Policy Title: District-Provided Access to Electronic Information, Services, and Networks **Policy No: 502.17**

GENERAL

Internet access and interconnected computer systems are available to the District's students and staff. 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.

Students and 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 to 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. The failure of any user to follow this Policy will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

2. **Privileges:** The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The system administrator **(AND/OR building principal)** will make all decisions regarding whether or not a user has violated these procedures, and may deny, revoke, or suspend access at any time. An appeal of such decisions may be made to the Superintendent within seven working (7) days. His or her decision is final.

UNACCEPTABLE USES OF NETWORK

The user is responsible for his or her actions and activities involving networks. 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:

1. 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; violating copyrights or other contracts; and/or accessing information pertaining to the manufacture of weapons.

2. 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.

3. 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.

4. 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.

5. Uses for private financial or commercial activities, including commercial or private advertising. 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.

6. Sending, receiving, viewing or downloading obscene materials, materials harmful to minors and materials that depict the sexual exploitation of minors.

7. 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.

8. 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.

9. Downloading, installing, or copying software or other files without authorization of the Superintendent or the Superintendent's designee.

10. Posting or sending messages anonymously or using a name other than one's own.

11. 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.

12. Plagiarism of material accessed online. Teachers will instruct students in appropriate research and citation practices.

13. Using the network while access privileges are suspended or revoked.

14. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;

15. Using another user's account or password or some other user identifier that misleads message recipients into believing that someone other than the sender is communicating;

16. Posting material authored or created by another, without his or her consent; and

17. Any other unacceptable uses as outlined in District Policy.

NETWORK ETIQUETTE

The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not become abusive in messages to others.

2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.

3. Do not reveal personal information (including the addresses or telephone numbers) of students or staff.

4. Recognize that e-mail is not private. People who operate the system have access to all e-mail. Messages relating to or in support of illegal activities may be reported to the authorities.

5. Do not use the network in any way that would disrupt its use by other users.

SECURITY

Network security is a high priority. If the user can identify a security problem on the internet, the user must notify the system administrator, Internet Safety Coordinator, or building principal. The user should not demonstrate the problem to other users. The user should keep his or her account and password confidential. The user should not user another individual's account. Attempts by the user to log on to the internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

VANDALISM

Vandalism will result in the cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the internet, or any other network. This includes, but is not limited to, the unloading or creation of computer viruses.

TELEPHONE CHARGES

The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long distance charges, per minute surcharges, or equipment or line costs.

COPYRIGHT WEB PUBLISHING RULES

Copyright law and District Policy prohibit the republishing of text or graphics found on the Internet or on District websites or file services, without explicit written permission.

1. For each republication on a website or file service of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the website address of the original source.

2. Students engaged in producing website pages must provide library media instructional assistants with e-mail or hard copy permissions before the website pages are published. Printed evidence of the status of "public domain" documents must be provided.

3. The absence of copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.

4. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

5. Student work may only be published if there is written permission from both the parent(s)/guardian(s) and the student.

6. Violation of the copyright web publishing rules may result in denial of access to the network.

USE OF ELECTRONIC MAIL

1. The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the District. When available, the District provides e-mail to aid students in fulfilling their duties and responsibilities and as an education tool.

2. Email could be subject to public records requests and disclosures depending upon the subject matter of the contents of the email.

3. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an electronic mail account is strictly prohibited.

4. Each person should use the same degree of care in drafting an electronic mail message that would be put into a written memorandum or document. Nothing

should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

5. Electronic messages transmitted via the District's internet gateway carry with them an identification of the user's internet "domain." This domain name is a registered domain name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

6. Any message received from an unknown sender via the internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any internet-based message is prohibited, unless the user is certain of that message's authenticity and the name of the file so transmitted.

7. Use of the District's electronic mail system constitutes consent to these regulations.

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.

Staff members shall supervise students while students are using District internet access at school, to ensure that the students abide by the Policy for internet access.

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 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
- Self-Harm: Sites containing content on self-harm including cutting, and sites that encourage anorexia, bulimia, etc.
- 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(s) or guardian(s) or, if the student is 18 or over, the permission of the student himself/herself. Students should be aware that conduct on the District's computers or using the District's server may be subject to public disclosure depending upon the nature of the communication. 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.

STUDENT USE OF SOCIAL MEDIA

Students will be held accountable for the content of the communications that they post on social media locations and are responsible for complying with District policy and procedures for content posted using a District computer, network, or software or when posted during school hours when the student is in attendance at school. Student posts on social media locations outside of school hours and school grounds using a personal computer, network, and software shall be private as long as they do not enter into the education setting and interfere with the orderly operation of the school. Posts to social network sites using a District computer, network, or software may be subject to public records requests. Students may not disrupt the learning atmosphere, education programs, school activities, or the rights of others.

All of the requirements and prohibitions in District Policy and procedure apply to the use of social media on school grounds, through the District network or using District equipment, or as part of a class assignment.

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 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.

INTERNET ACCESS CONDUCT AGREEMENT

Every student, regardless of age, must read and sign below:

I have read, understand, and agree to abide by the terms of the St. Maries Joint School District No. 41's Board Policy 502.17 - District-Provided Access to Electronic Information, Services, and Networks. Should I commit any violation or in any way misuse my access to the District's computer network or the Internet, I understand and agree that my access privileges may be revoked and school disciplinary action and/or legal action may be taken against me.

User's Name (Print)_____ Home Phone:_____
Cell Phone:_____

User's Signature:_____ Date:_____

Address:_____

Status: I am 18 or older___ I am under 18___

If I am signing this Policy when I am under 18, I understand that when I turn 18, this Policy will continue to be in full force and effect, and I agree to abide by this Policy.

PARENT(S) OR LEGAL GUARDIAN(S): (If the student is under 18 years of age, a parent/legal guardian must also read and sign this Agreement.) As the parent or legal guardian of the above named-student, I have read, understand and agree that my student shall comply with the terms of the District's Policy No. 502.17 – District-Provided Access to Electronic Information, Services, and Networks for the student's access to the District's computer network and the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the District to restrict access to all offensive and controversial materials and understand my student's responsibility for abiding by the Policy. I am, therefore, signing this Agreement and agree to indemnify and hold harmless the District, the Trustees, Administrators, teachers, and other staff against all claims, damages, losses, and costs, of whatever kind, that may result from my student's use of his or her access to such networks or his or her violation of the District's Policy. Further, I accept full responsibility for supervision of my student's use of his or her access account if and when such access is not in the school setting. I hereby give my student permission to use the building-approved account to access the District's computer network and the Internet.

Parent/Guardian (Print)_____ Home Phone:_____
Cell Phone:_____

User's Signature:_____ Date:_____

Address:_____

This Agreement is valid for the _____ school year only.

Policy Cross Reference:

Board Policy 502.07	Discipline
Board Policy 505.06	Student-Owned Electronic Communications Devices
Board Policy 505.10	Bring Your Own Technology Program
Board Policy 505.11	District Provided Mobile Computing Devices

Legal Reference:

Policy History:

Reviewed:	08/11//2011
Adopted:	08/11/2011
Reviewed:	12/09/2013
Amended:	12/09/2013
Reviewed:	07/13/2015
Amended:	07/13/2015