Emery County School District

Policy: IJNDCD—Internet Safety

Date Adopted: 19 June 2012
Current Review / Revision: 10 September, 2025

It is the policy Emery School District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

Key terms are as defined in the Children's Internet Protection Act.

Minor: The term "minor" means any individual who has not attained the age of 17 years.

Technology Protection Measure The term `technology protection measure' means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene: as defined in section 1460 of title 18, United States Code;

2. Child Pornography as defined in section 2256 of title 18, United States Code.

Harmful to Minors: The term "harmful to minors" means 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;

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

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Internet Protection—

Access to the internet through District computer networks or systems or by means of devices owned by the district or personal devices gaining access though the district's network shall be regulated by filtering software or other measures which prevent users from accessing images which are obscene or pornographic or otherwise harmful. Student online activity shall be monitored and specified staff shall have responsibility for supervision of

student online activities. In addition, students shall be educated by appropriate staff members regarding appropriate online behavior, including interacting with other individuals through chat rooms or social networking websites and cyberbullying awareness and response. Each school's community council shall also provide for education and awareness on safe technology use and digital citizenship which empowers students to make smart media and online choices and parents to know how to discuss safe technology use with their children.

Utah Admin. Rules R277-495-4(1)(d), (2)(f), (3)(c) (October 8, 2024)

Utah Code § 53G-7-216(3) (2018)

Utah Code § 53G-7-1202(3)(a)(iii)(A), (iv) (2024)

Due Process—

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the District system or District-owned devices.

In the event there is an allegation that a student has violated the District Internet Use Policy, the student will be provided with a notice and opportunity to be heard in the manner set forth in the student disciplinary code.

Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the student disciplinary code, the violation will be handled in accord with the applicable provision of the code.

Employee violation of the District Internet Use Policy will be handled in accordance with District policy

Any District administrator may terminate the account privileges of a guest user by providing notice to the user. Guest accounts that are not active for more than ninety days may be removed, along with the user's files, without notice to the user.

Search and Seizure—

System users do not have an expectation of privacy in the contents of their personal files and/or personal electronic mail accounts and records of their online activity accessed via the District's electronic communications system or through District-owned devices.

Routine maintenance and monitoring of the system may lead to discovery that the user has violated or is violating the District Internet Use Policy, the student disciplinary code, or the law.

An individual search will be conducted if there is reasonable suspicion that a user has violated the law or the student disciplinary code. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

District employees should be aware that their personal files and/or personal electronic mail accounts on the

District's system or on District-owned devices may be discoverable according to the Government Records Access Management Act.

Academic Freedom, Free Speech, and Selection of Material—

Board policies on academic freedom and free speech will govern the use of the Internet.

When using the Internet for class activities, teachers will:

1. Select material that is appropriate in light of the age of the students and that is relevant to the course objectives.

2. Preview the materials and sites they require students to access to determine the appropriateness of the material contained on or accessed through the site.

3. Provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly.

4. Assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussion about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

Parental Notification and Responsibility—

The District will notify the parents about the District network and the policies governing its use. Parents must sign an accessible use agreement to allow their student to have an individual account. Parents may request alternative activities for their child(ren) that do not require Internet access.

Parents have the right at any time to investigate the contents of their child(ren)'s email files. Parents have the right to request the termination of their child(ren)'s individual account at any time.

The District Internet Use Policy contains restrictions on accessing inappropriate material and student use will be supervised. However, there is a wide range of material available on the Internet, some of which may not be in accordance with the particular set of values held by an individual student's family. The District will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District system.

Parents are responsible for monitoring their student's use of district owned devices when they are accessing the system from home.

Access—

The following levels of access will be provided:

1. Individual Accounts for students

a. students may be provided with individual Internet accounts. Students will not have remote access to the system. A written agreement will be required for an individual account. This agreement must be signed by the student and his or her parent.

2. Individual Accounts for District Employees

District employees will be provided with an individual account and will not have remote access to the system. Communications within the course and scope of employees' duties shall be made through this account. A written agreement (employee acceptable use agreement will be required for an individual account. This agreement must be signed by the employee and filed at the school

Guidelines for Internet Use—

1. Personal Safety:

a. Users will not post or provide personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, work address, etc.

b. Students will not agree to meet with someone they have met online without their parent's approval and participation,

c. Users will promptly disclose to their teacher, supervisor, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

2. Illegal Activities

a. Users will not attempt to gain unauthorized access to the District system or to any other computer system through the District system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing."

b. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

c. Users will not use the District system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.

3. System Security

a. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person.

b. Users will immediately notify the system administrator if they have identified a possible security problem. Users will not search for or attempt to discover security problems, because this may be construed as an illegal

attempt to gain access.

c. Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures.

4. Inappropriate Language

a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, slanderous or disrespectful language.

c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.

d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks. Users will not harass another person.

i. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending the person messages, they must stop.

e. Users will not knowingly or recklessly post false or defamatory information about a person or organization

5. Request for Privacy

a. Users will not re-post a message that was sent to them privately without permission of the person who sent them the message.

b. Users will not post private information about another person.

6. Respecting Resource Limits

a. Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer or storage device.

b. Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people.

c. Users will check their email frequently, delete unwanted messages promptly.

d. Users will be subscribed only to high quality discussion group mail lists that are relevant to their education or professional/career development.

7. Plagiarism and Copyright Infringement

a. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

b. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

c. Users will document research done with AI tools and not present that material as their own

8. Inappropriate Access to Material

a. Users will not use the District system or District-owned electronic devices to access material that is profane or obscene (pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (hate literature). (See Policy JICJ and Policy GBEB.) For students, a special exception may be made if the purpose is to conduct research and access is approved by both the teacher and the parent. District employees may access the above material only in the context of legitimate research.

b. If a user inadvertently accesses such information, he or she should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the Internet Use Policy.

Utah Admin. Rules R277-495-4(1)(c) (October 8, 2024)

District Website—

The District may establish a website. Material appropriate for placement on the District website includes: District information, school information, teacher or class information, student projects, and student extracurricular organization information. Personal information not related to education will not be allowed on the District website.

The Superintendent will designate a District Web Publisher, responsible for maintaining the school websites and monitoring all ~~class, teacher, student, and extracurricular~~ web pages representing the district. The Web Publisher will develop style and content guidelines for official District and school web materials and develop procedures for the placement and removal of such material. All official District material posted on the District website must be approved through a process established by the District Web Publisher. The District website shall meet the domain and notice requirements set forth in Policy GAA.

Utah Code § 63A-16-110 (2025)

Utah Code § 63A-19-402.5 (2025)

School Websites—

The Principal will designate a School Web Publisher, responsible for managing the school website and

monitoring all web pages representing the school. All official material originating from the school will be consistent with the District style and content guidelines and approved through a process established by the School Web Publisher. The School Web Publisher will develop additional guidelines for the school website. Each school website shall meet the domain and notice requirements set forth in Policy GAA.

Utah Code § 63A-16-110 (2025)

Utah Code § 63A-19-402.5 (2025)

Student Information—

Each school shall develop standards for disclosure of student information that are considered generally acceptable in light of the age of the students attending the school.

Web Page Requirements—

1. All District Internet Use Policy provisions will govern material placed on the web.

2. Web pages shall not:

a. Contain personal contact information about students beyond that permitted by the school (or District) and parent.

b. Display photographs or videos of any identifiable individual without a signed release. Acceptable use releases for students under the age of 18 must be signed by their parent or guardian.

c. Contain copyrighted or trademarked material belonging to others unless written permission to display such material has been obtained from the owner. There will be no assumption that the publication of copyrighted material on a website is within the fair use exemption.

3. Material placed on the website is expected to meet academic standards of proper spelling, grammar, and accuracy of information.

4. Students may retain the copyright on the material they create that is posted on the web. District employees may retain the copyright on material they create and post if appropriate under District policies.

5. Each web page will carry a notice indicating when it was last updated and the email address of the person responsible for the page.

6. All web pages should have a link at the bottom of the page that will help users find their way to the appropriate home page.

Access to Inappropriate Material

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 inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Emery School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

Minors shall be educated, supervised and monitored in the appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the district IT department under the supervision of appropriate district administrative personnel.

Emery School District or designated representatives will provide age- appropriate training for students who use the district's Internet facilities. The training provided will be designed to promote the district's commitment to:

a. The standards and acceptable use of Internet services as set forth in the Internet Safety Policy;

b. Minor safety with regard to:

    i. safety on the Internet;

    ii. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and

    iii. cyber bullying awareness and response.

c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

All staff and students will sign and follow the provisions of the District's Acceptable Use policy and accept the terms of any other technology-related district policies, whether for district-owned equipment or for personal devices accessing the district's internet services.

All visitors will be notified of and expected to follow the provisions of the District's Acceptable Use policy and accept the terms of any other technology-related District policies, whether for District-owned equipment or for personal devices accessing the District's internet services.

Previous Revision - 1 May 2019