THOMAS MACLAREN SCHOOL

Internet Acceptable Use
Approved March 17, 2022

At Thomas MacLaren students have supervised access to the Internet for research and projects. For example, students in Geography may research a state for their state project or students in math may be directed to go to a website that will allow differentiated study for that hour of instruction.

While it is impossible to predict with certainty what information students might locate or come into contact with, the School shall take reasonable steps to protect students from accessing material and information that is illegal, obscene, pornographic, or otherwise harmful to students. Students shall take responsibility for their own use of School resources and computer systems to avoid contact with material or information that may be harmful. This policy applies to the use of Maclaren devices whether they are used at school or at home.

Student use is a privilege
Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student use of the Internet and electronic communications is a privilege, not a right. Failure to follow the use procedures contained in this policy shall result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result in school disciplinary action, including suspension or expulsion, and/or legal action. The School may deny, revoke or suspend access to School technology or close accounts at any time.

A parent or guardian shall be required to sign the School's Acceptable Use Agreement annually as part of the enrollment process before Internet or electronic communications accounts shall be issued or access shall be allowed.

Blocking or filtering obscene, pornographic and harmful information
A system that blocks or filters material and information that is obscene, pornographic, or otherwise harmful to minors shall be installed and maintained on the network for all School devices having Internet or electronic communications access through the School network. In the event that inappropriate material is accessed, the students shall report it to the supervising staff member. If a student becomes aware of other students accessing such material or information, he or she shall report it to the supervising staff member.

No expectation of privacy
School devices and computer systems are owned by the School and are intended for educational purposes at all times. Students shall have no expectation of privacy when using the Internet or electronic communications. The School reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of School computers and computer systems, including all Internet and electronic communications access and transmission/receipt of materials, computer files and information. Personal consent to monitor is required before a user account is activated. All material and information accessed/received through School devices and computer systems shall remain the property of the School.

Unauthorized and unacceptable uses
Students shall use computer systems and devices within the school in a responsible, efficient, ethical, and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of school computer systems and devices cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following:

- The use of computers and Internet access at MacLaren is for educational purposes only. No private communications are acceptable using school property.
- No MacLaren computer or network may be used for advertisement, personal websites, or political lobbying.
- No student shall access, create, transmit, retransmit, or forward material or information:
    - that contains personal information about themselves or others, including information protected by confidentiality laws
    - that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
    - that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the School's nondiscrimination policies
    - that uses inappropriate or profane language likely to be offensive to others in the school community
    - that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion
    - that is knowingly false or could be construed as intending to purposely damage another person's reputation
    - that plagiarizes the work of another without express consent
    - for personal profit, financial gain, advertising, commercial transaction or political purposes
    - in violation of any federal or state law, including but not limited to copyrighted material and material protected by trade secret
    - using another individual's Internet or electronic communications account
    - that impersonates another or transmits through an anonymous remailer
    - that accesses fee services without specific permission from the system administrator

Protection of assets
The School makes a significant investment in the hardware checked out for student use. Students have a responsibility to care for this equipment. For example, students should not use food or drink near school equipment; they should carry devices carefully; they should not expose School equipment to extreme weather conditions. Students will be charged a fee should devices be damaged.

Vandalism
Vandalism will result in cancellation of privileges and may result in school disciplinary action, including suspension or expulsion, and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt operation of any network within the School or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or School-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Unauthorized software
Students are prohibited from installing or using any software on School computer systems or devices that has been downloaded or is otherwise in the user's possession without prior approval and consent of a School system administrator, and appropriate registration and payment of any fees owed to the software owner.

Assigning student projects and monitoring student use
The School will make reasonable efforts to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers, and staff have a professional responsibility to work together to monitor students' use of the Internet and electronic communications, help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet their educational goals. Students shall have specifically defined objectives and search strategies prior to accessing material and information on the Internet and through electronic communications.

Security
Security on School computer systems and devices is a high priority. Students who identify a security problem while using the Internet or electronic communications must immediately notify their Head of School. Students should not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Students shall not:

- use, capture, or reveal another person's password or any other identifier
- gain or attempt to gain unauthorized access to School computers or computer systems
- read, alter, delete or copy, or attempt to do so, electronic communications of other system users
- connect, or attempt to connect, any personal devices of any kind to the School network without prior knowledge and authorization of the School system administrator
- modify, or attempt to modify, the configuration or settings of School computers or network devices without prior knowledge and authorization of the School system administrator

Any student identified as a security risk, or as having a history of problems with other computer systems, may be denied access to the Internet and electronic communications.

Safety

In the interest of student safety, the School shall educate students about appropriate online behavior and potential risks, including cyberbullying awareness and response, and interacting on social networking sites and in chat rooms.

Students shall not reveal personal information, such as home address or phone number, while using the Internet or electronic communications. Without first obtaining permission of the supervising staff member, students shall not use their last name or any other information that might allow another person to locate him or her. Students shall not arrange face-to-face meetings with persons met on the Internet or through electronic communications.