	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 AP149 – Social Media and Online Posting AP180 – Local Authority Freedom of Information and Protection of Privacy (LAFOIP) AP185 – Records Retention and Disposal AP306 – Technology / Online Acceptable Use (Student) AP321 – Student Information Systems AP481 – Employee Acceptable Use of Technology
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: April, 2025	Update: April, 2025

Background:

The purpose of this Administrative Procedure is to establish guidelines and procedures to safeguard 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, students, contractors, interns, parents, volunteers, guests, and third-party vendors who connect to the Division network. This Administrative Procedure applies to all matters related to access of the Division's network services, cloud storage, internet resources, and remote access connections

A. Definitions:

Multi-factor Authentication: Is a security process that requires users to provide two or more verification factors to gain access to a system, application or account.

Personal Information: Information that, on its own or combined with other data, can identify a person and disclose personal details.

Principle of Least Privilege (PoLP): A security concept of granting users only the minimum access necessary to perform their job functions.

Single Sign-On (SSO): an authentication process that allows users to access multiple applications or systems with a single set of login credentials, improving convenience and security by reducing the need for multiple passwords.

B. Information Security Principles

1. Only authorized users may have access to information held in local servers or cloud storage repositories.
2. All Division employees and students shall be provided access only to the Division's network systems they have been authorized to use.
3. All information, in whatever format, is the property of LCSD.
4. All information must be maintained in confidence and disclosed only if authorized by either Alberta or Saskatchewan government regulation.
5. Only authorized users 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.

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
- AP149 Social Media and Online Posting
- AP306 Technology / Online Acceptable Use (Student)
- AP251 Digital Media Instructional Resources
- AP321 Student Information Systems
- AP481 Employee Acceptable Use of Technology

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 Student Records Coordinator is accountable for monitoring; the Student Information System and Ministry Databases and, reporting security compliance and security incidents to the Chief Financial Officer as required.

3. 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:
   3.1. Division authority security requirements shall be communicated with external business vendors and agencies prior to commencement of service delivery agreement.
   3.2. Confidentiality agreements for protecting information shall be established and reviewed regularly by the Chief Financial Officer, in consultation with the IT Manager.
   3.3. 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.
   3.4. 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.
   3.5. Information exchange agreements between the school authority and other external organizations shall be documented by the Chief Financial Officer.

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

5. 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.

6. 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.

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.

E. Responsibility of Users

1. All users must familiarize themselves with School Division procedures for securing and protecting information. Employees are responsible for safeguarding the information they handle, following security protocols to prevent unauthorized access, modification, disclosure, or destruction, and ensuring data integrity in their duties.

2. All users are responsible for exercising reasonable care over IT hardware, devices, and printed copies, both within School Division facilities and off premises.

3. All users are responsible for storing all important and confidential files on the metropolitan area network (MAN). The MAN is routinely backed up. Users are advised to not save files to their computer hard drives (C:) or desktop as these files are not backed up.

4. Secure Storage of Division Confidential Information
   4.1. 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. USB sticks are to be encrypted and data wiped off when the information is no longer required; promptly retrieve confidential material from a printer or photocopier, close confidential files or applications; lock the computer when leaving your workstation and safeguarding passwords.
   4.2. 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.

5. Users are to immediately report lost or stolen IT devices to techhelp and to their direct supervisor.

6. Users are responsible for immediately notifying the IT department and their direct supervisor of any known or suspected virus, technology security breach or other threat, and immediately disconnect their computer from the network or wifi.

7. 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).

8. Remote Access:
   8.1. 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.
   8.2. 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.
   8.3. No personal device shall be used within the Division domain to connect to the Division Intranet/MAN.
   8.4. Organizations or individuals who wish to implement Remote Access solutions to Lloydminster Catholic School Division production network must obtain prior approval from the Division.

9. Email Use
   9.1. 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 immediately to their immediate direct supervisor
   9.2. All emails sent or received by employees via Division email systems (including Office365, School Messenger, MySchoolSask (MSS), whether personal or work-related, is considered LCSD property. 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.

9.3. All emails 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.

10. Mobile Employee Endpoint Responsibility:
    10.1. 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.
    10.2. 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, USB sticks, and cell phones.
    10.3. 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.

11. Workstation Security:
    11.1. Workstations include: laptops, desktops, tablets and other computer-based equipment containing or accessing Division information.
    11.2. 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.
        11.2.1. Employees using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.
        11.2.2. The Division will implement physical and technical safeguards for all workstations that access confidential student and employee information to restrict access to authorized users.
        11.2.3. Appropriate measures may include but are not restricted to:
            11.2.3.1. Restricting physical access to workstations to only authorized personnel.
            11.2.3.2. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
            11.2.3.3. Enabling a password-protected screen saver with a timeout period to ensure that workstations left unsecured will be protected.
            11.2.3.4. Complying with all applicable password policies and procedures.
            11.2.3.5. Ensuring workstations are used for authorized business purposes only.

11.2.3.6. Never installing unauthorized software on workstations.
11.2.3.7. Storing all sensitive information, including all personal information, on network servers, not local drives, whenever possible.
11.2.3.8. Complying with all applicable encryption requirements.
11.2.3.9. Ensuring that anti-virus programs are running and up to date.
11.2.3.10. Ensuring that monitors are positioned away from public view.
11.2.3.11. If wireless network access is used, ensuring that access is secured using appropriate security measures and standards.

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

13. 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:
    13.1. 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.
    13.2. 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.

14. Unacceptable Use: The following activities are strictly prohibited, with no exceptions:
    14.1. 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.
    14.2. 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.
    14.3. Introduction of malicious programs into the network or server.
    14.4. 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.

14.5. Using a Division computing asset to actively engage in any activity that is prohibited by law or Division policy.
14.6. 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.
14.7. Circumventing user authentication or security of any host, network or account.
14.8. Interfering with or denying service to any user other than the employee's host (e.g. denial of service attack).
14.9. 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.
14.10. Sending unsolicited email messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
14.11. Any form of harassment via email, text messaging, video, or telephone.
14.12. Unauthorized use, or forging, of official Division branding (e.g. Division logo, headers, etc.)
14.13. 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.
14.14. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
14.15. 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.

E. Responsibility of IT Department

The IT Department is responsible for developing, maintaining, communicating and monitory information technology security systems and practices to protect the access, availability, integrity and confidentiality of information systems and data.

1. Firewalls/Internet Security – Firewalls, web and spam filters are designed to permit or deny network transmissions based upon a set of rules and are used to protect the School Division network from unauthorized access while permitting legitimate communications to pass through. IT staff monitor Internet access and other logs for threats and security breaches. If users realize a site or email address has been blocked incorrectly or should be blocked, email tech help.

2. Access to and Control of Sensitive Data – All user accounts are setup using Microsoft Active Directory. Third party applications are configured to use these same accounts where possible. Access is granted using group permissions. Access to financial systems is setup and controlled by the Finance Department. Access to the Student Information System is setup and controlled by the Student Records Coordinator. Access to the Human Resource systems is setup and controlled by the HR Administrator. Employee access is granted on the principle of least privilege. Access to employee

mail and files are only provided upon the approval of the Director of Education or designate. Once approval is received, access will be granted by submitted a request to the IT Tech Help.

3. Password Policy – the IT department will configure the following password policies to assist users with compliance
   3.1. Active Directory password policy shall follow:
      3.1.1. Student Accounts: Minimum password length six characters. Passwords are reset by IT at least once per year. Account will lock after three unsuccessful attempts for a twenty-minute duration.
      3.1.2. Staff Accounts: Minimum password length six characters. Complexity is enforced. Passwords cannot be reused. Passwords to be changed once per year. Account will lock after three unsuccessful attempts for a twenty-minute duration.
   3.2. Windows based desktops and laptops will be configured to lock after 15 minutes of inactivity
   3.3. Staff Access to accounts will require MFA
   3.4. Smartphones must require a pin or passcode to unlock. Device will wipe after 10 successful unlock attempts. Encryption enforced. Inactivity auto locking after five minutes.

4. Anti-Virus – All LCSD computers and servers have antivirus software installed. A quick virus scan is run daily on all computers and servers with a full scan run weekly. Virus definition updates are checked before each scan and are also set to automatically update ever eight hours.

5. File backup – Backups are performed nightly on all division servers and a replica of the backup is stored off-site. Regular tests are conducted of the backups to verify the integrity of the stored data.

6. Disposal or Resell of Obsolete Equipment – Disposal of all obsolete or surplus information technology hardware is done under the supervision of the IT Manager. Prior to disposal, IT staff will delete and wipe all data from the machines. Hard drives which cannot be wiped will be shredded.

7. Email Disclaimer – The following email disclaimer is added to all emails sent from the School Division email server:

   CONFIDENTIALITY WARNING: Confidentiality Notice: This email and any attachments may contain confidential information intended solely for the recipient. If you are not the intended recipient and have received this email in error, please notify the sender immediately and delete the email from your system. Unauthorized use, disclosure, or distribution of this email or its contents is prohibited.

8. 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.