IFBGE Internet Safety

3/24/16

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. CIPA COMPLIANCE:

The District will have the following in continuous operation, with respect to all devices that connect to the internet in the District:

1. 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.
2. Procedures, materials and/or guidelines developed by the Teaching and Learning 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:
    a. 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;
    b. Promote the safety and security of minors when using electronic mail, chat rooms, social networking, and other forms of direct electronic communications;
    c. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
    d. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
    e. Restrict minors' access to materials "harmful to minors," as that term is defined in CIPA.
3. 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.

B. EDUCATION, SAFETY AND SECURITY OF MINORS:

Teachers and others working with students will, in accordance with District guidelines and terms of service, 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:

1. 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.

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

C. NETWORK AND INFORMATION SYSTEMS SECURITY:

Maintaining network and information systems 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 incident is identified.

D. ACCEPTABLE USE AGREEMENT:

Prior to receiving access to the District's technology resources, employees, students (Form JCDA-3), and other authorized users should complete an Acceptable Use Agreement indicating they accept and agree to the provisions of Administrative Rule IFBG-R (Technology Acceptable Use).

E. OBJECTIONS:

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.

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; 3/24/16

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