

Administrative Procedure 140 – Appendix

APPROPRIATE USE EXPECTATIONS

Educational Objective

Internet access and other computer and network resources are available to students and staff of Evergreen C.S.R.D. No. 2. We are very pleased to provide this access and believe that the Internet offers vast, diverse and unique resources to both students and teachers and have endorsed the use of technology to support teaching and learning. Our goal in providing this service is to promote education excellence in schools by facilitating resource sharing, innovation and communication. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The Division has taken reasonable precautions to monitor access to controversial materials. However, in an environment where internet access is ubiquitous it is impossible to control all access points available to users. We firmly **believe that the valuable information** and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of Evergreen Catholic Schools. We also believe that computer security cannot be achieved by specialists and security software alone. Computer security is an individual responsibility that requires commitment, responsibility and involvement of everyone dealing with information.

The use of the Internet and the computer and network resources of the Division is a privilege, not a right, and inappropriate use will result in revocation of those privileges. We expect students and staff to adhere to the expectations set out below.

Definition

In this Appendix, "Division resources" means Evergreen C.S.R.D. No. 2's entire computer and digital media network, including but not limited to: computers, file servers, application servers, communications server, mail servers, fax servers, Web servers, work stations, stand-alone computers, laptops, smartphones, web/video conferencing equipment, software, data files, Wi-Fi, and all internal and external computer and communications networks (for example, Internet, value-added networks, e-mail systems) whether connected using Division computers, personal computers or personal communication devices.

Expectations

- 1. Users will use Division resources to review and download only information or images which are classroom related, have educational value and are consistent with the Division's educational goals.**
- 2. Users will use Division resources for legal purposes only. Any illegal activity on Division resources, including but not limited to matters listed below, may be reported to law enforcement.**
- 3. Users will not use Division resources to access, download, save, display, send or receive any inappropriate material.**

Inappropriate material includes anything which is:

- sexually explicit,
- hateful or discriminatory based on sex, race, religion, origin, sexual orientation, etc.
- offensive
- profane or using profane language
- harassing or intimidating,
- illegal
- otherwise not appropriate for school.

4. **Users will not use Division resources for personal or commercial gain, or to sell anything, except if it is for a school project.**
5. **Users will not use Division resources to bully or harass any person.** Bullying is more than just physical – it includes personal attacks, intimidation, gossiping, humiliating, negative comments, threats, harassment, foul and abusive language, attempts to “fill” electronic mailboxes, the posting of obscene messages or texts, and other unkind online activity. These types of behaviours by students may lead to much more severe discipline under our schools’ discipline policy.
6. **Users will not vandalize any Division resources, or try to break security.** This includes damaging or infecting any computer hardware, software, network, or information on them, including creating computer viruses. Users will not attempt to access any users’ information, or any other “hacking” activity, or attempt to access any material from which they are blocked.
7. **Users are not authorized to download or install software on hard drives or the network.** No unauthorized software may be installed, downloaded or used on **Division resources**. Any software found in a user’s home directory may be removed and will be considered a breach of the user’s Acceptable Use Agreement.
8. **Users will not download music, video, games or any software on Division resources, unless specifically allowed for a school project.**
9. **Users will not use Division resources to play games, including Internet games, or access Internet gambling sites**
10. **Users will respect the copyright on all material accessed by the Internet, and will not illegally download material.** Users will not illegally copy material protected under copyright law, or make that material available to others for copying, including software, music or video files, or software obtained in violation of the appropriate vendor’s licence agreement. All materials from the Internet should be cited, just as you would cite other materials.
11. **Users may not waste, monopolize or disrupt Division resources.** This may include excessive printing, excessive amounts of time on the internet, playing games, streaming of video and music, VoIP, or many other internet activities.
12. **Users will follow accepted rules of “netiquette”.** These include (but are not limited to) the following:

- Users will be polite. Do not be abusive in your messages to others.
- Users must use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Substituting symbols (i.e. \$, #, %, *) in place of letters as part of such words, or other attempts to mimic inappropriate language, is also inappropriate.
- Users must not reveal personal information about themselves or others over the Internet, such as your name, phone number or address.

13. Users will use digital devices only designated areas identified by school administration.

13. Security Expectations

13.1 Appropriate password guidelines are to be followed:

13.1.1 No passwords may be given out to anyone. Staff members, teachers or Technical Services will not request your password for any reason.

13.1.2 Technical Services does not retain a list containing passwords. No username and password lists may be maintained anywhere in the Division.

13.1.3 If a password is forgotten, the password will be reset to the Division password default and the user will be required to change his/her password on next login.

13.1.4 Email passwords for new accounts will be set to the Division password default and the user will be required to change his/her password by visiting <https://ecsr.d.ab.ca:7443/cgi/user.cgi> and logging in with their username and the Division password default.

13.1.5 Forgotten email passwords will be reset to the Division default password by Technical Services.

13.1.6 All passwords must meet minimum password length requirements of six (6) characters.

13.1.7 Kindergarten students will have network access through a global username and password combination which cannot be modified.

13.1.8 Grade 1 and Grade 2 students will have network access through a unique username and password combination but will not be required to change their password or be required to select a password that meets the password length requirement.

13.1.9 Grades 3 to 8 will have network access through a unique username and password combination but will not be required to change their password,

but will be required to select a password that meets the password length requirement.

13.1.10 Grades 9 to 12 and staff must change their password every forty-five (45) days, and will be automatically prompted to do so by the network as the forty-five (45) day deadline approaches.

13.2 Network accounts are to be used only by the authorized owner of the account for authorized purposes. The user's login password must be kept private. Do not reveal passwords, personal addresses or phone numbers of yourself or others. Users are responsible for any traffic through their account as well as any data found in their home directory.

14. **It is the responsibility of each user to make good decisions as to what information is retrieved and what is done with that information.** No liability will be assumed by the Division or any Division employee for any user's use or misuse of the system.

15. **Users agree to report any observed violation to the Network Administrator immediately.** If a user feels s/he can identify a security problem or vulnerability in the computer system, s/he agrees to notify a staff member immediately. The user agrees not to demonstrate the problem to others.

Reference: Section 12, 60, 61, 113 School Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
ATA Code of Professional Conduct