MIDDLETON SCHOOL DISTRICT
#134 POLICY AND PROCEDURE
MANUAL
SECTION 3000 – Students

STUDENT TECHNOLOGY ACCEPTABLE USE POLICY……..POLICY 3094

District Provided Access to Electronic Information, Services, and Networks

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 online. 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 utilize 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 and students must be held responsible and accountable for their own conduct.

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. In compliance with the Children's Internet Protection Act (CIPA) this instruction will include information on the safe use of social networking sites and instant messaging, the characteristics of cyber-bullying, and recommended responses.

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 may, consistent with the District's Strategic Plan and Continuous Improvement Plan, 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

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 Student Acceptable Use 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.-

1. **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:

    - 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;

    - 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;

    - 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. Students will immediately notify the school's Administration if they have identified a possible security problem. Students will not go looking for security problems, because this may be construed as an illegal attempt to gain access.

    - 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.

    - 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.

    - 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.

    - 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.

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

- 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.

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

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

- 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.

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

- Using the network while access privileges are revoked.

- Middleton School District may provide students with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. If students are provided with email accounts, they should be used with appropriateness. Students should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district procedure or staff members. Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Internet Safety

Each District computer with internet access shall have a filtering device that blocks access to visual depictions that are obscene, pornographic, harmful, or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The District 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 any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. 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;

And, taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The term “harmful to minors” is also defined in Section 18-1514(6), Idaho Code, which provides:

1. 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:

    A. Appeals to the prurient interest of minors as judged by the average person, applying contemporary community standards; and

    B. 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:

        I. Intimate sexual acts, normal or perverted, actual or simulated; or

        II. 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.

2. 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 18 years.

Internet Filtering

Filtering is only one of a number of techniques used to manage students’ 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 and filtered. This list will be updated/modified as required.

1. Nudity/pornography: Prevailing U.S. standards for nudity, provocative semi-nudity, sites which contain pornography or links to pornographic sites;
2. 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;
3. Violence: Sites which promote violence, images or description of graphically violent acts, graphic autopsy or crime-scene images;
4. Crime: Information on performing criminal acts (e.g., drug or bomb making, computer hacking), illegal file archives (e.g., software piracy);
5. 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),

6. graphic medical images outside of a medical context;
7. Language/Profanity: Passages/words too coarse to be softened by the word filter, profanity within images/sounds/multimedia files, adult humor;
8. Discrimination/Intolerance: Material advocating discrimination (e.g., racial or religious intolerance); sites which promote intolerance, hate, or discrimination;
9. Interactive Mail or Chat: Sites which contain or allow inappropriate email correspondence, sites which contain or allow inappropriate chat areas:
10. Inappropriate Banners: Advertisements containing inappropriate images or words;
11. Gambling: Sites which allow or promote online gambling;
12. Weapons: Sites which promote illegal weapons, sites which promote the use of illegal weapons;
13. Self-Harm: Sites containing content on self-harm including cutting, and sites that encourage anorexia, bulimia, etc.; and
14. 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:

1. Educating students to be “Net-smart”;
2. Using recognized internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
3. Using “Acceptable Use Agreements”;
4. Using behavior management practices for which internet access privileges can be earned or lost; and
5. Appropriate supervision, either in person and/or electronically.

The District Technology Department and/or building administration 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.

The District Technology Department in coordination with District and school administration shall set a process for reviewing student claims that access has been denied to internet material that is not within the prohibitions of this policy and for unblocking such materials when appropriate.

Review of filtering technology and software shall be done on a periodic basis and is the responsibility of the District Administration. It shall be the responsibility of the Director of Instructional Technology to bring to the Superintendent or designee 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 and the student or, if the student is 18 or over, the permission of the student. Students should be aware that conduct on the District's computer or using the District's server may be subject to public disclosure depending upon the nature of the communication. Students should never give out private or confidential information about themselves or others on the internet, particularly credit card numbers and social security numbers. Middleton School District staff members may approve exceptions in the case of applications for college or employment.

Student Use of Social Media

Students will be held accountable for the content of the communications that they post on social media websites and are responsible for complying with this District policy. Social media refers to online tools and services that allow any Internet user to create and publish content. Many of these sites use personal profiles where students post information about themselves. Students may not disrupt the learning atmosphere, educational programs, school activities, or the rights of others.

All requirements of this policy apply to use of social media through the District network or equipment or as part of a class assignment.

Internet Access Conduct Agreements

Each student and his or her parent(s)/legal guardian(s) will be required to sign and return to the school at the beginning of each school year the Student 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 the school initiates an investigation of a user's use of his or her access to its computer network and the internet.

Violations

If any user violates this policy, the student's access to the District's network and computers will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action. The District Technology Department in coordination with District and school administration 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 or her 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.

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

Submission to State Department of Education

This policy shall be filed with the State Superintendent of Public Instruction every five years after initial submission and subsequent to any edit to this policy thereafter.

Cross Reference: 2326 Digital Citizenship and Safety Education
3330 Student Discipline

Legal Reference: I.C. § 33-132 Local School Boards Internet Use Policy Required
I.C. § 18-1514(6) Obscene Materials – Definitions
20 U.S.C. § 9134(f) Children's Internet Protection Act
20 U.C.C. § 7131 Internet Safety

Policy History
Adopted on: 12/11/17
Revised on: 08/12/19
Reviewed on: