Policy Title: Employee District-Provided Access to Electronic Information, Services, and Networks **Policy No: 401.21.2**

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 and lawful use of 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.

Employees are advised that the use of District-owned communications devices and any other District-owned technology does not provide any expectation of privacy. The use of District-owned devices is consent by the user of the District to access any and all uses and the content of such uses.

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 increase students' knowledge of safe practices for internet use.

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 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 USE

1. **Educational Purposes Only**. All 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 you 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, materials harmful to minors and materials that depict the sexual exploitation of minors.

G. Students are prohibited from using e-mail; this includes District e-mail accessed through a web browser. E-mail access may be given to students on a case-by-case basis (e.g., foreign exchange students keeping in contact with home). Students are prohibited from joining chat rooms, using school equipment or school systems for any such activity, unless it is a teacher-sponsored activity.

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]), 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.

The term "harmful to minors" is defined in Section 18-1514(6), Idaho Code as meaning one or both of the following:

- The quality of any material or of any performance of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:
    - Appeals to the prurient interest of minors as judged by the average person, applying contemporary community standards; and
    - Depicts or describes representations or descriptions of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse which are

patently offensive to prevailing standards in the adult community with respect to what is suitable material for minors and includes, but is not limited to, patently offensive representations or descriptions of:

- Intimate sexual acts, normal or perverted, actual or simulated; or
- Masturbation, excretory functions or lewd exhibits of the genitals or genital area. Nothing herein contained is intended to include or proscribe any matter which, when considered as a whole, and in context in which it is used, possesses serious literary, artistic, political or scientific value for minors, according to prevailing standards in the adult community, with respect to what is suitable for minors.

- The quality of any material or of any performance, or of any description or representation, in whatever form, which, as a whole, has the dominant effect of substantially arousing sexual desires in persons under the age of eighteen (18) years.

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, graphic autopsy or crime-scene images
- Crime – information on 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 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.

Review of filtering technology and software shall be done on a periodic basis and is the responsibility of the Internet Safety Coordinator. It shall be the responsibility of the Internet Safety Coordinator 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 Internet 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 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 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, 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.

INTERNET SAFETY COORDINATOR

The Superintendent shall serve, or appoint someone to serve, as "Internet Safety Coordinator" with responsibility and authority for ensuring compliance with the requirements of federal law, state law and this policy. The Internet Safety Coordinator shall develop and maintain administrative procedures to enforce the provisions of this

policy and coordinate with the appropriate District personnel regarding the internet safety component of the District's curriculum. The Internet Safety Coordinator shall handle any complaints about the enforcement of this policy.

The Internet Safety Coordinator shall maintain documentation evidencing that instruction by school personnel on internet safety is occurring District wide.

PUBLIC NOTIFICATION

The Internet Safety Coordinator 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.

I have read and do agree with the provisions of this District-Provided Access to Electronic Information, Services, and Networks Policy.

User Name (Print)	School
User Signature	Date

Policy Cross Reference:

Board Policy 502.17	District-Provided Access to Electronic Information, Services, and Networks

Legal Reference:

Policy History:

Reviewed:	08/20/2012
Adopted:	08/20/2012
Reviewed:	12/09/2013
Amended:	12/09/2013