Cascade School District No. 422

STUDENTS **3270**

District-Provided Access to Electronic Information, Services, and Networks

General

Internet access and interconnected computer systems are available to the District's students and faculty. Electronic networks, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

In order for the District to be able to continue to make its computer network and Internet access available, all students must take responsibility for appropriate and lawful use this access. Students utilizing school-provided Internet access are responsible for good behavior on-line. The same general rules for behavior apply to students' use of District-provided computer systems. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the District's teachers and other staff will make reasonable efforts to supervise use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Curriculum

The use of the District's electronic networks shall be consistent with the curriculum adopted by the District, as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students. Staff members may, consistent with the District's educational goals, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Uses

1. **Primarily for Educational Purposes:** The District provides students with an electronic network to support education and research and for the conduct of school business. Student personal use of computers that is consistent with the District's educational mission may be permitted during class when authorized by a student's teacher or appropriate administrator. Personal use of District computers and networks outside of class is permissible, but must comply with District policy. Use is a privilege, not a right. Students have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to access, monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage, including email and instant messages.

2. **Unacceptable Uses of Network.** The following are considered unacceptable uses and constitute a violation of this policy: Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

   A. Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages; offering for sale, use, or purchase any substance the possession or use of which is prohibited by the District's student discipline policy, local, State, or federal law; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate local, State, or federal law; information pertaining to the manufacture of weapons; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials;
   B. Uses that cause harm to others or damage their property, person, or reputation, including but not limited to engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating; reading another person's communications; sharing another person's pictures, private information, or messages without their permission; or otherwise using his or her access to the network or the internet;
   C. Uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information. Users will immediately notify the school's system administrator 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.
   D. Uses amounting to harassment, sexual harassment, bullying, or cyber-bullying defined as using a computer, computer system, or computer network to convey a message in any format, including audio or video, text, graphics photographic, or any combination thereof, that is intended to harm another individual.
   E. Uses that jeopardize the security of student access and of the computer network or other networks on the internet; uses that waste District resources including downloading very large files without permission from a teacher, unnecessary printing, and consuming excess file space on shared drives.
   F. Uses that are commercial transactions, including commercial or private advertising. Students and other users may not sell or buy anything over the internet. Students and others should not give personal information to others, including credit card numbers and social security numbers.
   G. The promotion of election or political campaigns, issues dealing with private or charitable organizations or foundations, ballot issues, or proselytizing in a way that presents such opinions as the view of the District.
   H. Sending, receiving, viewing, or downloading obscene materials, materials harmful to minors, or materials that depict the sexual exploitation of minors.
   I. Disclosing identifying personal information or arranging to meet persons met

on the internet or by electronic communications; sharing one's password with others or allowing them to use one's account.

J. Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee.
K. Posting or sending messages anonymously or using a name other than one's own.
L. Attempting to bypass internal or external security systems or controls using District equipment. Students and staff may only access the internet using the District network.
M. Plagiarism of material accessed online. Teachers will instruct students in appropriate research and citation practices
N. Using the network while access privileges are revoked.

Internet Safety

Each District computer with Internet access is subject to filtering at the internet gateway that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate and/or harmful to students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The school will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or other material that is inappropriate and/or harmful to minors. The Superintendent or designee shall enforce the use of such filtering devices.

The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that:

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Internet Filtering

Filtering should only be viewed as one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It should not be viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors. Anything that falls under at least one of the categories below shall be blocked/filtered. This list will be updated/modified as required.

- Nudity/ pornography – prevailing U.S. standards for nudity, provocative semi-nudity, sites which contain pornography or links to pornographic sites
- Sexuality – sites which contain material of a mature level, images or descriptions of sexual aids, descriptions of sexual acts or techniques, sites which contain inappropriate personal ads
- Violence – sites which promote violence, images or description of graphically violent acts, graphic autopsy or crime-scene images
- Crime – information of performing criminal acts (e.g., drug or bomb making, computer hacking), illegal file archives (e.g., software piracy)
- Drug Use – sites which promote the use of illegal drugs, material advocating the use of illegal drugs (e.g. marijuana, LSD) or abuse of any drug. Exception: material with valid-educational use
- Tastelessness – images or descriptions of excretory acts (e.g., vomiting, urinating), graphic medical images outside of a medical context
- Language/Profanity – passages/words containing profanity within images/sounds/multimedia files, adult humor
- Discrimination/Intolerance – Material advocating discrimination (e.g., racial or religious intolerance), sites which promote intolerance, hate or discrimination
- Interactive Mail/Chat – sites which contain or allow inappropriate email correspondence, sites which contain or allow inappropriate chat areas
- Inappropriate Banners – advertisements containing inappropriate images or words
- Gambling – sites which allow or promote online gambling
- Weapons – sites which promote illegal weapons, sites which promote the use of illegal weapons
- Body Modification – sites containing content on tattooing, branding, cutting, etc.
- Judgment Calls – whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

Filtering should also be used in conjunction with:

- Educating students to be "Net-smart;"
- Using "Acceptable Use Agreements;"
- Using behavior management practices for which Internet access privileges can be earned or lost; and
- Appropriate supervision, either in person and/or electronically.

The system administrator and/or building principal shall monitor student Internet access. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 18 and older.

Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and social security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

Computer Access Conduct Agreements

Each student and his/her parent(s)/legal guardian(s) will be required to sign and return to the school the Computer Access Conduct Agreement prior to having access to the District's computer system and/or Internet Service.

Warranties/Indemnification

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. The District will not be responsible for any unauthorized charges or fees resulting from access to the Internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event of the school's initiating an investigation of a user's use of his/her access to its computer network and the Internet.

Violations

If any user violates this policy, the student's access will be denied, if not already provided, withdrawn, or curtailed and he/she may be subject to additional disciplinary action. The system administrator and/or the building principal will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, suspend, or limit access at any time, with his/her/their decision being final.

Policy History:
Adopted on: 7/15/09
Revised on: 11/11/09, 10/15/14, 3/15/17 , 9/30/19