Agenda Request Form

Meeting Date	Agenda Item Number
September 16, 2021	C-1

Title

Approval of Modifications to School Board Policy (IFBG) Internet Acceptable Use - - on Final Reading

Requested Action

School Board Consideration of Superintendent's Recommendation for Approval of Modifications to School Board Policy (IFBG) Internet Acceptable Use - - on Final Reading

Summary Explanation and Background

After a legal review of the software to be utilized in our new Cybersecurity Pathway at the C3 Academy, it has been recommended that we have all students in that class sign a Cybersecurity Program User Agreement/Waiver relative to accessing systems and networks by exploiting security vulnerabilities. While students in this program of study will be accessing a server/network completely separate from the CCSD network, we will recommend a slight modification to the Board's Policy on Internet Acceptable Use (IFBG) on first reading at your August School Board meeting. The recommended Policy language will provide exemption to students in this pathway from some security provisions contained within the Policy and is attached for your review and approval on final reading.

Priority Area

Student Achievement: Access and Opportunity

Financial Impact

N/A

Exhibits: (List)

Proposed Policy

Source of Additional Information

Dr. Brian V. Hightower	770.479.1871
Tom Roach	770.479.1871
Dr. Nicole Holmes and Bobby Blount	770.479.1871

The Cherokee County Board of Education recognizes that electronic media, such as the Internet, offers vast, diverse, and unique resources to both students and teachers that should promote educational excellence in our schools. The intent of this ~~p~~Policy is to help ensure that all uses of the Cherokee County School District's (School District) Internet connection are for support of education and research and are consistent with the goals and educational philosophy of the School District.

I. INTERNET PROTECTION

The School District will utilize a required technology protection measure as defined in the Children's Internet Protection Act (CIPA). To the extent practicable, this technology protection measure will restrict access to visual depictions that are obscene, pornographic or harmful to minors, as defined in CIPA. Subject to administrative approval, technology protection measures may be disabled or minimized only for bona fide research or other lawful purposes.

All of the School District's Internet users are subject to the following rules and regulations:

II. STANDARDS FOR USAGE

1. **Acceptable Use** -- The purpose of the school Network/Internet is to support research and education in and among academic institutions in the United States and the world by providing access to unique resources and the opportunity for collaborative work. The use of the network must be consistent with the educational objectives of the School District. Transmission of any material in violation of any U.S., or state regulation or School District ~~p~~Policy is prohibited. This includes, but is not limited to the following: copyrighted material, threatening or obscene material or material protected by trade secret. Use for commercial activities or product advertisement is not acceptable unless approved by the School District. Use for political lobbying is prohibited, however, users may communicate with elected officials to express an opinion on political issues. All users will follow Internet Safety Guidelines developed by the School District.

2. **Privileges** -- Each user who receives access to the Internet must first participate in an Internet safety/acceptable use ~~p~~Policy training session. The use of the Internet is a privilege, not a right, and inappropriate use will result in a restriction of those privileges and may result in additional administrative disciplinary action. Also, the School District network administrator may close an account at any time as deemed necessary for the safety of the users and for the security and integrity of the School District's Network/Internet services.

3. **Security** -- Security on any computer system is a high priority, especially when the system involves many users. Passwords provide a level of security and must not be shared. Unauthorized attempts to logon to a Network/Internet as a network administrator or other system user may result in cancellation/denial of user

privileges. Any user(s) identified as a security risk or having a history of problems with other computer systems may be denied access to the Network/Internet services throughout the School District. If a security problem on the Network/Internet is suspected, users are required to notify the School District's Division of Technology and Information Services as soon as possible.

4. **Network/Internet Use Behavior Standards** -- All internet users are expected to abide by the following guidelines. These standards of behavior include, ~~(~~but are not limited to~~)~~, the following:

   a. Illegal activities are strictly prohibited.
      i. Violation of O.C.G.A. § 16-9-93 as it pertains to computer theft, computer trespass, and computer invasion of privacy, computer forgery, and computer password disclosure
      ii. Violation of O.C.G.A. § 16-11-37.1 as it pertains to dissemination of information through a computer or computer network of information, any picture, photograph, drawing, or verbal description designed to encourage, solicit or promote terroristic acts and/or threats

   b. Submitting, publishing or displaying profanity, vulgarities, defamatory language, intentionally inaccurate information, or inappropriate language is prohibited.

   c. Use of an identity other than the user's own is prohibited.

   d. Publishing personal information about students such as full name, address, phone number or social security number is prohibited.

   e. Electronic mail (e-mail) instant messages and other forms of messaging using District resources are not private. Inappropriate or illegal messages will be reported to the proper authorities.

   f. A user will not intentionally <u>and without authority</u> spread computer viruses, vandalize the data, infiltrate systems, damage hardware or software, or in any way disrupt the use of the <u>School District</u> network. <u>A student enrolled in a cybersecurity pathway course will not be in violation of this Policy when acting at the direction of the cybersecurity teacher(s). The teacher(s) of a cybersecurity pathway course will not be in violation of this Policy when acting within the guidelines for cybersecurity pathway courses established by the Superintendent.</u>

   g. Engaging in non-educational games and monopolizing resource time and materials is prohibited.

   h. All communications and information accessible via the network should be assumed to be subject to copyright law. The user is responsible for checking for copyrighted or licensing agreements. Data received through the Internet is subject

to the same rules of documentation as traditional information. Credit is to be given for all material used in research.

i. Copying or downloading software illegally from network sources, disks, or other electronic material to another computer is prohibited. Software installation must be approved by the School District's Division of Technology and Information Services.

j. Use of the Internet to access inappropriate matter is prohibited. This includes, but is not limited to the materials that are: obscene, sexually explicit, threatening, abusive, harassing, illegally damaging to another person's reputation and/or demeaning to genders, gender identity, sexual orientation, race, ethnicity, religion and national origins, contrary to the School District's ~~p~~Policy on harassment.

k. An authorized user will be ultimately responsible for all activity under their account and password. Accounts will be used only by the authorized user for the purposes specified.

l. Employee generated files are the property of the School District and may be accessed by appropriate authorized system personnel.

m. Local, state or federal officials may obtain access to electronic communications in conjunction with investigations or other purposes. In addition, messages sent over the electronic network may be subject to disclosure under the Open Records Act.

n. It will be the responsibility of all members of the School District staff to supervise and monitor usage of the computer, network device and access to the Internet in accordance with this ~~p~~Policy, the Children's Internet Protection Act and the Protecting Children in the 21st Century Act.

5. **Disclaimer** -- The School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The School District will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, service interruptions and exposure to offensive or threatening material. Use of any information obtained via the Network/Internet is at each user's own risk. The School District specifically denies any responsibility for the accuracy or quality of any information obtained through its services.

ADOPTED: August 21, 2008
REVISED: ~~September 1, 2016~~ August 19, 2021

Cherokee County Board of Education