	Lloydminster Catholic School Division – Administrative Procedures	
	AP 481 - Employee Acceptable Use of Technology	
Related LCSD AP's	AP 144 – Information Security AP 145 – Network Services: MAN/Internet Access AP 149 – Social Media Networking AP 180 – Local Authority Freedom of Information and Protection of Privacy	
Form(s)		
References:	*The Education Act, 1995* sections 85, 87, 175 *The Local Authority of Freedom of Information and Protection of Privacy Act, 2018*	
Received by the Board: April, 2025		Update: April, 2025

Background

The Division provides a network, including internet access for administrative and educational purposes. Employees using the Division's computer network are responsible for their behavior and communications over this network.

The Director or designate may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Staff, and stakeholders are advised that any matter created, received, stored in or sent from the Division's network (including Google Drive) or e-mail system is not necessarily private, and all material is subject to the LAFOIPP legislation of Saskatchewan. The Director or designate reserves the right to access any files to determine whether or not an employee is utilizing the network appropriately and within the guidelines of this procedure.

Procedures

Employees are expected to use the computer network in a legal and ethical manner and for the purpose of performing their duties. Use of the computer network shall be maintained in accordance with the policies and procedures of the Division and provincial and federal law.

Employees will be provided with annual training and awareness materials as necessary to ensure that they understand their security obligations.

The following procedures must be adhered to when using LCSD computing technology, networks, and online services:

1. Employees are prohibited from using the computer network for Illegal or Criminal Use:

    1.1 Staff will not attempt to gain unauthorized access to the Division system or to any other computer system through the Division system or go beyond their authorized access. This includes attempting

to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

1.2 Staff will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

1.3 Staff will not use the Division system to engage in any other illegal act defined by law.

2. System/Data Security

2.1 Staff are required to lock / logoff their computer when away from their desk

2.2 Staff will not provide access to unauthorized users of our network

2.3 Staff will not share passwords, PINS, multi-factor tokens or authentication information.

2.4 Staff will not record their password on any physical media such as a sticky note or under a keyboard.

2.5 Staff shall not store confidential student or personal material with vendors or networks not affiliated with the Division or on personally owned devices

2.6 Staff shall not redirect Division files, emails or communication to online services (third party storage, alternative or personal email accounts, etc.)

2.7 Staff must guard against targeted phishing schemes such as those that request information or actions through deceptive emails that may appear to be sent from a supervisor, familiar person, vendor or third-party. Confirm any unexpected email requests via secondary means such as by phone or in-person. All attempts are to be reported by staff to techhelp@lcsd.ca .

2.8 Staff will immediately notify the Division Office if they have identified or suspect a possible security problem.

2.9 Staff will not download or install any unlicensed software.

2.10 Staff should change their password at least once every 120 days. Passwords cannot be reused and must meet complexity requirements.

3. Inappropriate Language and Behaviour

3.1 Staff are prohibited from accessing sexually explicit or violent material not connected to curricular outcomes.

3.2 Staff will not post information that, if acted upon, could cause damage or expose the Division to significant cost or risk of liability.

3.3 Staff will not engage in personal attacks, including prejudicial or discriminatory attacks.

4. Privacy Security

4.1 Staff must adhere to privacy and data security as set out in legislation under *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP) and immediately report any privacy breach to their direct supervisor and the LAFOIP Coordinator as per AP180 Local Authority Freedom of Information and Protection of Privacy

4.2 Staff will ensure that they will not record student personal information on a third-party software program that could identify a particular student

4.3 Staff will take extra care when sending emails to parents and ensure that they have verified the recipient list prior to sending.

4.4 Only authorized staff with access to SchoolMessenger are permitted to send mass emails to parents.

5. Plagiarism and Copyright Infringement

5.1 Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

5.2 Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

6. Asset Protection
Employees will take measures to ensure hardware is safely secured and out of sight if left briefly in an unattended vehicle or public space. Hardware is not permitted to be left in a vehicle overnight.

7. Monitoring

7.1 The Board owns the computer network and reserves the right to access the contents of all files stored on the network and all messages transmitted through its computer network.

7.2 The Division maintains logs of equipment usage that may reveal information such as:

- Content of files, network activity, and communications of all Division-owned devices, regardless of their location
- Network activity and perform vulnerability scanning of all devices connecting to Division networks

Outcome of Unacceptable Use

1. Users in violation of this administrative procedure will be subject to a disciplinary process that may include:
    a. Removal of computer access and privileges
    b. Suspension, Termination
    c. Recovery of cost of damage to data or equipment

Any violation of this administrative procedure may result in disclosure and involvement of appropriate authorities.