	Lloydminster Catholic School Division – Administrative Procedures
	AP 306 – Technology / Online Acceptable Use (Student)
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 believes that technology provides an opportunity for students to explore, research, enhance learning and communicate. Independent access to network services is provided to students who agree to act in a considerate and responsible manner. Parental permission is required for all students. Access to LCSD network services is a privilege, not a right.

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

Students are advised that any matter created, received, stored in or sent from the Division emails (including Google Drive) is not necessarily private. The Director or designate reserves the right to access any files to determine whether or not a student is utilizing the network appropriately and within the guidelines of this procedure.

During school, teachers will guide students 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

Students are expected to adhere to the following procedure when using LCSD computing technology, networks, and online services:

1. Personal Safety

    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.

1.4 Students will not start chat groups without the knowledge and approval of a teacher or Principal.

2. Illegal or Criminal Use

2.1 Students 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".

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

3. System/Data Security

3.1 Students 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 Students are required to logout of all software upon leaving their device

3.3 Students will immediately notify their Teacher 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.

4. Inappropriate Language and Behaviour

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

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

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

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

4.5 Students 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 Students will not knowingly or recklessly post false or defamatory information about a person or organization.

5. Respect for Privacy

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

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

6. Plagiarism and Copyright Infringement

   6.1 Students 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.

   6.2 Students 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.

7. Inappropriate Access to Material

   7.1 Students 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.

   7.2 If a student 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.

8. Hardware

   8.1 Students shall not destroy, modify or abuse Division hardware or software. Intentionally altering the files and/or the hardware on school computers will be viewed as vandalism. Vandalism also includes the uploading or creation of computer viruses. Each student will be held responsible for the intentional altering of a computer that occurs while they are logged onto that computer or network.

9. Monitoring

   9.1 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.

Outcome of Unacceptable Use

1. Students 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 or expulsion
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.