

|              |                                                             |
|--------------|-------------------------------------------------------------|
| Book         | Policy Manual                                               |
| Section      | 800 Operations                                              |
| Title        | Acceptable Use of Internet, Computers and Network Resources |
| Code         | 815                                                         |
| Status       | First Reading                                               |
| Last Revised | February 11, 2021                                           |

## **Purpose**

The **Joint** Operating Committee supports use of the computers, Internet and other network **resources** in the school’s instructional **and operational** programs in order to facilitate learning, teaching **and daily operations** through interpersonal communications **and** access to information, research and collaboration.

**The school provides students, staff and other authorized individuals with access to the school’s computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.**

**For instructional purposes,** the use of network facilities shall be consistent with the curriculum adopted by the school as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

## **Definitions**

**The term child pornography is defined under both federal and state law.**

**Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:**[\[1\]](#)

- 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;**
- 2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or**
- 3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.**

**Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.**[\[2\]](#)

**The term harmful to minors is defined under both federal and state law.**

**Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:**[\[3\]](#)[\[4\]](#)

- 1. Taken as a whole, 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 lewd exhibition of the genitals; and**
- 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.**

**Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:**[\[5\]](#)

- 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;**
- 2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and**
- 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.**

**Obscene - any material or performance, if:**[\[5\]](#)

- 1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;**
- 2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and**
- 3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.**

**Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.**[\[4\]](#)

## **Authority**

The availability **of access to** electronic information does not imply endorsement by the school of the content, nor does the school guarantee the accuracy of information received. The school shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The school shall not be responsible for any unauthorized charges or fees resulting from access to the Internet **or other network resources.**

The Joint Operating Committee declares that computer and network use is a privilege, not a right. The school's computer and network resources are the property of the school. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the school's Internet, computers or network resources, including personal files or any use of the school's Internet, computers or network resources. The school reserves the right to monitor, track, and log network access and use; monitor files server space utilization by users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The school shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the school's Internet, computers and network resources. [6][7][8]

The Joint Operating Committee requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Director or designee.

The JOC is granted the right to determine what sort of content is specifically inappropriate to minors by 47 USC 254; this list should be included in the adopted policy. Such a list has been added to the Authority section, please review and revise as necessary. **IMPORTANT NOTE: There is a space in this list to add additional items as the CTC wishes.**

The Joint Operating Committee establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors: [4]

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory. [9][10][11]
5. Bullying. [12]
6. Terroristic. [13]
7. { } \_\_\_\_\_ (specify others).

The school reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Joint Operating Committee policy, or the use of software and/or online server blocking. Specifically, the school operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access. [3][4][14]

Upon request by students or staff, the Director or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy. [14]

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Director or designee for expedited review. [3][15]

#### Delegation of Responsibility

The school shall make every effort to ensure that this resource is used responsibly by students and staff.

The school shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the school website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request. [14]

Users of school networks or school-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the school uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Student user agreements shall also be signed by a parent/guardian.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the school and on the Internet.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

The Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the school's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to: [3][4][16]

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Joint Operating Committee.
2. Maintaining and securing a usage log.
3. Monitoring online activities of minors.

The Director or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including: [4]

1. **Interaction with other individuals on social networking websites and in chat rooms.**

2. **Cyberbullying awareness and response.**<sup>[12]</sup><sup>[17]</sup>

## Guidelines

Network accounts **shall** be used only by the authorized owner of the account for its **approved** purpose. Network users shall respect the privacy of other users on the system.

## Safety

**It is the school's goal to protect users of the network** from harassment **and** unwanted or unsolicited **electronic** communications. Any network user who receives threatening or unwelcome **electronic** communications **or inadvertently visits or accesses an inappropriate site shall report such** immediately to a teacher or administrator. Network users shall not reveal personal **information** to other users on the network, **including chat rooms, email, social networking websites, etc.**

**Internet safety measures shall effectively address the following:**<sup>[4]</sup><sup>[16]</sup>

1. **Control of access by minors to inappropriate matter on the Internet and World Wide Web.**
2. **Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.**
3. **Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.**
4. **Unauthorized disclosure, use, and dissemination of personal information regarding minors.**
5. **Restriction of minors' access to materials harmful to them.**

## Prohibitions

**Users** are expected to act in a responsible, ethical and legal manner in accordance with **Joint Operating Committee** policy, accepted rules of network etiquette, and federal and state law. **Specifically, the following uses are prohibited:**

1. **Facilitating illegal activity.**
2. **Commercial or for-profit purposes.**
3. **Nonwork or nonschool related work.**
4. **Product advertisement or political lobbying.**
5. **Bullying/Cyberbullying.**<sup>[12]</sup><sup>[17]</sup>
6. **Hate mail, discriminatory remarks, and offensive or inflammatory communication.**
7. **Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.**
8. **Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.**<sup>[18]</sup>
9. **Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Joint Operating Committee policy.**
10. **Inappropriate language or profanity.**
11. **Transmission of material likely to be offensive or objectionable to recipients.**
12. **Intentional obtaining or modifying of files, passwords, and data belonging to other users.**
13. **Impersonation of another user, anonymity, and pseudonyms.**
14. **Fraudulent copying, communications, or modification of materials in violation of copyright laws.**<sup>[19]</sup>
15. **Loading or using of unauthorized games, programs, files, or other electronic media.**
16. **Disruption of the work of other users.**
17. **Destruction, modification, abuse or unauthorized access to network hardware, software and files.**
18. **Accessing the Internet, school computers or other network resources without authorization.**
19. **Disabling or bypassing the Internet blocking/filtering software without authorization.**
20. **Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.**

## Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or school files. To protect the integrity of the system, **these** guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another student's or **employee's** name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

## Copyright

The illegal use of copyrighted **materials** is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines **and applicable laws and regulations**.<sup>[19]</sup><sup>[20]</sup>

## School Website

**The school shall establish and maintain a website and shall develop and modify its web pages to present information about the school under the direction of the Director or designee. All users publishing content on the school website shall comply with this and other applicable Joint Operating Committee policies.**

**Users shall not copy or download information from the school website and disseminate such information on unauthorized web pages without authorization from the building administrator.**

## Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.<sup>[14]</sup>

Illegal use of the network; intentional deletion or damage to files **or** data belonging to others; copyright violations; **and** theft of services **shall** be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

Vandalism **shall** result in **loss** of access privileges, **disciplinary action, and/or legal proceedings. Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

**Failure to comply with this policy or inappropriate use of the Internet, school network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.**<sup>[6]</sup><sup>[7]</sup><sup>[8]</sup>

## Legal

1. 18 U.S.C. 2256
2. 18 Pa. C.S.A. 6312
3. 20 U.S.C. 7131
4. 47 U.S.C. 254
5. 18 Pa. C.S.A. 5903
6. Pol. 218
7. Pol. 233
8. Pol. 317
9. Pol. 103
10. Pol. 103.1
11. Pol. 104
12. Pol. 249
13. Pol. 218.2
14. 24 P.S. 4604
15. 24 P.S. 4610
16. 47 CFR 54.520
17. 24 P.S. 1303.1-A
18. Pol. 237
19. Pol. 814
20. 17 U.S.C. 101 et seq
- 18 Pa. C.S.A. 2709
- 24 P.S. 4601 et seq
- Pol. 220