

The Emmett Independent School District No. 221 (Emmett School District) recognizes the importance of providing positive, productive educational experiences through the district's Internet, computer, and network services. An account on the Emmett School District computer network and subsequently, access to the Internet, is provided for all students, unless otherwise requested by parents or guardians. Computers and computer networks, including internet access, provide valuable tools that support the education of students in Emmett School District. Network users are expected to use all network resources for purposes appropriate to the education environment at all times. Users must refrain from any use that is not consistent with the policies, purposes, or objectives of Emmett School District. To promote this objective and protect its staff and students, the board authorizes the superintendent or designee to:

1. Prohibit and prevent school computers and other school owned technology-related services from sending, receiving, viewing or downloading materials that are deemed to be harmful to minors, as defined by Idaho Code Section 18-1514.
2. Prohibit and prevent unauthorized online disclosure, use, or dissemination of personally identifiable information of students. Users will not reveal personal information regarding others and should be cautious when revealing users' own personal information (home address, telephone number, etc).
3. Select and employ technology protection measures on the district's computers to filter or block Internet access to obscene materials, materials harmful to minors, and materials that depict the sexual exploitation of a minor, or other information that is determined to be in violation of district policies.
4. Establish and enforce appropriate disciplinary measures to be taken against persons violating this policy.
5. Handle complaints regarding the enforcement of the district's Internet use policies and procedures.

#### **INTRODUCTION/EXPLANATION OF PURPOSE:**

Any use of the Emmett School District's network shall be for the exchange of information related to education. Emmett School District Standards must be followed at all times. Users of electronic communications (including, but not limited to email, web pages, on-line collaborations, list servers and discussion groups) should be mindful that communications originating within the district may be construed as representative of the school or district.

The district will limit Internet access to materials that enrich and support the curriculum and educational needs of users, contribute to the delivery of efficient and effective business or educational functions, and expedite professional district communications.

#### **PRIVACY**

Use of the district's technology resources is a privilege and not a right. Access has not been established as a public access service or a public forum. The district reserves the right to monitor, inspect, copy, review, delete, and/or store at any time and without prior notice any and

all results of usage of the Internet, computers, network resources, and any and all information transmitted or received in connection with such usage. All such information will be and remains the property of the district and users have no expectation of privacy regarding such materials. The district has the right to place restrictions on the use of the district's Internet, computers, and network resources and may also deny access to staff and students who violate related policies and procedures.

### **INTERNET SAFETY FOR STUDENTS**

The Emmett School District's instructional program will include a component of Internet safety for students. The curriculum shall include appropriate online behavior, including interacting with other individuals on social networking websites and chat rooms and cyberbullying awareness and response.

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 principal or designee may authorize the disabling of the Internet filter system only for the purpose of enabling access for bona fide research or other lawful purpose. Disabling of the Internet filter system by any other staff member or student will result in disciplinary action.

As required by the Children's Internet Protection Act, this district will hold annual public meetings to receive input from parents and other patrons regarding the district's Internet safety plan, including the use of an Internet filtering service.

Any staff member, student, parent, or patron may file a complaint regarding enforcement of this policy or request that the district either block, or disable a block of, a particular website. The individual must file a *written* complaint with the superintendent. The superintendent's decision will be final.

### **PROHIBITED USES**

The district's Internet, computers, and network resources may only be used for approved district activities and educational purposes. All users must fully comply with this policy and immediately report any violations or suspicious activities to the classroom teacher or building principal. 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, 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 harassing, intimidating, or bullying, or is otherwise intended to harm another individual.
  - 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 email.
2. Engaging in Illegal Activities
- a. Participating in the sale, purchase or promotion of illegal items or substances.
  - b. Accessing or transmitting:
    - i. Pornography of any kind.
    - ii. Obscene depictions.
    - iii. Harmful materials.
    - iv. Materials that encourage others to violate the law.
    - v. Confidential information.
    - vi. Copyrighted materials without authorization or as provided by fair use regulations.
  - c. 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:
    - i. Personal financial gain.
    - ii. Personal advertising or promotion.
    - iii. For-profit business activities.

- iv. Unapproved fundraising.
- v. Inappropriate public relations activities such as solicitation for religious purposes.
- vi. Inappropriate political purposes.
- vii.

**CONSEQUENCES FOR INAPPROPRIATE USE**

Failure to comply with this policy or inappropriate use of the district’s Internet, computers, or network resources may result in usage restrictions, loss of access privileges, and/or disciplinary action up to and including expulsion. The superintendent or designee may also report the violation to law enforcement where appropriate.

Users are responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Users will not engage in cyberbullying.

**INTELLECTUAL PROPERTY**

All works of any kind that an employee of the school district creates on the network or district computers shall be the intellectual property of the school district as such property shall be deemed “work for hire” as defined in 17 USC § 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 administration, information systems personnel, and /or designees of administrators. All files, materials or documents may be reviewed and may be deleted by designated technology staff.

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

**COPYRIGHT AND PLAGIARISM**

All users should abide by current copyright law. Plagiarism will not be tolerated. (Plagiarism is copying the ideas, writings or artistic creations of others and presenting them as though they were your own.) If text or multimedia files from the internet or other electronic sources are used, they must be used according to the Fair Use Guidelines established by federal copyright law and policies of Emmett School District #221 and cited accordingly.

**ELECTRONIC DEVICES**

Electronic communication or data devices will be used only in a manner consistent with the policies of Emmett School District. These devices include, but are not limited to, handheld calculators, PDA's (personal digital assistants), cell phones, pagers, electronic book devices, and laptop computers.

**SOFTWARE AND PERIPHERAL DEVICES**

Only district approved software will be installed by designated personnel on networks or individual machines. Appropriate licenses must be held for all software. Peripheral devices (including, but not limited to, printers, scanners, and storage/data devices) must be approved and installed by designated personnel. Donated equipment and software are subject to the same policies.

Any conditions or activities not specifically listed above that are not consistent with the policies, purposes, and objectives of Emmett School District are prohibited.

**WEBCAMS AND VIDEOCONFERENCING EQUIPMENT**

The district makes use of digital technologies that automatically capture and send still and/or video images through the Internet. Students may be involved in activities where their image, or an image of their work, will be digitally transmitted to other people, including those outside the school district. Specific conditions of use may be seen in Policy #694.

**CONSEQUENCES FOR INAPPROPRIATE USE**

Failure to comply with this policy or inappropriate use of the district’s Internet, computers, or network resources may result in usage restrictions, loss of access privileges, and/or disciplinary action up to and including expulsion. The superintendent or designee may also report the violation to law enforcement where appropriate.

Users are responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

**NOTICE**

The district will inform staff, students, parents/guardians, and other users about this policy through posting on the district website and by publishing in the student handbook. A copy of this policy will be available for review at the district office and will be provided in writing to parents/guardians upon request. The district will also file this policy with the state superintendent of public instruction every five years.

By accessing the district’s Internet, computers and network resources, users acknowledge awareness of the provisions of this policy and awareness that the district uses monitoring systems to monitor and detect inappropriate use.

All students and staff are required to sign a technology user agreement that signifies their understanding and agreement to follow these regulations.

**DISTRICT LIMITATION OF LIABILITY**

Emmett School District makes no warranties of any kind, either expressed or implied, that the

functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data, or interruptions of service. The district is not responsible for the accuracy or the quality of the information obtained through or stored on the system. The district will not be responsible for the financial obligations arising through the unauthorized use of the system.



**LEGAL REFERENCE:**

Idaho Code Sections

- 6-210 – Recovery of Damages for Economic Loss Willfully Caused by a Minor
- 18-917A – Student Harassment – Intimidation – Bullying
- 18-1507 – Definitions – Sexual Exploitation of a Child – Penalties
- 18-1514 – Obscene Materials - Definitions
- 18-2201 – Computer Crime – Definitions
- 18-2202 – Computer Crime
- 33-132 – Local School Boards – Internet Use Policy Required

Children’s Internet Protection Act, Sections 1703 to 1721, USC Section 254(h)(1)

*Cowles Publishing Co. v. Kootenai County Board of Commissioners*, 144 Idaho 259 (2007)

**LEGAL REFERENCE:**

17 USC Section 1001, *et seq.*

*Childrens’ Internet Protection Act, Sections 1703 to 1721, U.S.C. Section 254(h)(1)*

Idaho Code Sections

- 6-210
- 18-917A
- 18-1507
- 18-1514
- 18-2201
- 18-2202
- 33-132

**ADOPTED:** December 9, 2002

**Reviewed:** December 13, 2012; September 14, 2017

**AMENDED:** April 11, 2013; October 12, 2017

“Supplemented with the permission of © 1999 Eberharter-Maki & Tappen, PA”