COMPUTER AND NETWORK SERVICES - ACCEPTABLE USE POLICY

GENERAL INFORMATION

Computer and network services are provided by Mountain Home School District for students and staff. Use of this District's computer and network services must be directly related to an educational goal and consistent with the instructional objectives of this District. The District reserves the right to monitor all activity on the computer and network services and use content filtering to assure compliance with educational goals of the District, and to remove access when necessary.

The Network Services provided by this District may not always meet student or staff requirements or be uninterrupted or error-free. It is provided on an "as-is/as available" basis. No warranties are implied or given with respect to any service, information, or software contained therein.

The system administrators of the Network Services are District employees who are responsible for monitoring use of the Network Services.

The superintendent or designee shall be responsible for establishing procedures as needed to implement this policy.

DEFINITIONS

"Network Services" includes voice and data information, e-mail, equipment, software, and the Internet.

"Child pornography" is defined as any visual depiction…whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The product of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. Such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or
4. Such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct. 18 U.S.C. § 2246.

"Minor," for the purposes of this policy, is an individual who has not attained the age of 17.

"Harmful to minors" is a visual depiction containing any picture, image, graphic image file, or other visual depiction (text, audio, or video) that taken as a whole and with respect to minor:

1. Appeals to a prurient interest in nudity, sex, or excretion;
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 defined in section 2256 of title 18, United States Code, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
3. Lacks serious literary, artistic, political, or scientific value to minors, as otherwise defined in Idaho Code Section 18-1514; or
4. Would endorse or promote the following unless the material is being used for a legitimate educational purpose:

    a. Abusive or threatening material
    b. Alcohol, tobacco, and drug use or abuse
    c. Gambling
    d. Hate/discrimination materials
    e. Murder/suicide material
    f. Racially offensive material
    g. School cheating information
    h. Violence and weapons

"Obscenity" is defined in section 1460 of Title 18, United States Code as any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole, appeals to a prurient [i.e. erotic] interest;
2. Depicts, describes or represents in a patently offensive way an actual or simulated sexual act or sexual contact or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value. 18 U.S.C. § 1460.

PRIVILEGES & RESPONSIBILITIES

The use of Mountain Home School District Network Services is a privilege, not a right. System administrators reserve the right, at their sole discretion to suspend or terminate members' access to and use of computer and network services upon any breach of the Computer and Network Services Acceptable Use policy.

All staff and students will be provided with access to computers and the internet. Students and staff using computer and network services agree to follow the Computer and Network Services Acceptable Use Policy. Use of the District's computers and/or network services constitutes an agreement to follow all District rules and policies.

District Technology Support staff and their designees may violate the Computer and Network Services Acceptable Use policy as needed to provide technology support and maintain the District's systems.

INFORMATION CONTENT

This district provides students and staff access to other computer systems around the world through the Internet and users may encounter information that is controversial or potentially harmful. Because the information and sources of information on such computer network services is continually changing, it is impossible for the district to monitor all the content. Some computer systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal materials. This district does not condone the use of such materials and does not knowingly permit use of such materials in the school environment. Students or staff bringing such materials into the school environment will be dealt with according to the discipline policies of the individual schools and this district. Intentionally accessing or using such materials may result in termination of access to this district's computer network services capacities as well as in-school suspension, suspension from school or expulsion; or disciplinary actions for staff, including termination.

INTERNET SAFETY FOR STUDENTS

The district will take appropriate steps to protect all students from access, through the district's computers, to visual depictions that are obscene, contain child pornography, are harmful to minors, or depicting the sexual exploitation of a minor, as defined in Idaho Code Section 18-1507, by installing and utilizing specific technology that blocks or filters Internet access to such visual depictions.

The building administrator or designee may request the disabling of the Internet block or filter system only for the purpose of enabling access for bona fide research or other lawful purpose.

Disabling of the Internet block or filter system by any other staff member or student will result in disciplinary action.

Any staff member, student, parent, or patron may make a request to the IT department that the district either block, or disable a block of, a particular website. If the requester does not agree with the IT departments decision they may file a written request with the superintendent to override the IT departments decision. The superintendent will appoint a five (5) member committee, including three (3) staff members and two (2) patrons. The committee will meet with the individual who filed the request in a timely manner, allow that individual to make oral or written arguments to support the request, and make a written recommendation to the superintendent regarding whether the district should block, or disable a block of, a particular website. Upon reviewing the request and the committee's recommendation, the superintendent will render a written decision and notify the individual who made the request. The superintendent's decision in this matter will be final. The procedure for handling a complaint

shall be available for review in the district office. The district will include a component of Internet safety for students that is integrated into the district's instructional program.

ONLINE USE

All district policies and school rules pertaining to behavior and communications apply to online use. The use of this district's computer network services capabilities must be for educational purposes only and be consistent with this district's mission.

1. Users are prohibited from accessing the district's computer network services for any private or commercial purposes. Users are not allowed to advertise, attempt to sell or offer for sale any goods or services that could be construed as a commercial enterprise, unless pre-approved by the board or superintendent.
2. Users are prohibited from engaging in cyberbullying, including, but not limited to, using a computer, computer system, or computer network service to convey a message in any format (audio or video, text, graphics, photographic, or any combination thereof) that is harassment, intimidation, or bullying, or is otherwise intended to harm another individual.
3. Users are prohibited from submitting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material, nor encourage the use of controlled substances.
4. Illegal activity is prohibited and may result in referral to law enforcement.

    a. Sending, receiving, viewing, downloading, or otherwise accessing obscene or pornographic material, or material deemed to be harmful to minors, is prohibited.
    b. Sending, receiving, or accessing harassing, threatening, or objectionable material is prohibited.

5. Using programs to infiltrate a computing system and/or damage the software components is prohibited.
6. Students and staff will use the computer network service resources efficiently to minimize interference with others.
7. Users are responsible for making back-up copies as needed.
8. Users are responsible for taking precautions against computer viruses on their own equipment and this school district's equipment.
9. Users will not transmit materials, information, or software in violation of any local, state, or federal law.
10. Attempts to log in to the system using another user's account will result in termination of the user's account.
11. Users will not reveal personal information regarding others and should be cautious when revealing users' own personal information (home address, phone number, etc.).
12. The computer network service may not be used in such a way that use would disrupt the use of the computer network service by others.
13. All communications and information accessible via the computer network service should be assumed to be private property, but open to district scrutiny and review at any time.

14. Any online conduct that is determined by the system administrator to constitute an inappropriate use of the district's computer network service or to improperly restrict or inhibit other users from using and enjoying this district's computer network service is strictly prohibited and may result in disciplinary action.

ONLINE DATA AND ACCOUNTS OPT-OUT FORM

Parents who do not want their students name, picture, or work displayed online must sign the Online Data and Accounts Opt-out Form.

INTELLECTUAL PROPERTY

All works of any kind that an employee of the District creates on the network or District computers shall be the intellectual property of the District, as such property shall be deemed "work for hire" as defined in 17 USC Section 1001(1). Student works prepared pursuant to an assignment for any class, project, school-sponsored activity or club shall be the property of the student, if it represents original work.

All works on the network, computers, or storage devices are subject to the monitoring/scrutiny of District and building administrators, information system personnel, and/or designees of administrators. All files, materials, or documents may be reviewed and may be deleted by designated technology staff.

For the purpose of this policy, "works" shall mean an original expression, a fixed and tangible form, that may be entitled to common-law or statutory copyright protection. Works may take different forms and include, but are not limited to, art, literature, music, software, and photography.

COPYRIGHTED MATERIALS

Copyrighted material must not be placed on Network Services or on any networks connected to this District's Network Services without the author's written permission. The following will apply to copyrighted materials:

1. Only the copyright owner(s) or persons specifically authorized may upload copyrighted material to the Computer Network Services.
2. Users may download only that copyrighted material for which permission has been requested and granted, or that falls within the fair use exception to the copyright laws.
3. Users may redistribute copyrighted programs and/or materials only with the express written permission of the owner or authorized person or as provided by the fair use exception.

    a. Permission must be specified in the document, on Network Services, or must be obtained directly from the author.

EMAIL AND ELECTRONIC COMMUNICATION

The District maintains an electronic mail system. E-mail is one of the primary methods of communication with staff and is used to assist in the conducting of business within the District.

Electronic mail not designated as spam mail is retained (archived) by the District for a period of two years starting January 1, 2014.

The electronic mail system hardware and software is District property. Additionally, all messages or communications composed, sent, or received on the electronic mail system are the property of the District. They are not the private property of any student or employee.

Use of the electronic mail system must be in support of education, research, and consistent with the purpose of Mountain Home School District. It shall conform to State, Federal regulations, and District Policy.

The electronic mail system shall not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

The electronic mail system shall not be used to create any offensive or disruptive messages. Among those considered offensive are any messages that contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, religious or political beliefs, national origin, or disability.

The electronic email system shall not be used to send or receive copyrighted materials, confidential information, proprietary financial information, or similar materials without prior written authorization.

The District reserves and intends to exercise the right to review, audit, intercept, access, and disclose all messages created, received, or sent over the electronic mail system. The contents of electronic mail may be disclosed within the District without the permission of the employee.

The confidentiality of any message should not be assumed. Even when a message is erased by the user, it may still be possible to retrieve and read that message. Further, the use of password for security does not guarantee confidentiality.

Employees should not use an encryption or pass code on email or any stored information, unless authorized to do so.

The amount of e-mail messages stored will be limited to the amount of space allocated to its members.

All files, including e-mail, will be deleted from a canceled network account.

THIRD PARTY INFORMATION

Opinions, advice, goods, services, and all other information expressed or delivered by students or staff, information providers, service providers, or other third party personnel on Network Services are those of the providers and not of Mountain Home School District No. 193.

DISK USE

The system administrator reserves the right to set quotas for disk use on the computer system. Users exceeding their quota will be required to delete files to return to compliance. Users may request that their disk quota be increased. System administrators reserve the right to delete user files that exceed the quota. Users will respect network resource limits. They will use their directories on the network to store documents they have created and will delete them when they are no longer needed. They will not download or copy large files unless they are necessary for a school-related project. Such files must be deleted when they are no longer needed. Through routine maintenance, individual files may be reviewed and deleted by designated technology staff.

Users are responsible to maintain a back-up of their files. The District does not guarantee access to user files.

WEBSITE AND WEB-SERVICES ACCOUNTS

The District retains the right to create online accounts for website and web-services for students unless parents sign the Online Data and Accounts Opt-out Form.

SECURITY

Mountain Home School District recognizes information and network resources as assets. These assets include but are not limited to the following:

1. Student/Staff records and information
2. School District policies
3. Business and financial operations information
4. Curriculum and instructional programs
5. Network services - "Network Services" includes voice and data information, e-mail, equipment, software, and the Internet.

Mountain Home School District will establish security measures and assign responsibilities to protect the network services from loss, theft, and unauthorized use, modification, or disclosure.

Mountain Home School District's security measures apply to all District-owned information, either physical or electronic. All regular and contract employees, student users, and guests must comply with these security measures.

VANDALISM

Vandalism is defined as any malicious attempt to harm or destroy data of users, Network Services equipment, or any agencies of other networks that are connected to the Internet. This includes, but is not limited to the uploading intentional spreading and/or creation of computer viruses. Vandalism will result in disciplinary actions mentioned above.

CONSEQUENCES

Any violation by staff of the Computer and Network Services policy shall be subject to discipline, up to and including termination of employment.

Student discipline for violation of any part of this policy shall be based on the student's age and the severity of the infraction. Student discipline may involve actions up to and including suspension and/or expulsion for violations occurring on any District premises, at any District sponsored activity, or using any district provided or owned accounts or equipment, regardless of location.

The Superintendent or designee shall submit the violation to the appropriate law enforcement agency when the circumstances warrant such action.

UPDATING USER ACCOUNT INFORMATION

The computer network service may occasionally require new registration and information from users to continue the service. User must notify the designated administrator of any changes/deletions in user information (address, phone, name, etc.).

COMPLIANCE WITH STATE LAW

Mountain Home School District will file this policy with the state superintendent of public instruction no later than August 1, 2011, and every five (5) years thereafter.

PRIVACY

Network administrators will not intentionally inspect the contents of e-mail or any other storage device on the District's equipment unless necessary for support purposes. However, network administrators reserve the right to cooperate fully with administration and local, state, or federal officials in any investigation concerning or relating to any aspect of Network Services.

BREACHES OF SECURITY

Students or staff identifying breaches of security or other abuses should notify a teacher, administrator, or Technology Support.

Intentional breaches of security will be considered vandalism.

PASSWORDS

Passwords, accounts, and home directories shall not be shared. Attempts to log into network services using another user's account will be considered a breach of security.

WEB PUBLISHING

The Mountain Home School District's website offers staff and students the opportunity to publish educational information.

1. **Goals Statement**

   a. Provide patrons a resource for obtaining information about the District.
   b. Provide teachers a forum for enhanced teaching and for informing patrons about classroom activities and policies.
   c. Provide students a place to demonstrate what they have learned.

2. **General Procedures**

   a. Advertising
      - Users may not be compensated for advertising another site or a product on their website.
      - Users may not run a business from the District's website.
      - Users may not create a link to an external site (commercial and/or personal) unless that site clearly supports the educational content of the school's site.
   b. Designated webmasters at each school will be faculty or staff members.
   c. Building principals, building technical coordinators, and program administrators are responsible for being knowledgeable about the content of their building/program webpages.
   d. Any deliberate tampering with or misuse of District webpages will be considered vandalism and will be handled in accordance with the District's Network Acceptable Use Procedures.

3. **Ownership & Control**

   a. All webpages hosted by the District are the property of the Mountain Home School District.
   b. Students may create and publish webpages to be hosted on the District's website for educational purposes directly related to a course that the student is currently enrolled. It is the responsibility of the instructor to ensure that student websites are in total compliance with District rules and procedures before the material is published.
   c. Only active files that are required for the proper operation of a website will be stored on the District's site. It is the responsibility of the page's author to maintain and/or delete files.

- Staff webpages will be deleted when the staff member leaves the District.

d. Staff webpages will be moved when the staff member changes locations due to an assignment change.
e. The District's technology administrator or District Webmaster will have the authority to remove any content deemed inappropriate.
f. The Superintendent will have final authority for issues related to the content of all pages on the District's website.

4. **Security & Privacy**

a. Remember that sites are accessible to anyone and that the safety of students, colleagues, and their families is of paramount concern.
b. Information relating to emergency responses, including but not limited to facility maps, floor plans, or emergency procedures will not be posted in non-secure areas of the website. No maps of school floor plans or emergency routes will be posted on the website.
c. According to the Federal Family Educational Rights and Privacy Act of 1974 (FERPA), "directory information" about students may be released by the District without parental consent, provided annual notification has been given and the school does not have on file written denial to release "directory information."
   - Directory information is defined as information contained in an education record of a student, which would not generally be considered harmful or an invasion of privacy if disclosed. A copy of the FERPA policy is available online at **www.mtnhomesd.org**. It includes, but is not limited to:
     ~ The student's name
     ~ Photographs of the student used by the District for recognition of student achievement and community relations, including, but not limited to, publication in the District's or school's newsletters or publications, in the school setting, and on the District's or school's website
     ~ Participation in officially recognized activities such as sports
   - Authors will exercise discretion in making judgments concerning publication of student information and take reasonable precautions to insure security and privacy.
   - A staff member's name, assignment, District e-mail address, District phone number, and photo may be published. Staff members have the right to request that their photographs not be published.
   - Inclusion of a student's phone number, address, e-mail address, or information indicating the physical location of a student at a given time, other than attendance at a particular school or participation in a District sponsored activity, is prohibited.
   - If grades or other personal student information is to be published for parental access, complete confidentiality must be built into the process.

5. **Copyright Issues**

a. Copyright protection extends to the Internet. Treat all online materials (such as website

contents, e-mails, newsgroups postings) as you would other copyrighted material. No unlawful copies of copyrighted materials may be knowingly produced on or transmitted via the District's equipment, including its web servers.

b. Student work (art, short stories, projects, etc.) may be published unless the parent or student have signed the Online Data and Accounts Opt-out Form.
c. Students and staff will adhere to all copyright laws.
d. It is not necessary for a work to have a copyright notice or to be registered to receive copyright protection, however reminding a visitor of your rights as an author by including a copyright notice as a footer on every page is recommended.

INTERNET FILTERING

The Board recognizes the importance of providing students with positive, productive educational experiences through the District's Internet services. To the extent practical, the Board directs the Superintendent or designee to:

1. Prevent user access over the District computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
2. Prevent unauthorized access and other unlawful online activity;
3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. Comply with federal and state laws.

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to:

1. Obscene material;
2. Materials that depict sexual exploitation of minors;
3. Material deemed harmful to minors; or
4. Other information that is determined to be in violation of District policies.

The following principles shall be the guide for Internet website access and site filtering. The District shall provide access to:

1. Materials that will enrich and support the curriculum and educational needs of users, taking into consideration the varied interests, abilities, learning styles, maturity levels, socioeconomic, and ethnic backgrounds
2. Materials that will stimulate growth in factual knowledge and ethical standards and that will develop literary, cultural, and aesthetic appreciation
3. Background information which will enable students to make intelligent judgments in their daily lives
4. Materials on opposing sides of controversial issues so that the users may develop, under guidance, the practice of critical analysis
5. Materials which realistically represent our pluralistic society and reflect the contributions made by all groups and individuals to our American and global heritage

The District will hold a public meeting for input and comments by parents and other patrons regarding the District's Computer and Network Services Policy which is the District's Internet safety policy.

PROHIBITED USES

The technology system should only be used for approved District activities and educational purposes. Prohibited uses of District technology include, but are not limited to:

1. **Causing Harm to Individuals or to Property**

   a. Use of obscene, profane, vulgar, inflammatory, abusive, threatening, disrespectful language or images.
   b. Making offensive, damaging, or false statements about others.
   c. Posting or printing information that could cause danger or disruption.
   d. Bullying, hazing or harassing another person.
   e. Deleting, copying, modifying, or forging other users' names, e-mails, files, or data.
   f. Disguising one's identity, impersonating other users, or sending an anonymous e- mail.
   g. Posting personal information (e.g. phone number, address) about oneself or any other person, except to responsible agencies

2. **Engaging in Illegal Activities**

   a. Participating in the sale, purchase or promotion of illegal items or substances
   b. Accessing or transmitting:
      - Pornography of any kind;
      - Obscene depictions;
      - Harmful materials;
      - Materials that encourage others to violate the law;
      - Confidential information; or
      - Copyrighted materials without authorization or as provided by fair use regulations.
      - Attempting to disrupt the computer system or destroy data by any means

3. **Breaching System Security**

   a. Sharing one's or another person's password with others
   b. Entering another person's account or accessing another person's files without authorization
   c. Allowing others to gain access to one's individual account.
   d. Interfering with other users' ability to access their accounts
   e. Allowing student access to sensitive data
   f. Attempting to gain unauthorized access to another computer
   g. Using software or hardware tools designed to interfere with or bypass security

mechanisms
h. Utilizing software or hardware applications that are not approved for business use
i. Attempting to evade the District's computer filtering software

4. **Improper Use or Care of Technology**

a. Accessing, transmitting or downloading large files, including posting chain letters or engaging in spamming
b. Attempting to harm or damage District technology, files or data in any way
c. Alteration of configured equipment, including the addition of unauthorized passwords and user accounts.
d. Leaving an account open or unattended
e. Attempting to remedy a security problem and not informing a school official
f. Failing to report the abuse of District technology
g. Installing, uploading or downloading unauthorized programs
h. Copying District software for personal use
i. Using District technology for:
   - Personal financial gain
   - Personal advertising or promotion
   - For-profit business activities
   - Unapproved fundraising
   - Inappropriate public relations activities such as solicitation for religious purposes
   - Inappropriate political purposes

♦ ♦ ♦ ♦ ♦ ♦ ♦

LEGAL REFERENCE:
17 USC Section 101 and 1001(1), *et seq*.
47 USC Section 254(h)(1)
Children's Internet Protection Act, Sections 1703 to 1721, U.S.C. Section 254(h)(1)
Idaho Code:
6-210
18-917A, 18-1507, 18-1514, 18-2201, 18-2202
33-131, 33-132, 33-512
Cowles Publishing Co. v. Kootenai County Board of Commissioners, 144 Idaho 259 (2007)

ADOPTED: March 18, 2014 (Previous Network Services Use Policy - Adopted: January 16, 1996; with last revision on February 16, 2010)
Revised: March 18, 2014 Revised: July 19, 2016

