4012.1
Internet – Acceptable Use Policy

Acceptable Use guidelines will be developed by the Superintendent, in conjunction with the technology committee that will insure the appropriate use of internet access for employees, students, and community members, while using the Cozad Community Schools net. These guidelines will identify registration procedures and consequences for the inappropriate use of the system. Guidelines shall be placed in the staff and student handbooks.

Internet Safety Policy

It is the policy of Cozad Community Schools to comply with the Children's Internet Protection Act (CIPA). With respect to the District's computer network, the District shall: (a) prevent user access to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) provide for the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prevent unauthorized access, including so-called "hacking," and other unlawful activities online; (d) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (e) implement measures designed to restrict minors' access to materials (visual or non-visual) that are harmful to minors.

Definitions

Key terms are as defined in CIPA. "Inappropriate material" for purposes of this policy includes material that is obscene, child pornography, or 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 indecent 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.

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 CIPA, 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 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 District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA, 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.

Supervision and Monitoring.
It shall be the responsibility of all members of the District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and CIPA. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent and the Superintendent's designees.

Social Networking.
Students shall be educated about appropriate online behavior, including interacting with others on social networking websites and in chat rooms, and cyberbullying awareness and response. The plan shall be for all students to be provided education on these subjects. The Superintendent or the Superintendent's designee shall be responsible for identifying educational materials, lessons, and/or programs suitable for the age and maturity level of the students and for ensuring the delivery of such materials, lessons, and/or programs to students.

* Staff shall confine e-mail use to work-related purposes and a reasonable, appropriate and limited personal use that does not interfere with their district duties.

Adopted 6/14/98 Amended 7/12/99 Amended 5/14/01 Reviewed 7/12/10
Revised 6/11/12 Revised 11/19/18

Policy 4012.1
Cozad Community Schools Acceptable Use Policy

The school's information technology resources, including email and Internet access, are provided for educational purposes. Adherence to the following policy is necessary for continued access to the school's technological resources:

I. Staff/Students must

A. Respect and protect the privacy of others.

1. Use only assigned accounts.
2. Not view, use, or copy passwords, data, or networks to which they are not authorized.
3. Not distribute private information about others or themselves.

B. Respect and protect the integrity, availability, and security of all electronic resources.

1. Observe all network security practices, as posted.
2. Use personal mobile devices on the public network only.
3. Not log in (authenticate) to the private network unless using district owned/authorized devices or services.
4. Report security risks or violations to a teacher or network administrator.
5. Not destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner.
6. Conserve, protect, and share these resources with other students and Internet users.

C. Respect and protect the intellectual property of others.

1. Not infringe copyrights (no making illegal copies of music, games, or movies!).
2. Not plagiarize.

D. Respect and practice the principles of community.

1. Communicate only in ways that are kind and respectful.
2. Report threatening or discomforting materials to a teacher.
3. Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).
4. Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).

5. Not use the resources to further other acts that are criminal or violate the school's code of conduct.
6. Not send spam, chain letters, or other mass unsolicited mailings.
7. Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

Staff/Students may, if in accord with the policy above

A. Design and post web pages and other material from school resources.
B. Responsibly use social networking and internet communication resources with a teacher's permission and within the guidelines stated above.
C. Install or download software, if also in conformity with laws and licenses, and under the supervision of a teacher.
D. Use the resources for any educational purpose.

Social Networking:

Social networking sites and resources (Facebook, YouTube, Twitter, etc) can be useful tools in the school environment, and may be utilized in the classroom. Certain guidelines should be followed:

Follow the District Handbook etiquette guidelines and the school's code of conduct when posting online. What is inappropriate in the classroom is inappropriate online.

Do not use other people's intellectual property, including pictures, without their permission. It is a violation of copyright law to copy the words of others without proper attribution.

If you encounter inappropriate material, feel threatened or harassed, or find material that violates the school’s code of conduct, notify a teacher or administrator immediately.

All student online activity making use of school equipment or websites must be in compliance with the district’s Acceptable Use Policy.

Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of 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.

Administrative Guidelines for Policy 4012.1

Following are examples of what does, or does not, constitute "fair use:"

1. Fair use applies only to reproduction for such purposes as criticism, comment, news reporting, teaching, scholarship, or research.
2. The fact that copying is for nonprofit use has no bearing on the question of fair use;
3. Copying portions of a news article may be fair use, but copying from a workbook designed for a course of study is not;
4. Photocopying or duplicating by an individual for personal use, as long as it is a single copy of an article, short poem, or small portion of the work as a whole, is generally considered fair use;
5. Fair use allows teachers, acting of their own, to copy small portions of a work for the classroom, but does not allow an institution to do so;
6. Systematic duplication, whether making multiple copies at one time or single copies that in the aggregate add up to multiples, is not considered fair use; and
7. If resulting economic loss to the copyright owner can be shown, even making a single copy of certain materials may be a violation.

The following notice shall be placed on or near all equipment capable of duplicating or transmitting copyrighted materials.

> "The copyright laws of the United States govern the duplication, retention, transmittal and use of copyrighted material. Anyone using this equipment is responsible for compliance with the law. Person who secures permission, license, or other contractual agreements shall maintain adequate records regarding the use of copyrighted materials."

Adopted 12/8/98 Reviewed 6/14/10 Revised 11/19/18