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 users, including students must take responsibility for appropriate use. The same general rules for behavior apply to students' use of District-provided computer systems. The District's teachers and other staff will make reasonable efforts to supervise use of network and Internet access.

Curriculum

In accordance with this policy and the Board's philosophy to ensure the safety of all students, the District shall provide an appropriate planned instructional component for Internet safety which shall be integrated into the District's regular instructional program. The purpose of the program is to educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

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, and shall comply with the selection criteria for instructional materials and library-media center materials. Staff members will, consistent with the District's educational goals, use the Internet throughout the curriculum.

Acceptable Uses

1. **Educational Purposes Only.** Use of the District's electronic network must be (1) in support of education and/or research, and in furtherance of the District's stated educational goals; or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members 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 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.

2. **Unacceptable Uses of Network.** The following are considered examples of 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 or use 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; 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 to 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 the actual sender is communicating, or otherwise using his/her access to the network or the Internet; 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.
   C. 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 (audio or video, text, graphics photographic, or any combination thereof) that is intended to harm another individual.
   D. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.
   E. Uses that are commercial transactions. Students ~~and other users~~ may not sell or buy anything over the Internet. Students and others should not give information to others, including credit card numbers and social security numbers.
   F. Sending, receiving, viewing or downloading obscene materials.
   G. Students are prohibited from joining chat rooms unrelated to online classes, using school equipment or school systems for any such activity, unless it is a teacher-sponsored activity with building administrator approval.

<u>Plagiarism and Copyright Infringement</u>

A. Students will not plagiarize works that are found on the network or Internet. Plagiarism is taking the ideas or writings of others and presenting them as original thought.

B. Students will respect the rights of copyright owners. Copyright infringement occurs when a person inappropriately reproduces a work or loads software that is protected by copyright, without owner's permission. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If unsure whether or not a work may be used, permission should be requested from the copyright owner. Direct any questions regarding copyright law to a teacher.

Rights

A. Free Speech – Rights to free speech, as set forth in the school disciplinary code, applies also to communication on the Network. The Network is considered a limited forum, and therefore the District may restrict rights to free speech for valid educational reasons. The District will not restrict rights to free speech on the basis of its disagreement with expressed opinions.

B. Search and Seizure – Students should expect no privacy of the contents of personal files on the District system. Routine maintenance and monitoring of the system may lead to discovery that policies, school code, or the law have been violated. An individual search may be conducted if there is reasonable suspicion that a student has violated this policy, the school disciplinary code, or the law. The investigation will be reasonable and related to the suspected violation.

C. Due Process. The District will cooperate fully with local, state, or federal officials in any investigation related to illegal activities conducted through the school district computers. In the event of a claim that a student has violated this policy, the school disciplinary code, or the law in use of the school district computers (Network), he or she will be given written notice of suspected violations and an opportunity to present an explanation according to school code and/or state and federal law. Additional restrictions may be placed on his or her use of the Network Account.

Internet Safety

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for 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 for 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]), and also defined in Section 18-1514(6), Idaho Code

Internet Filtering

Filtering is only one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It is not 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 that have no educational value, 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 too coarse to be softened by the word filter, 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 recognized Internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
- 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 Director of Technology and/or designee 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.

Review of filtering technology and software shall be done on a periodic basis and is the responsibility of the Director of Technology. It shall be the responsibility of the Director of Technology to bring to the Board any suggested modification of the filtering system and to address and assure that the filtering system meets the standards of Idaho Code 18-1514 and any other applicable provisions of Chapter 15, Title 18, Idaho Code.

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.

Internet Access Conduct Agreements

Each student and his/her parent(s)/legal guardian(s) will be required to sign and return to the school at the beginning of each school year the Acceptable Use Policy 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 to the school's internet system and computers will be denied, if not already provided, or withdrawn and he/she may be subject to additional disciplinary action. The Director of Technology, teacher, and/or the building administrator will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his/her/their decision being final. Actions which violate local, state or federal law may be referred to the local law enforcement agency.

If the actions of the individual are also in violation of other District discipline policies, said student shall be subject to additional possible disciplinary action based upon these policies.

Public Notification

The Director of Technology shall inform the public via the main District webpage of the District's procedures regarding enforcement of this policy and make them available for review at the District office.

Submission to State Department of Education

This policy shall be filed with the State Superintendent of Public Instruction no later than August 1, 2011 and every five (5) years after initial submission and subsequent to any edit to this policy thereafter.

Cross Reference: 3255 Student Conduct Code

Legal Reference: I.C. § 33-132 Local school boards internet use policy required

Communications Act of 1934 (47 USC Section 254 [h][7])

Section 18-1514(6), Idaho Code

Policy History:
Adopted on: July 27, 2011
Revised on: August 14, 2012