or involve confidential student and personnel data.

9. The IT Manager shall be responsible for the production, protection, and monitoring of audit logs recording user activities, exceptions, faults and information security events. Results of the monitoring activity shall be reviewed quarterly with the Chief Financial Officer.

D. Role and Responsibilities for Users of Division Technology Infrastructure

1. Mobile Phones, E-mails and Faxes: Caution must be considered by the employee when conveying confidential information over insecure technologies such as mobile phones, e-mail and faxes.

2. Secure Storage of Division Confidential Administrative Information

    2.1. Sensitive or confidential information must be stored in a secure location with restricted access, such as secure electronic storage, a locked room, or a locked filing cabinet. Security measures must be appropriate for the sensitivity of the information being stored regardless of the physical or electronic medium on which it is stored.
    2.2. Diligence must be taken when transporting or transferring sensitive or confidential information so that it reaches its intended destination intact and without unauthorized access or disclosure.

3. Disposal of information: Any information that is no longer required for either administrative, educational, financial, legal or historical purposes, and the retention of which is not regulated by any provincial or Federal law may only be destroyed in accordance with records management procedures and practices as determined by the Division (AP 185 Records Retention and Disposal).

4. Remote Access:
    4.1. It is the responsibility of each of the Division's employees, contractors, vendors and agents with remote access privileges to the Division's corporate network to ensure that their remote access connection is secure.
    4.2. All hosts that are connected to Division internal networks via remote access technologies must use the most up-to-date anti-virus software, including personal computers.
    4.3. No personal device shall be used within the Division domain to connect to the Division Intranet/MAN.
    4.4. Organizations or individuals who wish to implement Remote Access solutions to Lloydminster Catholic School Division production network must obtain prior approval from the Division.

5. Email Use
    5.1. The Division email system shall not be used for the creation or distribution of any disruptive or offensive messages. Employees who receive any emails with this content from any Division employee should report the matter to their immediate administrative supervisor immediately.
    5.2. All email sent or received by employees via Division email systems (including Office365, School Messenger), whether personal or work-related, is in the custody or under the control of the Division for records management, security and Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP) purposes. Personal email messages may be included in Division responses to LAFOIP access requests or privacy complaints. Within the parameters of LAFOIP, and any other relevant legislation, the IT Department may review files and communications to ensure system integrity and responsible use of resources.
    5.3. All email sent by employees via MySchoolsSask (MSS) email system, whether personal or work-related, is subject to Saskatchewan Education’s control for records management, security and Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP) purposes.

5.4. All email sent by employees via the Division's Follett's Destiny library email system shall be consistent with the expressed purpose of providing informational updates to parents regarding their child(ren)'s library account.

6. Canadian Anti-Spam Legislation: Canada's Anti-Spam Legislation (CASL) was enacted on July 1, 2014. CASL is federal legislation aimed at addressing the harmful effects of spam and electronic threats. The Division has incorporated a statement to clarify the manner in which schools communicate electronically with parents, students, service providers, stakeholders, organizations and others, to ensure CASL compliance.

7. Mobile Employee Endpoint Responsibility:
   7.1. This policy applies to any mobile device, or endpoint computer either issued by the Division or owned personally by an employee used for Division business which contains stored data owned by the Division.
   7.2. All employees shall assist in protecting devices issued by the Division or storing Division data. Mobile devices are defined to include but not limited to desktop computers, laptops, tablets, external hard drives, memory sticks, and cell phones.
   7.3. Portable computing devices and portable electronic storage media that contain data owned by the Division must use password protection or encryption or equally strong measures to protect the data while it is being stored.
   7.4. Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall be made aware and confirm awareness that compliance with the all applicable policies, procedures, and standards related to mobile and personal computing devices is mandatory.

8. Workstation Security:
   8.1. Workstations include: laptops, desktops, tablets and other computer-based equipment containing or accessing Division information.
   8.2. Appropriate data security measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including personal information as defined in the *Local Authority Freedom of Information and Protection of Privacy Act*, health information as defined in the *Health Information Protection Act* (HIPA) and student information as defined in the *Saskatchewan Cumulative Records 2019*, Alberta *Student Records Regulation*, as well as any other information of a sensitive or confidential nature.
      8.2.1. Employees using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.
      8.2.2. The Division will implement physical and technical safeguards for all workstations that access confidential student and employee information to restrict access to authorized users.
      8.2.3. Appropriate measures may include but are not restricted to:

8.2.3.1. Restricting physical access to workstations to only authorized personnel.
8.2.3.2. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
8.2.3.3. Enabling a password-protected screen saver with a timeout period to ensure that workstations left unsecured will be protected.
8.2.3.4. Complying with all applicable password policies and procedures.
8.2.3.5. Ensuring workstations are used for authorized business purposes only.
8.2.3.6. Never installing unauthorized software on workstations.
8.2.3.7. Storing all sensitive information, including all personal information, on network servers, not local drives, whenever possible.
8.2.3.8. Complying with all applicable encryption requirements.
8.2.3.9. Ensuring that anti-virus programs are running and up to date.
8.2.3.10. Ensuring that monitors are positioned away from public view.
8.2.3.11. If wireless network access is used, ensuring that access is secured using appropriate security measures and standards.

9. Passwords for Access to Division Network Systems and Cloud Applications Storing Data:
   9.1. The IT Department shall store all Network System Services 'master' passwords in a secured location in the Division Office.
   9.2. All system-level passwords (e.g., Division network system, applications, administration accounts, etc.) must be changed when any member of the IT Department leaves the employ of Lloydminster Catholic School Division.
   9.3. All user-level passwords (e.g., email, web, device, etc.) should be changed at least every 120 days.

10. Disaster Recovery: The decision to initiate disaster recovery procedures will be made by the Director of Education, in consultation with the IT Department and administrative personnel responsible for the data, after assessing the situation following a disaster or crisis.

11. Unacceptable Use: The following activities are strictly prohibited, with no exceptions:
   11.1. Violations of the rights of any person or the Division that are protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Division.
   11.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Division or the end user does not have an active license is strictly prohibited.
   11.3. Introduction of malicious programs into the network or server.

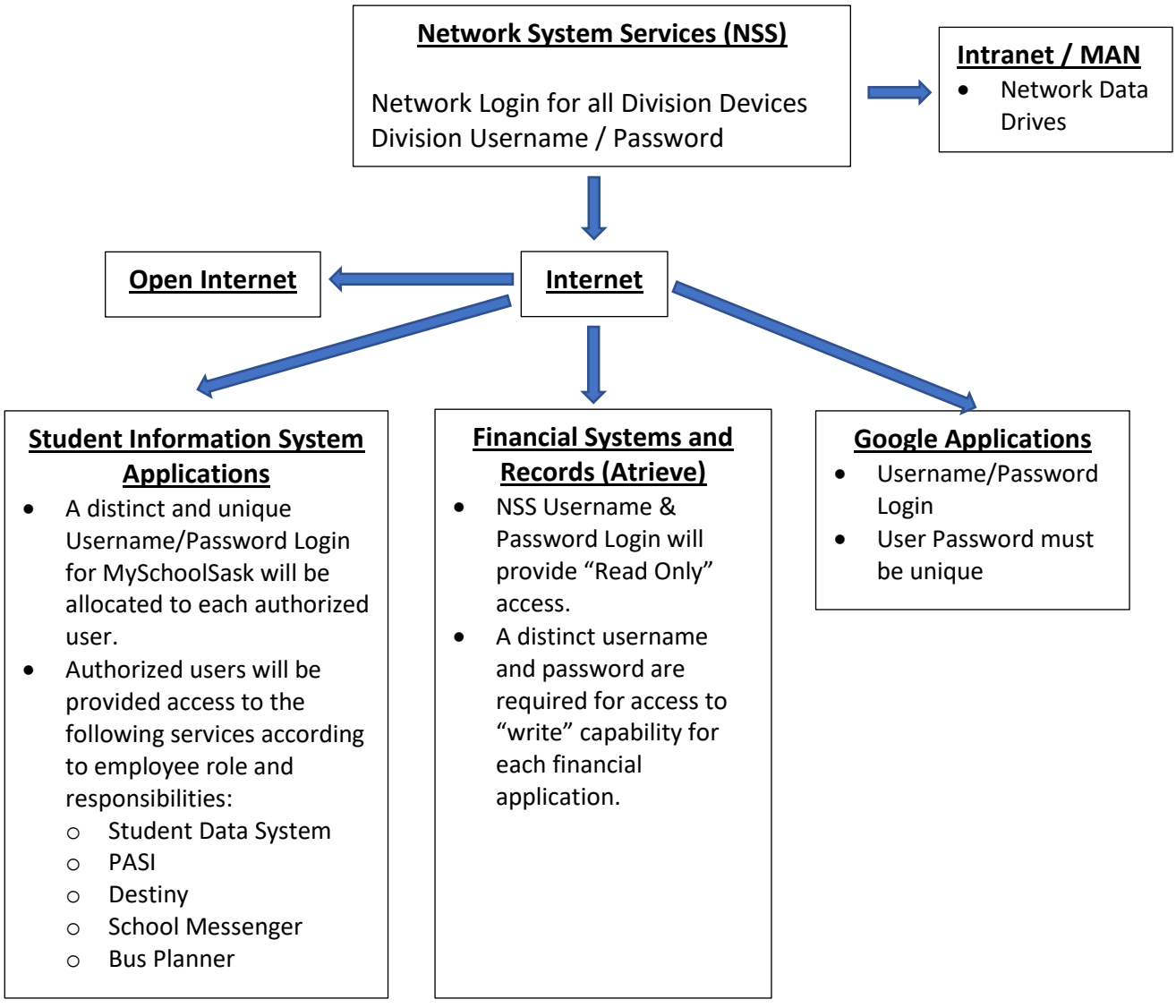
11.4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
11.5. Using a Division computing asset to actively engage in any activity that is prohibited by law or Division policy.
11.6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
11.7. Circumventing user authentication or security of any host, network or account.
11.8. Interfering with or denying service to any user other than the employee's host (e.g. denial of service attack).
11.9. Providing personal information to any third party without express authorization to do so, either as part of employment responsibilities or as authorized on a case-by-case basis.
11.10. Sending unsolicited email messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
11.11. Any form of harassment via email, text messaging, video, or telephone.
11.12. Unauthorized use, or forging, of official Division branding (e.g. Division logo, headers, etc.)
11.13. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
11.14. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
11.15. Any other activity that is not a normal part of the user's employment responsibilities with the Division unless that activity has been expressly authorized in advance.

12. Application Service Providers (ASPs): Any business process, system or application that is proposed to be outsourced to an ASP must be evaluated against the following:
12.1. In the event that Division data or applications are to be hosted or affected by an ASP, a binding contract with the ASP should fully specify the privacy and security measures to be employed to ensure that ASP services provide an acceptable level of data protection.
12.2. If the ASP provides confidential information to the Division, the Division is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. The Division's legal services department should be contacted for further guidance if questions about third-party data arise.

Appendix 1: Information Technology Access Chart

Lloydminster Catholic School Division
Information Technology Access Chart

1. Access to Division Network System Services by Full Time Employees:



2. Contracted Employee Access to Division Network System Services:

Authorized contracted employees will be provided access to the following network system services:

a. Teachers

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)
   2. MySchoolSask – The Data Coordinator will authorize access for the period of assignment in excess of two (2) days.

b. Educational Assistants

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)

c. School Secretary

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)
   2. School Office Network Drives
   3. MySchoolSask – The Data Coordinator will authorize access
   4. Bus Planner – The Transportation Supervisor will authorize access

d. Library Technicians

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)
   2. Follett Destiny – The Learning Resources Coordinator will authorize the Library Technician's access to Follett with a distinct username/password (annual).

e. Bus Driver

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services

ii. Services:
   1. Division email services (annual)

3. Substitute Employee Access to Division Network System Services:

Short-term employees who are authorized by administration to act as a substitute employee will be provided access to the following network system services:

a. Teachers

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)
   2. MySchoolSask – The Data Coordinator will authorize access for the period of assignment in excess of two (2) days.

b. Educational Assistants

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)

c. School Secretary

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)
   2. MySchoolSask – The Data Coordinator will authorize access

d. Library Technicians

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services
   2. Google Docs username/password (annual)

ii. Services:
   1. Division email services (annual)

2. Follett Destiny – The Learning Resources Coordinator will authorize access to Destiny

e. Bus Driver

i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
   1. Network System Services

ii. Services:
   1. Division email services (annual)
   2. Bus Planner: The Transportation Supervisor will authorize access to Bus Planner