Blount County Board of Education

Monitoring:	Descriptor Term:	Descriptor Code:	Issued Date:
Review: Annually, in November	**Internet, Network Access and Computer Hardware/Software Rights and Obligations/Security Plan**	**4.406**	**10/13/16**
		Rescinds: **4.406**	Issued: **03/05/09**

The board supports the right of staff and students to have reasonable access to various information formats and believes that it is incumbent upon staff and students to use this privilege in an appropriate and responsible manner.

Employees

Before any employee is allowed use of the district's Internet or intranet access, the employee shall sign a written agreement, developed by the director/designee that sets out the terms and conditions of such use. Any employee who accesses the district's computer system for any purpose agrees to be bound by the terms of that agreement, even if no signed written agreement is on file.

The director of schools shall develop and implement procedures for appropriate Internet use which shall address the following:

1. Development of the Network and Internet Use Agreement.
2. General rules and ethics of Internet access.
3. Guidelines regarding appropriate instruction and oversight of student Internet use.
4. Prohibited and illegal activities, including but not limited to the following:[1]
    a. Sending or displaying offensive messages or pictures
    b. Using obscene language
    c. Harassing, insulting, defaming or attacking others
    d. Damaging computers, computer systems or computer networks
    e. Hacking or attempting unauthorized access to any computer
    f. Violation of copyright laws
    g. Trespassing in another's folders, work or files
    h. Intentional misuse of resources
    i. Using another's password or other identifier (impersonation)
    j. Use of the network for commercial purposes
    k. Buying or selling on the Internet
    l. Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation
    m. Installing software or hardware that has not been inspected and authorized by the Technology Department
    n. Attaching any device that has not been authorized by the Technology Department. Attaching non-county owned computers without written permission from the Technology Department
    o. Using network resources to play or download games, music or videos that are not in support of business or educational functions

p. Leaving workstation unattended without engaging password protection for the key board or workstation
q. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing
r. Utilizing unauthorized virtual private networks (VPNs)
s. Using network resources for or in support of unlawful activities as defined by federal, state, and local law
t. Utilizing network resources for activities that violate conduct policies established by the Board of Education or the user's department
u. Sending unsolicited junk email, advertising, items-for-sale postings, or chain letters (e.g. "spam") to any users of the network
v. Knowingly sending any material that contains viruses, Trojan horses, worms, timebombs, bots, or any other harmful or deleterious programs
w. Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher
x. Sending or receiving communications that violate conduct policies established by the Board of Education or the user's department
y. Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary) being met
z. Use for partisan political purposes
aa. Confidential and sensitive information such as performance reviews, disciplinary and/or corrective actions, attorney-client privileged information, personal information, and health or medical information should not be communicated via e-mail
bb. Using the Internet to access non-County Schools provided web email services
cc. Using unapproved Instant Messaging or Internet Relay Chat (IRC)
dd. Using the Internet for broadcast audio for non-business use

Students

The director of schools shall develop and implement procedures for appropriate Internet use by students. Procedures shall address the following:

1. General rules and ethics of Internet use.
2. Prohibited or illegal activities, including, but not limited to:[1]
    a. Sending or displaying offensive messages or pictures
    b. Using obscene language
    c. Harassing, insulting, defaming or attacking others
    d. Damaging computers, computer systems or computer networks
    e. Hacking or attempting unauthorized access to any computer
    f. Violation of copyright laws
    g. Trespassing in another's folders, work or files
    h. Intentional misuse of resources
    i. Using another's password or other identifier (impersonation)
    j. Use of the network for commercial purposes
    k. Buying or selling on the Internet
    l. Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation

m. Installing software or hardware that has not been inspected and authorized by the Technology Department
n. Attaching any device that has not been authorized by the Technology Department. Attaching non-county owned computers without written permission from the Technology Department
o. Using network resources to play or download games, music or videos that are not in support of business or educational functions
p. Leaving workstation unattended without engaging password protection for the key board or workstation
q. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing
r. Utilizing unauthorized virtual private networks (VPNs)
s. Using network resources for or in support of unlawful activities as defined by federal, state, and local law
t. Utilizing network resources for activities that violate conduct policies established by the Board of Education or the user's department
u. Sending unsolicited junk email, advertising, items-for-sale postings, or chain letters (e.g. "spam") to any users of the network
v. Knowingly sending any material that contains viruses, Trojan horses, worms, timebombs, bots, or any other harmful or deleterious programs
w. Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher
x. Sending or receiving communications that violate conduct policies established by the Board of Education or the user's department
y. Sending confidential material to an unauthorized recipient, or sending confidential e-mail without the proper security standards (including encryption if necessary) being met
z. Use for partisan political purposes
aa. Confidential and sensitive information such as performance reviews, disciplinary and/or corrective actions, attorney-client privileged information, personal information, and health or medical information should not be communicated via e-mail
bb. Using the Internet to access non-County Schools provided web email services
cc. Using unapproved Instant Messaging or Internet Relay Chat (IRC)
dd. Using the Internet for broadcast audio for non-business use

INTERNET SAFETY MEASURES[3]

Internet safety measures shall be implemented that effectively address the following:

- Controlling access by students to inappropriate matter on the Internet and World Wide Web
- Safety and security of students when they are using electronic mail, chat rooms, and other forms of direct electronic communications
- Preventing unauthorized access, including "hacking" and other unlawful activities by students on-line
- Unauthorized disclosure, use and dissemination of personal information regarding students
- Restricting students' access to materials harmful to them

The director of schools/designee shall establish a process to ensure the district's education technology is not used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

- Utilizing technology that blocks or filters Internet access (for both students and adults) to material that is obscene, child pornography or harmful to students
- Maintaining and securing a usage log
- Monitoring on-line activities of students

The Board shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate, its Internet safety measures. A written parental consent shall be required prior to the student being granted access to electronic media involving district technological resources. The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations, must be signed by the parent/legal guardian of minor students (those under 18 years of age) and also by the student. This document shall be executed each year and shall be valid only in the school year in which it was signed unless parent(s) provide written notice that consent is withdrawn. In order to rescind the agreement, the student's parent/guardian (or the student who is at least 18 years old) must provide the director of schools with a written request.

E-MAIL

Users with network access shall not utilize district resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system. All data including e-mail communications stored or transmitted on school system computers shall be monitored. Employees/students have no expectation of privacy with regard to such data. E-mail correspondence may be a public record under the public records law and may be subject to public inspection.[2]

INTERNET SAFETY INSTRUCTION[4]

Students will be given appropriate instruction in internet safety as a part of any instruction utilizing computer resources K-12. Parents and students will be provided with material to raise awareness of the dangers posed by the internet and ways in which the internet may be used safely. Professional development opportunities will be provided for teachers and staff across the District.

SOCIAL NETWORKING

1. District staff who have a presence on social networking websites are prohibited from posting data, documents, photographs, or inappropriate information that is likely to create a material and substantial disruption of classroom activity.

2. District staff are prohibited from accessing personal social networking sites on school computers or during school hours except for legitimate instructional purposes.

3. The board discourages district staff from socializing with students on social networking websites. The same relationship, exchange, interaction, information, or behavior that would be unacceptable in a non-technological medium is unacceptable when done through the use of technology.

VIOLATIONS

Violations of this policy or a procedure promulgated under its authority shall be handled in accordance with the existing disciplinary procedures of this District.

Legal References

1. TCA 39-14-602
2. TCA 10-7-512
3. Children's Internet Protection Act (Public Law 106-554)
4. TCA 49-1-221

Cross References

Use of Electronic Mail (e-mail) 1.805
School and System Websites 4.407