CARBON CAREER & TECHNICAL INSTITUTE

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMPUTER NETWORKS/DIGITAL TECHNOLOGY/INTERNET AND INTERNET SAFETY

ADOPTED: August 19, 2004

REVISED: December 17, 2009, June 21, 2012

815. ACCEPTABLE USE OF COMPUTER NETWORKS/DIGITAL TECHNOLOGY/INTERNET AND INTERNET SAFETY

1. Purpose	The Joint Operating Committee supports use of the Internet and other computer networks in the school's instructional program in order to facilitate learning and teaching through interpersonal communications and access to information, research and collaboration. The use of network facilities shall be consistent with the curriculum adopted by the Joint Operating Committee as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.
2. Authority	The Joint Operating Committee reserves the right to determine which network services will be provided through school resources.
SC 1303.1-A 24 P.S. Sec. 4601 et seq 47 U.S.C. Sec. 254	The District recognizes the importance of teaching acceptable use and online safety to students. The District curriculum shall include instruction for educating minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response. The electronic information available to students and staff does not imply endorsement of the content by the school, nor does the school guarantee the accuracy of information received on the Internet. 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. The school reserves the right to log network use and to monitor fileserver space utilization by users, while respecting the privacy rights of both school users and outside users. The Joint Operating Committee establishes that use of the Internet and the mail server is a privilege, not a right; inappropriate, unauthorized or illegal use will result in cancellation of those privileges and appropriate disciplinary action.

P.L. 106-554 Sec. 1732	The Joint Operating Committee shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.
3. Definitions 18 U.S.C. Sec. 2256	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. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
18 Pa. C.S.A. Sec. 6312	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. Federal and state law defines a minor as an individual under the age of eighteen (18) years.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 18 Pa. C.S.A. Sec. 5903	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. 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.
18 Pa. C.S.A. Sec. 5903	**Obscene** - any material or performance, if: 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.
47 U.S.C. Sec. 254	**Technology protection measure** - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors
47 CFR Sec. 54.520	1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, pornographic, harmful to minors when used by minors, or determined inappropriate by the Board for use by minors. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
47 U.S.C. Sec. 254	The District shall develop and implement curriculum that ensures students are educated on network etiquette and other appropriate online behavior, including: 1. Interaction with other individuals on social networking web sites and in chat rooms. 2. Cyberbullying awareness and response.
SC 1303.1-A Pol. 249 3. Delegation of Responsibility	The school shall make every effort to ensure that this educational resource is used responsibly by students and staff. Administrators, teachers and other staff have a professional responsibility to help students develop the skills necessary to discriminate among information sources, identify information appropriate to their age and developmental levels, and evaluate and use the information to meet their educational goals. Through a program of education, the school will educate students and teachers about their individual responsibility to refrain from engaging unacceptable uses of the network, as well as the consequences if they violate the policy. Students and staff have the responsibility to respect and protect the rights of every other user in the school and on the Internet. The building principal shall have the authority to determine what is inappropriate use.
P.L. 106-554 Sec. 1711, 1721	The Administrative Director or designee shall be responsible for implementing technology and procedures to determine whether the school's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to: 1. Utilizing a technology protection measure that blocks or filters Internet access to obscene visual depictions, child pornography, or other material determined inappropriate for use by minors by the Joint Operating Committee.

	2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
4. Guidelines	Network accounts shall be used only by the authorized owner of the account for its authorized purpose. Network users shall respect the privacy of other users on the system. <u>E-mail</u> E-mail is restricted to teacher-assigned projects as an integral part of a curriculum process; therefore, e-mail is subject to review by school personnel and should never be considered as private. If there is a reason to believe that e-mail is being used for purposes specifically prohibited by this policy or for illegal activity, the user account will be disabled until school authorities can confer with the user to determine the nature of the problem. The school reserves the right to revoke user privileges, remove user accounts, and refer matters to legal authorities when violation of this and any other applicable school policies occur, including, but not limited to those governing network use, copyright, security, and vandalism of school resources and equipment. <u>Access To Accounts</u> Accounts/Access will be made available according to a schedule developed by appropriate staff given the capability of school hardware. Account/Access will be given only to those individuals who: 1. Have read this policy and indicate their agreement with its provisions by signing the signature page and returning it to the appropriate school authority. Students must have their parent/guardian sign this signature page indicating the parent/ guardian's agreement with the policy and his/her consent to allow the student to access and use the network. Staff members must sign this form and also return it to the Administrative Director or designee. 2. Have successfully completed the appropriate orientation/instruction on network access, use, acceptable vs. unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities. This requirement shall apply to both students and employees.

Prohibitions

Students and staff 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.

The activities listed below are strictly prohibited by all users of the network. The school reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the network. These prohibitions are in effect any time school resources are accessed in any way whether in the school, or indirectly through another Internet service provider:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Hate mail, harassment or discriminatory remarks, and other anti-social, offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Access to or transmission of obscene or pornographic material or child pornography.
8. 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.
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of local, state or federal laws.

14. Loading or using of unauthorized games, programs, files, or other electronic media.

15. Disruption of the work of other users.

16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

17. Quoting of personal communications in a public forum without the original author's prior consent.

18. Allowing an unauthorized person to use an assigned account.

19. Communicating through e-mail for noneducational purposes or activities.

20. Participating in inappropriate and/or objectionable discussions or newsgroups.

21. Ordering or purchasing in the name of the school or in the name of any individual any type of merchandise or service. All costs to the school or any individual incurred because of this type of violation will be the responsibility of the user.

22. Malicious use of the network to develop programs that harass other users or infiltrate a computer system and/or damage the software components of a computer system.

23. Participating in unauthorized Internet Relay chats (online real-time conversation).

24. Advocate illegal drug use, whether expressly or through a latent pro-drug message. This does not include a restriction on political or social commentary on issues, such as the wisdom of the war on drugs or medicinal use.

25. Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/proxies or any websites that mask the content the user is accessing or attempting to access.

26. Attempt to and/or obtain personal information under false pretenses with the intent to defraud another person.

27. Access to sexually oriented chat rooms, e-mail exchanges and/or visuals, texts and sounds that are sexually oriented, obscene, pornographic and extremely violent.

28. Students are not permitted to record video/audio on school grounds without the prior consent of administration. Violators will be subject to CCTI disciplinary policy.

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, the following 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 teacher'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.

User names and passwords shall only be used in an authorized manner in the course of official school business. Furthermore, they shall be stored in a secure location accessible only by the Technology Coordinator and the Administrative Director, subject to the terms of this policy. The Administrative Director and Technology Coordinator are responsible for authorizing, adding, deleting, or changing a User ID.

Consequences For Inappropriate Use

Any user of the network, whether student or employee, who violates the prohibitions listed in this policy, engages in any other act determined to be unacceptable use of the network by school authorities, or violates any school policy will have his/her user privileges revoked in progressive fashion and may be subject to other disciplinary procedures according to existing and applicable school policies.

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.
Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will 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. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

	Vandalism will result in cancellation of access privileges. 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. <u>Copyright</u>
P.L. 94-553 Sec. 107	The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines. <u>Safety</u> To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications immediately shall bring them to the attention of a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc. Any school computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
P.L. 106-554 Sec. 1732	Internet safety measures shall effectively address the following: 1. Control of access by minors to inappropriate matter on the Internet. 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.
20 U.S.C. Sec. 6777 School Code 24 P.S. Sec. 4601 et seq	