CONRAD WEISER AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF TECHNOLOGY

ADOPTED: June 17, 2009

REVISED: June 20, 2012

815. ACCEPTABLE USE OF TECHNOLOGY

1. Purpose

The Board supports use of the Internet and other information technology resources to facilitate learning, teaching, and educational operations. Access to and use of these resources is essential to the learning, teaching and administration that occurs in our schools. Our goal is to give all users the opportunity to pursue educational and research activities in a safe and effective manner that complies with the law and regulations and our mission as a public school.

2. Authority

SC 4601
Title 22
Sec. 403.1

This policy applies to all users of district computers, network connectivity, and information technology resources (IT Resources). Each user of IT Resources agrees to abide by this policy by virtue of employment by the district. Additionally, all students are granted access to IT Resources and must obtain their parent's/ guardian's signature to restrict them from usage of the Internet. This policy shall be stated in the Student Handbook and distributed every year, and shall be available to parents/guardians upon written request.

The district reserves the right to access all IT Resources for any purpose and to disclose them to any other party, as it deems necessary and/or appropriate. Users should understand that there is no right of privacy with respect to information contained in the IT Resources, and the district's designated personnel may access such information at their discretion.

SC 1303.1-A
24 PS
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, chat rooms and cyberbullying awareness and response.

3. Guidelines

If any user has questions concerning this policy or its content, the user shall contact district IT personnel or an administrator. IT Resources are to be used only for purposes that are lawful, authorized, have educational value to the user consistent with the educational mission of the district, and are permitted by this policy.

	Use Of IT Resources The primary use of district IT Resources is reserved for those who need to access or obtain information and materials of educational value. Educational value means that the information and/or materials must have a direct impact on the user's current education program in which s/he is enrolled or is seeking to enroll. Entertainment or social-type activities, such as exchanging e-mail messages with friends; engaging in chat rooms; reading message boards; and other activities outside the scope of the user's education program, do not fall under the definition of educational value. Users who use IT Resources for noneducational purposes may be responsible for any costs associated with such noneducational use. The district may impose time restrictions on use of its IT Resources to ensure that all users have equal opportunity for use. The district also may create and enforce storage management procedures and revise such storage procedures, at its option. Prohibited Uses
47 U.S.C. Sec. 254	Users must act in a responsible, ethical and legal manner when using the IT Resources. They must also follow this and all other Board policies, use acceptable network etiquette, and comply with federal and state law. The following uses of district IT Resources are specifically prohibited: 1. Use in violation of any law or governmental rule or regulation. 2. Commercial or for-profit use. 3. Excessive nonwork or nonschool-related work. 4. Product advertising or political lobbying. 5. Exchanging (by sending, receiving, or in any way participating in) any hate mail or harassing, defamatory, offensive, fraudulent, abusive, obscene, profane, sexually-oriented, threatening, racially-offensive or illegal activities, materials or communications containing inappropriate language.
Pol. 814	6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials; copying, distributing, modifying, or using copyrighted materials in violation of copyright laws.

	7. Accessing or obtaining materials that are obscene, pornographic materials, or child pornography. 8. Access by students to material that is harmful or is determined by the district to be inappropriate for students. 9. Quoting a personal communication by means which make it public without the original author's prior consent. 10. Intentionally obtaining or modifying files, passwords, or data belonging to other users; impersonating another user; anonymity or using pseudonyms. 11. Loading or using unauthorized games, programs, files, or other electronic media. 12. Destruction, modification, abuse or unauthorized access to network hardware, software and files, including unauthorized access to the Internet or Intranet, unauthorized access to any sites on the Internet, and hacking activities. 13. Disrupting the work of others. 14. Other unacceptable activities as delineated in administrative guidelines or procedures. <u>Procedures</u>
SC 4601 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The Superintendent or designee is responsible for implementing technology and procedures to determine whether district computers are being used for lawful purposes, according to Board policy. These procedures include blocking or filtering Internet access on each computer to prevent access to visual depictions that are obscene, pornographic materials, or child pornography, and to prevent access by students to visual depictions that are harmful or are determined by the Board to be inappropriate for use by students. The district has the right to use additional measures to ensure that IT Resources are used responsibly and in accordance with laws and regulations, including security measures, intrusion detection measures, monitoring of utilization levels of file server space, and activity logging. The district also has the right, at any time, to monitor and supervise use of the IT Resources by students. <u>Disabling Filter Technology</u>
47 U.S.C. Sec. 254	Only the Superintendent or designee shall disable filtering technology or any other technology protection measure the district has placed on its computers. A user may not disable such technology.

	Any employee who desires to have such technology disabled must present a request in writing to the Superintendent or designee, and the Superintendent or designee shall determine whether or not to grant the request. Disabling of technology shall occur only for the purpose of enabling access by employees to the Internet to perform bona fide research or for other lawful purposes. Confidential Information Confidential information of the district, personnel, students, any personal identification information regarding personnel or students, and any other confidential information and/or information protected by the Family Educational Rights and Privacy Act or by a Board policy may not be transmitted by users via the IT Resources to other users or to third parties without authorization. This includes transmission via chat rooms, e-mail, the Internet, or any other means. Additionally, all users of IT Resources must be aware and understand that communications via e-mail or the Internet are not secure and are subject to hacker or other interference, the confidentiality of information communicated via e-mail or the Internet cannot be guaranteed during transmission, and recipients might not keep information confidential. Therefore, users shall not transmit any confidential information via e-mail or the Internet and any confidential information which a user wishes to transmit (which may not include any district confidential information) shall be transmitted by traditional nonelectronic forms of communications. In the event that confidential information is or must be shared via the Internet or e-mail, the district's security or encryption procedures must be followed. Communications Compliance
18 U.S.C. Sec. 251 et seq	Users must comply with all laws, governmental rules, and regulations, including the Electronic Communications Privacy Act, which prohibits the unauthorized interception or disclosure of e-mail messages by third parties. The district has the authority to monitor all electronic communications and file server use. Security Procedures Each user shall log on and log off the IT Resources using proper security conventions established by the district. Users must lock or log off when leaving IT Resources unsupervised. Users shall be responsible to follow log-in procedures and to select appropriate passwords that must be kept private and not shared with anyone else.

It is each user's responsibility to periodically, as set by district guidelines, change their passwords and select passwords that cannot be easily guessed. Users may not allow others to use their passwords or to share their accounts.

Users are further responsible for all e-mail and Internet or Intranet activity that occurs through the use of their passwords and/or log-ins.

Any attempt to circumvent IT security measures, to guess passwords, or to otherwise gain unauthorized access to or use IT Resources is strictly prohibited.

Inappropriate/Improper Use

Use of IT Resources is a privilege, not a right.

Users are responsible for following all district procedures, guidelines and Board policies for use of IT Resources. Copies of applicable procedures, guidelines, and policies are available upon request or can be viewed at the central administration office. Users who violate district procedures, guidelines and/or Board policies or engage in inappropriate, unauthorized and/or illegal use of IT Resources shall have their privileges canceled and be denied access to IT Resources for a period of time and, in the sole discretion of the administration, may be subject to other disciplinary measures, including suspension or expulsion for students and suspension or termination of employment for employees.

Users are responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

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

Vandalism shall result in cancellation of access privileges. **Vandalism** includes any malicious attempt to harm or destroy data of another user, Internet or other networks and includes, among other actions, uploading or creating computer viruses.

Devices

Users may not repair, reconfigure, modify, or attach external devices to the IT Resources unless approved by authorized district IT Resources personnel. Hardware and software shall only be installed by authorized technology personnel.

Users may not download or install applications or executable files from the Internet.

	Disclaimer Of Liability The district shall have no liability or responsibility for any direct, indirect, or consequential losses or damages to a user or a third party, or data resulting from use of the IT Resources. The fact that electronic information is made available to users via district computers does not imply endorsement by the district of any content, nor does the district guarantee the accuracy or security of any information. The district shall have no liability for any information that may be lost, damaged, or unavailable when using the IT Resources or for any information retrieved via the Internet or Intranet. Employee Education
Pol. 829	All current employees shall receive a copy of the Whistleblower Policy. All new employees shall be required to sign a statement indicating that they have read and understand this policy as part of their orientation. The district shall annually inform all employees of the Whistleblower Policy and the identification of the Compliance Officer. References: Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. United States Copyright Law – 17 U.S.C. Sec. 101 et seq. Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777 Internet Safety – 47 U.S.C. Sec. 254 Electronic Communications Privacy Act – 18 U.S.C. Sec. 2511 School Code – 24 P.S. Sec. 4601 State Board of Education Regulations – 22 PA Code Sec. 403.1 Board Policy – 814, 829