Network Acceptable Use and Internet Safety Policy

Educational Service Unit No. 13 (ESU #13) recognizes the value of computer and other electronic resources to improve student learning and enhance the administration and operation of its schools. To this end, ESU #13 encourages the responsible use of computers, computer networks (including the Internet), and other electronic resources in support of the mission and goals of ESU #13 and its schools.

It is the policy of ESU #13 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)].

It is the policy of ESU #13 to maintain an environment that promotes ethical and responsible conduct in all online network activities by staff and students. It shall be a violation of this policy for any employee, student, or other individual to engage in any activity that does not conform to the established purpose and general rules and policies of the network. Within this general policy, ESU #13 recognizes its legal and ethical obligation to protect the well-being of students in its charge.

The following uses of school-provided electronic resources, including Internet and e-mail, are not permitted:

- to access, upload, download, or distribute pornographic, obscene, or sexually explicit material
- to transmit obscene, abusive, sexually explicit, or threatening language;
- to violate any local, state, or federal statute;
- to vandalize, damage, or disable the property of another individual or organization;
- to access another individual’s materials, information, or files without permission; and,
- to violate copyright or otherwise use the intellectual property of another individual or organization without permission.
- to distribute or forward “chain letters” via email.

Any violation of District policy and rules may result in loss of District-provided access to the Internet. Additional disciplinary action may be determined in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

Students may…

- Design and post web pages and other material from school resources.
- Use direct communications such as e-mail, online chat, or instant messaging with a teacher's permission.
- Use the resources for any educational purpose.

Consequences for Violation. Violations of these rules may result in disciplinary action, including the loss of a student's privileges to use the school's information technology resources.

Supervision and Monitoring. School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions and will furnish evidence of crime to law enforcement.

<u>Enforcement of policy</u>

- 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.
- An ESU #13 staff member may override the technology protection measure that blocks or filters Internet access for a student to access a site with legitimate educational value that is wrongly blocked by the technology protection measure that blocks or filters Internet access.
- ESU #13 staff will monitor students' use of the Internet by either direct supervision or by monitoring Internet use history to ensure enforcement of policy.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of ESU #13 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

It shall be the responsibility of all members of ESU #13 staff to educate, supervise and monitor 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 Director of Technology or designated representatives.

The Director of Alternative Education or designated representatives will provide age appropriate training for students who use ESU #13 Internet facilities. The training provided will be designed to promote ESU #13's commitment to:

a. The standards and acceptable use of Internet services as set forth in the ESU #13 Network Acceptable Use and Internet Safety Policy;

b. Student 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. cyberbullying awareness and response.

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

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the ESU #13 Network Acceptable Use and Internet Safety Policy. Curriculum materials and a Scope and Sequence can be found at Common Sense Media. www.commonsensemedia.org

Disclaimers

- ESU #13 and its individual schools, administrators, faculty, and staff thereof, make no warranties of any kind for the service provided and will not be held responsible for any damage suffered by users. This includes the loss of data resulting from delays, non-deliveries, and intrusion by computer virus or service interruption.
- Use of any information obtained via network access is at the risk of the user, and ESU #13 specifically denies any responsibility for the accuracy or quality of the information obtained.

- ESU #13 cannot guarantee complete protection from inappropriate material. Furthermore, it is impossible for the district or content filter to reflect each individual or family's opinions of what constitutes "inappropriate material." If a student mistakenly accesses inappropriate information, he/she should immediately notify a district staff member.
- ESU #13 is not liable for an individual's inappropriate use of the district's electronic communications systems, for violations of copyright restrictions or other laws, and for other costs incurred by users through use of ESU #13's electronic communication systems.
- The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's electronic communication systems.

*CIPA definition of terms

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 that term is defined in section 1460 of title 18, United States Code;
2. **CHILD PORNOGRAPHY,** as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

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.

SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Educational Service Unit No. 13
Network Acceptable Use and Internet Safety Policy Employee's Agreement

By signing this form, I acknowledge receipt of, understand, and agree to abide by the rules and standards set forth in the ESU #13 Network Acceptable Use and Internet Safety Policy. I understand that to gain or retain access to the ESU #13 computer network systems, I must sign and submit this form as directed. I further understand that any violation of the Policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, monetary liability may be incurred, school disciplinary and/or appropriate legal action may be taken. I, as a staff member, agree to abide by the rules and standards addressed in this policy as it pertains to me and to help ensure that students also abide by these rules and standards as well. I understand that this agreement will be in effect for the duration of my employment with the district or until the policy is revised.

PRINTED Staff Member Name _____

Staff Member Signature_____Date:_____

Department/Job Title: _____

Cell Phone # for DUO App:_____

Educational Service Unit No. 13
Network Acceptable Use and Internet Safety Policy Student's Agreement

By signing this form, I acknowledge receipt of, understand, and agree to abide by the rules and standards set forth in ESU #13 Network Acceptable Use and Internet Safety Policy. I understand that to gain access to the ESU #13 computer network systems, I must return this form signed by me and my parent or legal guardian. I further understand that any violation of the Policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, monetary liability may be incurred, school disciplinary and/or appropriate legal action may be taken. I understand that this agreement will be in effect for one school year and must be re-signed in subsequent years.

PRINTED Student Name _____

Student Signature_____Date:_____

Educational Service Unit No. 13
Network Acceptable Use and Internet Safety Policy Parent's or Legal Guardian's Agreement

I have read, understand, and agree with the ESU #13 Network Acceptable Use and Internet Safety Policy. I understand that by signing this form I give permission for ESU #13 to grant access to district electronic communication systems, including the Internet. I understand that this access is designed for educational purposes. I understand that ESU #13 has taken reasonable precautions to eliminate access to inappropriate material and I will not hold the district or staff members responsible if inappropriate material is inadvertently accessed. I understand that this agreement will be in effect for one school year and must be re-signed in subsequent years.

PRINTED Parent Name _____

Parent Signature_____Date:_____