IFBGE Internet Safety

7/1/13

It is the policy of the Cobb County School District (District) 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) educate minors about appropriate online behavior, including interacting with other individuals on social networks, websites, and in chat rooms and cyber bullying awareness and response; and (e) comply with the Children's Internet Protection Act, the Neighborhood Children's Protection Act and the Protecting Children in the 21st Century Act (collectively "CIPA").

A. GENERAL PROVISIONS:

1. **CIPA COMPLIANCE:**
   The District will have the following in continuous operation, with respect to all computers belonging to the District:
   a. A qualifying "technology protection measure," as that term is defined in CIPA, to block or filter access to the Internet by adults and minors to visual depictions that are obscene, pornographic or harmful to minors as those terms are defined in CIPA. Subject to staff supervision and advance approval by a technology administrator or other person authorized by the District, the technology protection measure may be disabled for adults engaged in bona fide research or other lawful purposes.
   b. Procedures, materials and/or guidelines developed by the Curriculum, Instruction and Assessment Division and the Technology Services Division which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA, and to material deemed inappropriate for minors as determined by the District. Such procedures, materials or guidelines will be designed to:
      (1) Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to harmful or inappropriate matter on the Internet and the World Wide Web;
      (2) Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
      (3) Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
      (4) Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
      (5) Restrict minors' access to materials "harmful to minors," as that term is defined in CIPA.
   c. Educational materials, guidelines and procedures which shall be used to educate minors on appropriate online behavior, including without limitation interacting with other individuals on social networking Web Sites and chat rooms and cyber-bullying awareness and response.
2. **Education, Safety and Security of Minors:**
   Teachers and others working with students will, in accordance with District guidelines, educate minors on appropriate online behavior, including without limitation interacting with other individuals on social networking Web Sites and chat rooms and cyber-bullying awareness and response and caution students that they should:
   a. Never place personal contact information or a personal photograph on the Internet, e-mail or any on-line communication device. Personal contact information includes full name, address, telephone number, school address, or names of family or friends.

b. Never arrange a face-to-face meeting with someone you meet online.
c. Never open attachments or files from unknown senders.
d. Always report to a teacher any inappropriate sites you observe being accessed by another user or that you access accidentally.

3. **Internet Searches:**
Students should be supervised by instructional personnel when accessing network and internet resources and the following guidelines apply:
   a. **Elementary School**:
   Elementary school students may visit sites a teacher has pre-selected for them. Searches should be completed with child friendly Internet search engines (for instance see: www.nettrekker.com)
   b. **Middle School/High School**:
   Middle school and high school students may visit sites a teacher has pre-selected for them. They may use search engines other than child-friendly search engines when directed to do so by their teacher.
   c. Non-instructional personnel, such as After School Program (ASP) workers, are not permitted to allow students to access technology resources unless it is an instructional activity.
4. **Network Security:**
Maintaining network security is the responsibility of all users. Users should:
   a. Not leave an unsecured workstation without logging out of the network;
   b. Not share or disclose passwords; and
   c. Notify appropriate personnel immediately if a potential security problem is identified.
5. **Acceptable Use Agreement:**
Prior to receiving access to the District's technology resources, employees and students (Form JCDA-3) should complete an Acceptable Use Agreement indicating they accept and agree to the provisions of Administrative Rule IFBG-R (Internet Acceptable Use).
6. **Copyright:**
   a. Students and employees should comply with Administrative Rule GBT-R (Professional Publishing), as well as federal, state or local laws governing copyrighted material.
   b. Students/employees will not:
      (1) Download or upload files to the District's technology that might cause copyright infringement; or
      (2) Install, use, store, distribute or transmit unauthorized copyrighted or trademarked materials on District technology.
7. If students or employees believe that the implementation of this Rule denies access to material that is not prohibited by this Rule, he/she should submit that concern in writing to the school principal or designee or his/her supervisor or designee. The principal, supervisor or designee should report this concern to the appropriate District office within ten (10) school days.

B. E-MAIL:
E-mail accounts are provided to employees for professional purposes (see Administrative Rule ECI-R [Communications System]). Students may access their personal e-mail accounts for educational purposes. Where used in the following guidelines, User/Users refers to both employees and students:

1. Persons outside the District may be able to receive information regarding an employee's communications and use of the network from the District. (see Administrative Rule EF-R [Data Management]).
2. Employees should request permission from the appropriate administrator prior to sending an e-mail message to an entire school staff or District level division.
3. Employee use of e-mail to transmit confidential student information, as defined in Administrative Rule JR-R (Student Records), or sensitive personnel information is prohibited, except where the confidential information is sent in an e-mail directly to a parent/guardian, the subject of the e-mail, or a school official.
4. When an employee sends e-mail that contains confidential information, the employee should refer to the subject of the e-mail by first name only and should include the following disclaimer:

"This e-mail may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any unauthorized dissemination, distribution or copying of any information from this e-mail is strictly prohibited. If you receive this e-mail in error, please notify us immediately by collect telephone call at (telephone number) or electronic mail (e-mail)."

5. The District reserves the right to monitor whatever a User does on the network and to make sure the network functions properly.
6. A User has no privacy as to his/her communications or the uses he/she makes of the Internet.
7. Users should not use e-mail for personal gain or personal business activities.
8. Users will not use e-mail to distribute inappropriate material through pictures, text, forwards, attachments, and other forms of information.
9. Users will not send anonymous e-mail, nor will they harass others through e-mail.

C. PROHIBITED USES

Ethical use of District technology prohibits the following activities by all users:

1. Accessing, sending, creating or posting material or communication that is:
   a. Damaging;
   b. Abusive;
   c. Obscene, lewd, profane, offensive, indecent, sexually explicit, or pornographic;
   d. Threatening or demeaning to another person; or
   e. Contrary to the District's Rules on harassment and/or bullying.
2. Posting anonymous or forging electronic communications.
3. Using the network for financial gain, advertising or political lobbying to include student elections.
4. Engaging in any activity that wastes, monopolizes, or compromises the District/school's technology or other resources.
5. Illegal activity, including but not limited to copying or downloading copyrighted software, music or images, or violations of copyright laws.
6. Using the District network for downloading music or video files or any other files that are not for an educational purpose or, for students, a teacher-directed assignment.
7. Attempting to gain unauthorized access to District/school technology resources whether on or off school property.
8. Using non-educational Internet games, whether individual or multi-user.
9. Participate in any on-line communication that is not for educational purposes or, for students, that is not specifically assigned by a teacher.
10. Using voice over IP, internet telephony, video and/or audio communication devices without teacher supervision.
11. Using District/school technology resources to gain unauthorized access to another computer system whether on or off school property (e.g. "hacking").
12. Attempting to or disrupting District/school technology resources by destroying, altering, or otherwise modifying technology, including but not limited to, files, data, passwords, creating or spreading computer viruses, worms, or Trojan horses; engaging in DOS attacks; or participating in other disruptive activities.
13. Bringing on premises any disk or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.
14. Attempting/threatening to damage, destroy, vandalize, or steal private/school property while using school technology resources.
15. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
16. Using or attempting to use the password or account of another person, utilizing a computer while logged on under another user's account, or any attempt to gain unauthorized access to accounts on the network.
17. Connecting to or installing any personal technology computing device or software without prior approval of the District's Technology Services Division.
18. Attempting to obtain access to restricted sites, servers, files, databases, etc.

19. Exploring the configuration of the computer operating system or network, running programs not on the menu, or attempting to do anything not specifically authorized by District personnel or policies, Rules or regulations.
20. Leaving an unsecured workstation without logging out of the network.

D. DEFINITIONS:

As used in this Rule, the terms and definitions contained in CIPA are expressly incorporated herein by reference and the following additional definitions shall also apply:

"**Chat Rooms**" means a Web site, part of a Web site, or part of an online service, that provides a venue for communities of users with a common interest to communicate in real time.

"Cyber-bullying" means bullying through an electronic medium such as a computer or cell phone.

"**DoS attack**" means a denial-of-service attack designed to overload an electronic network with useless traffic and messages.

"**Educational purposes**" means it relates to curriculum and instruction, research, career or professional development, or administrative purposes.

"**E-mail**" means an electronic message generated using the District's e-mail and/or Web based e-mail. It is also used generically to mean either the District's e-mail system or a Web-based e-mail system.

"**Hacking**" means the illegal activity of breaking into a computer system or electronic network, regardless of intent to cause harm.

"**Inappropriate material**" means material that does not serve an instructional or educational purpose and that includes, but is not limited, to material that:

(i) is profane, vulgar, lewd, obscene, offensive, indecent, sexually explicit, or threatening;
(ii) advocates illegal or dangerous acts;
(iii) causes disruption to Cobb County School District, its employees or students;
(iv) advocates violence; or
(v) contains knowingly false, recklessly false, or defamatory information.

"**Instructional activity**" means a classroom activity that focuses on appropriate and specific learning goals and objectives.

"Social networking" means the use of Web sites or other online technologies to communicate with people and share information, resources, etc.

"**Teacher directed**" means that the teacher gives to the students' specific instructions for activities and assignments.

"**Teacher supervised**" means that a staff member will oversee the activities of the students.

"**Technology**" means but is not limited to electronic media systems such as computers, computing devices, peripheral devices, telecommunication equipment, electronic networks, messaging, and Web site publishing, and the associated hardware and software programs used for purposes such as, but not limited to, developing, retrieving, storing, disseminating, and accessing instructional, educational, and administrative information.

"**Trojan Horse**" means a destructive computer program that enters onto a computer by pretending to be a simple and safe computer application.

"**Users**" means District students, certain employees, including school and Central Office staff, and other authorized persons who use the District's technology.

"**Virus**" means a replicating computer program or piece of code that is loaded onto a computer without the user's knowledge and may attach itself to other computer programs and spread to other computers.

"**Web Page**" means a single document or file on the Web, identified by a unique URL.

"**Web Site**" means a collection of "pages" or files on the Web that are linked together and maintained by a company, organization, or individual.

Adopted: 12/14/00
Revised: 7/26/01
Reclassified an Administrative Rule: 9/1/04
Revised: 5/25/06; 5/14/08; 4/11/12
Revised and re-coded: 9/27/12 (Previously coded as part of Administrative Rule IJNDB)
Revised: 7/1/13

Legal Reference

O.C.G.A. 16-09-0090	Georgia Computer Systems Protection Act
O.C.G.A. 16-09-0091	Computer Related Crime
O.C.G.A. 16-09-0092	Definitions
O.C.G.A. 16-09-0093	Computer crimes defined
O.C.G.A. 16-09-0093.1	Misleading transmittal
O.C.G.A. 16-09-0094	Violations
O.C.G.A. 20-02-0149	Online internet safety education
O.C.G.A. 39-05-0002	Subscriber's control of minor's use of internet
O.C.G.A. 16-11-0037.1	Dissemination of information relating to terroristic acts
20 USC 6777	Internet Safety
47 USC 254(h)	Universal Service
15 USC 6501	Children's Online Privacy Protection Act - Definitions
15 USC 6502	Children's Online Privacy Protection Act - Collection and use of personal information from and about children on the Internet
15 USC 6503	Children's Online Privacy Protection Act - Safe harbors
15 USC 6504	Children's Online Privacy Protection Act - Actions by states
15 USC 6505	Children's Online Privacy Protection Act - Administration and Applicability