

DISTRICT-WIDE NETWORK AND INTERNET APPROPRIATE USE

Background

School District No.43 (Coquiltam)'s District-wide network provides data communication links among all District sites and a high-speed connection to sites outside the District including the "Internet". Internet services and technologies offer valuable learning experiences for students and sources of information for teachers. At the same time, there are potential hazards. Students may receive offensive communications and may access material which is not appropriate. As with other methods of communication, there are opportunities with computer networks for students to create and distribute inappropriate materials and to conduct themselves in ways that are unacceptable. Therefore, the District is obliged to inform parents of potential risks and benefits, and impose rules on what students see and do.

Our primary business purpose is the education of our students; therefore, business and administrative use of District computers is intended for the direct support of the District's operation.

Access to the Internet is available through use of electronic mail and the World-Wide Web (WWW) and is provided to staff members to assist in the performance of their work.

The District does not permit the use of its computers and networks to create, distribute, or access any material which would not be considered suitable for any sector of our clientele, particularly students. Inappropriate use of District computers has the potential to cause severe public embarrassment and damage the trust relationship that we have with our public. Users must avoid accessing sites that might bring the District into disrepute. Internet usage must be able to survive public scrutiny and/or disclosure. Users must comply with all applicable laws and regulations and must respect the legal protection provided by copyright and licenses with respect to both programs and data.

In providing Internet access for students the District also affirms that it will not permit the creating, distributing, or accessing of any material which is not suitable for classroom learning.

Procedures

The following procedures are therefore intended to ensure appropriate use. Inappropriate behaviors may lead to disciplinary action for students under the District Code of Conduct for Students, corrective action up to and including termination for staff, and/or suspension or limitation of network access privileges:

1. The District's local and wide area networks are intended only for educational purposes and for the business and administrative functions directly in support of the District's operation.

2. Network services, and access to these services shall only be used by authorized persons. Where password-protected accounts are used, network users are personally responsible for all activity that occurs within their account. Where possible, students are to have their own password-protected account and teachers are not to permit students to operate under the teacher's account. Teachers are expected to take all reasonable precautions to ensure that their students are not accessing inappropriate material on the Internet.
3. When interacting with other users on the District-wide network or Internet, users are expected to behave as they would in any other environment where they represent their school. It is important that users conduct themselves in a responsible, ethical, and polite manner in accordance with the standards of propriety in the District.
4. Using the District's networks and the Internet for illegal, obscene, harassing or inappropriate purposes, or in support of such activities, is prohibited.
5. The District's networks are shared resources and must be used in moderation. From time to time, users may be asked to limit or relinquish access to high priority processes or to accommodate others.
6. Users are advised that computer systems (and files/records including email records) are District property and may be inspected or monitored at any time if misuse is suspected.
7. All above rules apply whether District network access is gained from in or out of school/work settings and/or school/work time.
8. Inappropriate use of network services includes, but is not limited to, the following:
 - 8.1 Users may not use the District's networks or computing equipment to:
 - 8.1.1 transmit any materials in violation of Canadian laws
 - 8.1.2 download, duplicate, store, or transmit pornographic materials
 - 8.1.3 transmit or post threatening, abusive, obscene or harassing material
 - 8.1.4 duplicate, store, or transmit copyrighted material that violates copyright law
 - 8.1.5 participate in pyramid schemes or chain mail
 - 8.1.6 harassment of other users
 - 8.2 Users may not violate, or attempt to violate, the security of the District's computers, data or network equipment or services. Users must not attempt to obscure the origin of any message or download materials under and assumed Internet address.
 - 8.2.1 Any attempts at unauthorized access of District data is prohibited and will result in termination of the user's computer and network privileges.
 - 8.2.2 Any attempt to vandalize District network accounts or systems is prohibited and will result in termination of the user's computer and network privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another member, the District, or any of the

agencies or other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses.

8.2.3 Use of another individual's password-protected account is prohibited.

8.2.4 Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the District's networks and services.

8.3 Users may not:

8.3.1 use abusive, vulgar, profane, obscene, harassing, or other inappropriate language;

8.3.2 criticize the spelling, writing or keyboarding of others;

8.3.3 re-post personal electronic mail received to public forums (e.g., listserves, newsgroups) without the permission of the author.

8.3.4 share password(s) with others;

8.3.5 distribute or use anyone else's account name and password;

8.3.6 reveal anyone else's personal address, phone number, or picture without their consent, except as required in the course of one's duties;

8.3.7 use network access for business purposes or anything else not related to the individual's position in the District.

8.3.8 Transmit or expose to Internet access, personal, confidential or protected information which is reasonably likely to be excepted or excluded from access under the Freedom of Information and Protection of Privacy Act.

9. Schools will, where and when appropriate, ensure that the Student Internet Registration Form (Form 140-1) is completed and signed.

Reference: Section 65, 85, School Act
Form 140-1 Student Internet Registration Form

Board Minutes

June 1997 Volume 39 Page 85 Policy II-B-77

June 2005 Volume 47 Page 78 AP 140