	Lloydminster Catholic School Division – Administrative Procedures	
	AP 158 – Technology / Online Acceptable Use	
Related LCSD AP's	AP 145 – Network Services: MAN/Internet Access	
Form(s)	F 150.1 – Internet and Media Release	
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: December, 2020		Update: December, 2020

Background

The Division believes access to technology provides an opportunity for students and staff to explore, research, enhance learning, communicate and perform day-to-day operational activities. To ensure optimal learning experiences appropriate behaviour and communication are required. Generally, communications on the network are public in nature.

The Division provides a network for students and staff to conduct research and communicate with others. Independent access to network services is provided to students who agree to act in a considerate and responsible manner. Parent permission is required for all students. Access to LCSD network services is a privilege, not a right; access entails responsibility.

Individual users of the Division's network system are responsible for their behavior and communications over this network. It is presumed users will comply with Division standards, administrative procedures and will honor the agreement they have individually signed. All communications between staff, students, parents and others outside of the divisions shall not conflict with Board Policy and Administrative Procedures.

Administrative access to digital service storage areas will follow the same administrative procedures that dictate how to access a student's school locker. The Director or designate may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Staff, students and stakeholders are advised that any matter created, received, stored in or sent from the Division's network (including Google Drive) or email system is not necessarily private, and all material is subject to the Saskatchewan *Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP)*. The Director or designate reserves the right to access any files to determine whether or not an employee or student is utilizing the network appropriately and following the guidelines of this procedure.

During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

Procedures

The following procedures must be adhered to when using Division's devices, networks, and online services:

1. Personal Safety (Restrictions are for students only)

    1.1 Students will not post personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, work address, photographs, etc.

    1.2 Students will not agree to meet with someone they have met online without their parent's/teacher's approval and participation.

    1.3 Students will promptly disclose to their teacher or other school employees any message they receive that is inappropriate or makes them feel uncomfortable.

2. Illegal or Criminal Use

    2.1 Users will not attempt to gain unauthorized access to the Division system or to any other computer system through the Division network 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".

    2.2 Users 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.

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

3. Data Security for Division Network System Users

    3.1 Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no circumstances should a user provide their password to another person.

    3.2 Users are required to logout of all software upon leaving their device.

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

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

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

    3.6 Users will immediately notify the IT Manager if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.

    3.7 Users shall not download software onto a Division device without the IT Manager's authorization.

4. Inappropriate Language and Behaviour

    4.1 Restrictions against inappropriate language apply to public messages, private messages, and material posted on web pages.

4.2 Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

4.3 Users will not post information that, if acted upon, could cause damage or a danger of disruption.

4.4 Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

4.5 Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.

4.6 Users will not knowingly or recklessly post false or defamatory information about a person or organization.

5. Respect for Privacy

5.1 Users will not post/share private information and photos about another person.

5.2 Users will not re-post a message/photo that was sent to them privately without permission of the person who sent them the message.

6. Respecting Division Network System Services and Devices

6.1 Users will use the Division's network system for educational and professional or career development activities.

6.2 Student users will not download files onto LCSD devices without permission from the teacher.

6.3 Users will not post chain letters or engage in "spamming" (i.e. sending an annoying or unnecessary message to a large number of people).

6.4 Users will check their email frequently and delete unwanted messages promptly.

6.5 Users will only subscribe to high quality online services that are relevant to their education or professional / career development.

7. Plagiarism and Copyright Infringement

7.1 Users will not plagiarize work 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.

7.2 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.

8. Inappropriate Access to Material

8.1 Users will not use the Division's system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made for hate literature if

the purpose of such access is to conduct research and the access is approved by both the teacher and the parent. Division employees may access the above material only in the context of legitimate research.

8.2 If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated this protocol.

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 Division network system access and privileges
    b. Suspension, expulsion or termination
    c. Cost recovery for damage to Division data, devices, or other technology equipment

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