for CEAP Blended or Distance Learners...

Technology & Internet Use Guidelines

Rationale

School District #69 (Qualicum)'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 Board is obliged to inform parents of potential risks and benefits, and impose governance on what students see and do.

Policy

The Board of Education believes that the Internet is a valuable resource for students, teachers and employees; and that understanding and being able to make effective use of the Internet is a key skill in our technological society. Therefore, the Board of Education has provided access to the Internet through the district computer network to meet learning, program and department goals. Furthermore, the Board of Education believes that appropriate use of computer networks by students is the shared responsibility of students, parents, and teachers.

CEAP Network and Internet Appropriate Use Guidelines

Following is a list of guidelines and a list of specific behaviors that may lead to disciplinary action under the CEAP Code of Conduct, 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 school 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.

(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.

(6) Users are advised that computer systems 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 settings.

(8) Inappropriate use of network services includes, but is not limited to, the following:

(a) Users may not use the District's networks or computing equipment to:

- Transmit any materials in violation of Canadian laws
- Duplicate, store, or transmit pornographic materials
- Transmit or post threatening, abusive, obscene or harassing material
- Duplicate, store, or transmit copyrighted material that violates copyright law
- Participate in pyramid schemes or chain mail harassment of other users

(b) Users may not violate, or attempt to violate, the security of the District's computers, data or network equipment or services.

- Any attempts at unauthorized access of District data will result in termination of the user's computer and network privileges.
- Any attempt to vandalize District network accounts or systems 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.
- Use of another individual's password-protected account is prohibited.
- 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.

(c) Users may not:

- Use abusive, vulgar, profane, obscene, harassing, or other inappropriate language;
- Criticize the spelling, writing or keyboarding of others;
- Re-post personal electronic mail received to public forums (e.g., listserves, newsgroups) without the permission of the author.

(d) Users may not:

- Share password(s) with others;
- Distribute or use anyone else's account name and password;
- Reveal anyone else's personal address, phone number, or picture without parental consent;
- Use network access for business purposes or anything else not related to the individual's position in the district.