Colquitt County Schools
Internet Safety Policy

Introduction

The Board recognizes that as telecommunications and other new technologies shift the ways that information may be accessed, communicated, and transferred by members of the society, those changes may also alter instruction and student learning. The Board generally supports access by students and staff to rich information resources. In a free and democratic society, access to information is a fundamental right of citizenship.

Telecommunications, electronic information sources, and networked services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, instructional and library media materials could usually be screened--prior to use--by committees of educators and community members intent on subjecting all such materials to reasonable selection criteria. Board Policy IFAA requires that all such materials be consistent with district-adopted guides supporting and enriching the curriculum while taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students. Telecommunications, because they may lead to any publicly available file server in the world, will open classrooms to electronic information resources which have not been screened by educators for use by students of various ages.

Electronic information research skills are now fundamental to preparation of citizens and future employees during an Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources. Staff will use Board Policies IFAA, IFBD, and IFBGC to (a) consult the guidelines for instructional materials and honor the goals for selection of instructional materials contained therein; (b) establish classroom and media center guidelines for student use of network services; and (c) closely supervise student use of the Internet/Intranet.

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. The network is provided for students to conduct research and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner.

Independent student use of telecommunications and electronic information resources will be permitted for instructional purposes. A form will be posted on the Colquitt County School System website and is available at each school for the parents or legal guardians of minor students (under 18 years of age) who wish to decline permission for his or her student to participate in instructional activities using these resources. Independent student use of personal electronic devices will be permitted for instructional purposes at the discretion of the attending school administration.

It is the policy of Colquitt County School System to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms

of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; (d) comply with the Children's Internet Protection Act (CIPA) [Public Law 106-554 (TITLE XVII) and 47 United States Code 254(h)]; and (e) provide instruction to students on the inherent dangers of social networking sites, online safety and privacy, and the characteristics of cyber-bullying and the recommended responses. School administrators will include cyber-bullying in school bullying prevention plans, provide parents anti-cyber-bullying information maintained on the district technology web page, and educate students about cyber-bullying, online safety and privacy, and appropriate online behavior which includes interacting with other individuals on social networking websites and in chat rooms/forums.

The Board authorizes the Superintendent to prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on instruction and student achievement.

Definitions

TECHNOLOGY PROTECTION MEASURE: The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;
2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United State Code; or
3. HARMFUL TO MINORS.

HARMFUL TO MINORS: The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

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

SEXUAL ACT; SEXUAL CONTACT: The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, and/or access to inappropriate information. Schools that permit educational use of personal electronic devices may choose to prohibit devices that access the Internet via personal WI-FI accounts or any

manner other than connecting through the secure wireless connection provided by the school system.

Specifically, as required by the Children's Internet Protection Act (CIPA), blocking shall be applied to visual depictions of material deemed obscene, child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled, bypassed, or, in the case of minors, minimized only for bona fide research or other educational and lawful purposes.

Acceptable Use

Operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. Therefore, the use of the network, personal devices approved by school administration, or school equipment must be in support of education and research consistent with the educational objectives of the Colquitt County School System. Transmission of any material in violation of any United States regulation, state regulation, or Colquitt County School System's policies is prohibited. This includes, but not limited to, copyrighted material, threatening, indecent, or obscene material, or material protected by trade secret, use for commercial activities, product advertisement, or political lobbying.

In schools where the educational use of personal electronic devices is permitted, the student is responsible for the device. The school/system is not responsible for damage or theft of devices.

Students are responsible for ensuring that any personal electronic devices or storage media are virus free and do not contain any unauthorized or inappropriate files.

Unacceptable Use

The purpose of the Colquitt County School System network is to support research and education. The Board reserves the right to determine the acceptability of any specific use of the network. The following guidelines, although not exclusive, constitute examples of unacceptable use of the Internet/Intranet:

1. No person shall use computers of the Colquitt County School System for commercial business or profit or for solicitations of purchases of any kind.
2. Neither students nor employees will use network resources to play non-instructional computer games.
3. No person shall damage classroom technology equipment, remove device batteries/components, or move equipment without permission. Any person found responsible for damages may be required to reimburse the school/district for the monetary value of repair or replacement.
4. No person shall deliberately access, remove, or copy any program or file on a computer belonging to someone else without specific authorization.

5. No person shall add, delete, or copy programs, tamper with existing programs in such a way that causes the computer to stop performing computer operations, or that disrupts the use of the network by others.
6. No person shall engage in any conduct, including taking or distributing still or motion images, e-mail, chat rooms/forums, or instant messaging, which harasses, libels, slanders, or in any way damages the reputation of another individual.
7. No person shall access, display, or send any materials that are profane, vulgar, threatening, pornographic, indecent, or harmful to minors.
8. No person may disguise or hide his/her identity, including changing his/her name on the system. Only members of the technology department may change any aspect of a user's account.
9. Under no circumstances should students arrange to meet an individual they have contacted while using system-computing resources. Students should notify the classroom teacher and their parent or guardian immediately upon an attempt by any user to arrange to meet them or upon a contact from a user for an illicit or suspicious purpose.
10. Teachers and students shall not use social networking or texting to interact for any reason other than educational purposes. Communication between school personnel and students/parents should always be transparent, accessible, and professional.

The teacher, principal, and Technology Director will have the discretion to immediately suspend or restrict any student or employee's access to and use of the Colquitt County School System's network resources or personal electronic devices upon the apparent breach of these terms and conditions of acceptable use. Teachers and administrators may request suspension of another user's access rights upon notification of the Technology Director. The user will be informed of the suspected breach of the Acceptable Use Policy and given the opportunity to explain the situation. If this explanation is not satisfactory, the principal or the employee's supervisor will provide a written incident report to the Technology Director.

Supervision, Monitoring, and Privilege

The use of the Internet/Intranet is a privilege, and as such is conditional upon the individual's compliance with any and all state and federal laws, school regulation, and the exercise of good manners. It shall be the responsibility of all members of the Colquitt County School System staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act (CIPA).

Procedures for the disabling, or otherwise modifying, of any technology protection measures shall be the responsibility of the Director of Network Services or designated representatives. Likewise, the Technology Director or Network Director may suspend or revoke privileges as deemed necessary.

Privacy

No student shall give out his/her personal information while using the Internet/Intranet resources of the Colquitt County School System unless authorized and as required for participation in approved sites. In addition, information of this kind should not be given regarding any other

user. No user shall give out his/her password to anyone other than the members of the Technology Department, nor shall any person use the account or password of any other Colquitt County School System user. Breaches of privacy are direct violations of the Acceptable Use Policy.

It is not the intention of the Colquitt County School system to actively monitor the electronic mail (e-mail) of account holders. However, there is no guarantee or reasonable expectation of privacy when e-mail is sent or received. During the course of maintaining the network, the members of the Technology Department will have access to all electronic messages and may inadvertently access inappropriate private messages or content that requires notification of the proper authorities. The Technology Director or Network Director may be requested to access a user's e-mail by the Superintendent or other officials if inappropriate or harmful use of the network is suspected.

Security

Security of any computer system is a high priority. Any user who suspects or identifies a network security problem must notify a classroom teacher or building-level administrator immediately. The principal or central office administrator should then notify the Technology Director. Network security problems must not be demonstrated to other users. User passwords are one element of network security and should remain private. Users should not reveal their passwords or allow another person to use their password. Any individual who steals or attempts to steal another user's password will lose network privileges. Access rights are another level of network security. Any user who attempts to change the level of his/her access rights or attempts to log into the network as a user with higher access rights will have his/her network privileges immediately canceled and face disciplinary action. Any user identified as a security risk, or having a history of problems with other computer systems, may be denied access to the Colquitt County School System's computer networks.

Facebook accounts for school activity groups such as clubs, class projects, or other student groups may not be created without prior approval by the school principal.

Voice-assisted Devices that can recognize individual students' voices and "understand" their specific learning needs or requests raise concerns with the Children's Online Privacy Protection Act (COPPA) and the Family Educational Rights and Privacy Act (FERPA). The laws' guidelines are designed to protect children's privacy online and require explicit, verifiable consent from parents in order to store a child's personal information. Furthermore, the Children's Online Privacy Protection Act (COPPA) gives parents control over what information websites can collect from children. Parents have the right to review and delete information gathered about their children, and the law forbids the passive tracking of a child online. Voice-assisted devices like Amazon/Alexa, Google Assistant, or even iPhone/Siri are specifically designed for passive tracking but offer no means to review or delete information gathered. These products are designed for personal home use. Although Amazon/Alexa is beginning to enter the education market at the university level, company representatives do not endorse the use of the devices in the PK-12 setting.

Copyright Guidelines

The Colquitt County School System abides by all federal copyright guidelines, laws, and licensing agreements governing the use of software. All users must also abide by these guidelines. To avoid copyright infringements, individual users must not download software without the express prior permission of the Technology Director. Commercial software must be properly obtained and documented with official school system purchase orders. Single user software may not be installed on multiple machines, and multi-station software must be installed in compliance with the number of users specified in the licensing agreement.

Personal streaming services (e.g., Netflix, Amazon Prime, Hulu, Sling TV, etc.) may not be accessed and used in classrooms. Most streaming services do not include legal rights to stream their content into a classroom. Technically, showing any streaming service for personal use in a classroom breaks the terms of service as it does not include an additional fee for a public display license. Streaming the content of personal use services into classrooms will raise the risk of future legal action due to copyright infringement.

Copyright infringement regarding commercial software must be reported to the Technology Director immediately. Employees may try "shareware" or "freeware" available on the Internet after approval by a member of the Technology Department. All conditions established by the authors of freeware and shareware must be followed including payment after a trial evaluation period or limitation on the number of users. If there is a time limit on the use of the software, it must be removed in compliance with the author's wishes.

On the Internet, there are other forms of digital information (e.g., text, images, audio, sound, animations, etc.) that may also be affected by copyright laws. The creators of this information may claim such materials as their "intellectual" property. Users must avoid plagiarism (i.e., claiming the works of someone else as your own). Students or school system employees may not download online materials for use without complying with the conditions established by the creator (e.g., payment, acknowledgment, etc.). Users may capture such digital information (e.g., text, images, audio, sound, animations, etc.) for use on Internet web pages, multimedia presentation, or school-related projects as long as copyright laws or a creator's specific restrictions are met. Copyright laws generally allow the use of someone else's information for educational purposes but with the restriction that it cannot be sold nor publicly displayed. All questions and concerns about possible copyright violations of material obtained over the Internet must be directed to a school's Media Specialist or the Technology Director.

Colquitt County Schools **Last Revised Date:** 06/03/2019
Original Adopted Date: 11/22/1999

References

Colquitt County Schools Board Policies
Colquitt County Board of Education Policy Manual
https://simbli.eboardsolutions.com/SB_ePolicy/SB_PolicyOverview.aspx?S=4042

CIPA Background
Summary with Full Text of the Children's Internet Protection Act (CIPA)
https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

FCC Regulations for Implementing CIPA: FCC 01-120
http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01120.doc

USAC's FAQ on E-Rate Certification Procedures for CIPA
http://www.sl.universalservice.org/reference/CIPAfaq.asp

These references are not intended to be part of the policy itself, nor do they indicate the basis or authority for the board to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

State Reference	Description
GA Code § 10-1-912 (2017)	Notification required upon breach of security regarding personal information
GA Code § 16-9-90 (2017)	Georgia Computer Systems Protection Act
GA Code § 16-9-91 (2017)	Legislative findings related to computer crimes
GA Code § 16-9-92 (2017)	Definitions
GA Code § 16-9-93 (2017)	Computer crimes defined
GA Code § 16-9-93.1 (2017)	Misleading transmittal
GA Code § 16-9-94 (2017)	Venue/Violations
GA Code § 16-9-122 (2017)	Attempting or conspiring to attempt identity fraud
GA Code § 16-11-37.1 (2017)	Dissemination of information relating to terroristic acts
GA Code § 16-12-100.1 (2017)	Electronically furnishing obscene material to minors
GA Code § 16-12-100.2 (2017)	Computer or electronic pornography and child exploitation prevention
GA Code § 20-2-324 (2017)	Internet safety policies in public schools
GA Code § 39-5-2 (2017)	Subscriber's control of minor's use of Internet
GA Code § 39-5-3 (2017)	Immunity
GA Code § 39-5-4 (2017)	Online Internet Safety report of certain information

Federal Reference	Description
15 USC 6501	Children's Online Privacy Protection Act - Definitions
15 USC 6502	Children's Online Privacy Protection Act - Regulation of unfair and deceptive acts in collection and use of personal information from and about children on the Internet
15 USC 6503	Children's Online Privacy Protection Act - Safe harbors
20 USC 7131	Internet Safety
47 USC 254(h)(5)	Universal Service-Requirements for certain schools with computers having Internet access