COBB COUNTY SCHOOL DISTRICT

Office of the Superintendent

One Team, One Goal: Student Success

TO: Board Members

FROM: Chris Ragsdale

DATE: February 26, 2016

SUBJECT: Modifications to Administrative Rules for March 9, 2016 Board Work Session

VIA EMAIL

The Superintendent recommends the following revisions to Administrative Rules:

Administrative Rule IFBG-R (Internet Acceptable Use)

In accordance with Administrative Rule CMA-R and Board Policy BD, administrative rules and board policies are to be reviewed on a regular basis. During a review of Section I of the Cobb County Board of Education's policy manual, the Instructional Technology Department has recommended changes regarding Administrative Rule IFGB-R.

On behalf of the Instructional Technology Department, Policy, Planning and Student Support recommends the following changes to Administrative Rule IFBG-R:

1. Addition of clarifying language in the Rational/Objective section
2. Addition of language regarding authorized users
3. Addition of language relocated from Board Policy IFBGE

Gregory, Doyle, Calhoun & Rogers has reviewed all suggested changes and concurs with Administration.

Administration is providing this information in compliance with Board of Education Policy BDF (Review of Administrative Rules), which reads:

> *"The proposed Rule(s) shall be sent to the Board for their review in advance of issuance. Specifically, their review shall include at least the ten (10) days immediately prior to the next Board Work Session. If no objection is indicated by Board member(s) to the Chair prior to the adjournment of the Board Work Session, the Rule(s) shall be deemed accepted."*

GREEN font indicates content recommended by Technology Services
BROWN font indicates conforming/editorial changes
BLUE font indicates additional content recommended by Technology Services (Coordination Record)
ORANGE font indicates content recommended by Gregory, Doyle, Calhoun & Rogers

COBB COUNTY SCHOOL DISTRICT

DISTRICT ADMINISTRATIVE RULE

IFBG-R ~~Internet~~ Technology Acceptable Use

~~7/24/13~~ **?/?/16**

RATIONALE/OBJECTIVE:

The Cobb County School District (District) believes that technology and its utilization enhances the quality and delivery of education and is an important part of preparing children for life in the 21st century. The community of technology users must understand that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable educational tool, there are sections that are not commensurate with community, school, or family standards. The District believes that the Internet's advantages far outweigh its disadvantages and will provide an Internet filtering device which shall be used to block or filter access to inappropriate information and material on the Internet, in electronic mail or other forms of electronic communications. It should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

Additionally, the District considers access to the Internet and **technology** ~~computer~~ resources a privilege, not a right. Therefore, users violating Board of Education Policies or District Administrative Rules may be subject to revocation of these privileges, potential disciplinary action, **and possible referral to any appropriate authority, including law enforcement**. **Users should have no expectation of privacy regarding their use of District technology, and the superintendent or designee may record or monitor User's use of District technology.**

RULE:

A. AUTHORITY:

1. **The District:**
   The District provides its students and authorized employees with access to and use of its technology consistent with the District's vision and strategic goals. Therefore, the District reserves the right to monitor, access, and disclose the contents of any user's files, activities, or communications to any appropriate authority, including law enforcement.
2. **Employees:**
   Principals and Administrators will endeavor to inform students, employees**, guests, and other authorized users** of the responsibilities associated with use of the District's technology. To this end, Administrative Rule IFBG-R (~~Internet~~ **Technology** Acceptable Use) and Board of Education Policy IFBGE (Internet Safety) are included in the Parent Information Guide. Any attempts to harm, modify, destroy or otherwise change the District's data and technology should be reported to appropriate District authorities. Staff will refer to District Administrative Rules governing employee and student conduct, including, Administrative Rules JCDA-R (Elementary), JCDA-R (Middle), JCDA-R (High), when addressing inappropriate use or abuse of District technology privileges.
3. **Students, guests, and other authorized users**
   Students**, guests, and other authorized users** will adhere to all policies, Rules and regulations issued by the District and their respective school.

B. 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.**

C. ~~B.~~ PENALITIES FOR PROHIBITED USE:

Students**,** ~~and~~ employees, **guests, or other authorized users** who violate District/school policies, Rules or regulations governing the use of the District's technology and network resources may have their network privileges suspended or revoked. **Users** ~~and~~ will **also** be subject to District Administrative Rules that apply to employee and student conduct **(including but not limited to Administrative Rules JCDA-R and GBK-R)** ~~including, for students, the provisions of the appropriate Student Code of Conduct (Administrative Rules JCDA-R [Elementary], JCDA-R [Middle], JCDA-R [High])~~. **The District may also refer incidents to law enforcement or other authorities as appropriate.**

D. GENERAL INTERNET ACCESS:

The District's network and internet access is provided solely for instructional use and District business.

1. **Students should be supervised by instructional personnel when accessing network and internet resources and the following guidelines apply:**
   a. **Students using district technology should access only those websites and applications that are educationally relevant to the curriculum as directed by a teacher.**
   b. **Students authorized by their school to connect personal devices to the District's BYOD ('Bring Your Own Device') network should access only educational websites and applications that are educationally relevant to the curriculum as directed by a 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**
2. **Employees, guests, and other authorized users (not students) are permitted some limited, incidental use of internet resources for personal use. Such personal use must not:**
   a. **Interfere with any District operation or activity,**
   b. **Be for a personal business or personal monetary gain,**
   c. **Cause any harm or embarrassment to the District, our schools, our students or our employees,**
   d. **Be for any unethical purposes or illegal activity, or**
   e. **Negatively affect the District's mission or any employee's effectiveness or ability to perform his/her duties and responsibilities.**
3. **The District reserves the right to monitor whatever a User does on the network and to make sure the network functions properly.**
4. **A User has no privacy as to his/her communications or the uses he/she makes of the network or internet.**

E. COPYRIGHT:

1. **Students and employees should comply with Administrative Rule GBT-R (Professional Publishing), as well as federal, state or local laws governing copyrighted material.**
2. **Students and employees will not:**
   a. **Download or upload files to the District's technology that might cause copyright infringement; or**
   b. **Install, use, store, distribute or transmit unauthorized copyrighted or trademarked materials on District technology.**

F. ~~C.~~ WEB SITE PUBLISHING:

1. Publication of student information, work and pictures is governed by Administrative Rule JG(1)-R (Monitoring-Recording Staff and Students).
2. Web pages or blogs hosted on or linked from Cobb County School District's Web server will not:
   a. Include any information that indicates the physical location of a student at a given time, other than attendance at a particular school or participation in school activities where appropriate consent has been received.
   b. Display personal information, work samples, photographs, videos, streaming video, or audio clips of any identifiable student without a prior written permission slip (Form JG(1)-1 [Permission to Display Student Photograph/Name/Work Sample]) if a parent/guardian has "opted out" of the release of directory information as stated in the Directory Information Statement in the Parent Information Guide.
3. Students may retain the copyright on the material they create that is subsequently displayed or performed on the District's Web site or individual school Web pages or blogs.

G. ~~D.~~ EMPLOYEE CREATED WEB PAGES AND/OR BLOGS:

The District assumes no responsibility for schools or individual employees who do not comply with the following provisions:

1. Employees may create or link to individual Web pages and/or blogs on an external site provided these external sites meet the District's definition of "educational purposes" as stated in Section ~~J~~ **K** below. Any links to external sites that fail to meet that definition will be removed.
2. Each employee will be responsible for maintaining his/her Web pages or blogs in cooperation with the school Web Publisher. Specifically, all material originating from the employee and placed on the employee Web pages/blogs will be consistent with the Web Page Publishing and Compliance Guidelines and approved through the compliance process established by the District Web Publisher (Web Master).
3. The District Web site and individual employee Web pages/blogs will not:
   a. Contain public message boards or chat-room areas. However, employees may allow two-way communication on blogs or private message boards as a part of the classroom curriculum as long as the employee previews (moderates) and approves all blog comments before they are posted on the Internet.
   b. Allow the display of unsolicited comments from the general public. Any solicited public feedback should be reviewed by the employee before posting. Any questionable or inappropriate content will immediately be removed by the employee, the School Web Publisher or by the District Web Publisher (Web Master) with no notification.

H. 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 employees, students, and other authorized users:

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 message is intended only for the use of the individual or entity to which it is addressed and 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 dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and/or 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.

I. THIRD PARTY SERVICES:

Access to third party applications or services hosted by an external entity ('hosted services') may be provided to users under the following guidelines:

1. The District will not be responsible for any actions of users utilizing hosted services.
2. Use of hosted services will be subject to all applicable laws, including but not limited to: CIPA, COPPA, and FERPA, along with the District's Administrative Rules and Policies, including but not limited to IFBG-R, IFBGE, JR, and JR-R.
3. The District reserves the right to monitor whatever a User does on hosted services and to make sure the hosted services function properly whether on or off site.
4. A User has no privacy as to his/her communications or the uses he/she makes of the District provided hosted services whether utilized on or off site.
5. A user must be eligible and comply with the terms of service.

J. 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. **Disclosing or failing to secure account password(s)**
18. **Connecting to or installing any personal technology computing device or software without prior approval of the District's Technology Services Division.**
19. **Attempting to obtain access to restricted sites, servers, files, databases, etc.**
20. **Exploring the configuration of the computer operating system or network, running programs or applications not approved for use ~~not on the menu~~, or attempting to do anything not specifically authorized by District personnel or policies, Rules or regulations.**
21. **Leaving an unsecured workstation without logging out of the network.**
22. **Executing or installing software or applications not approved by the District's Technology Services Division.**
23. **Failing to notify appropriate District personnel of potential security incidents.**

K. 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:

"**Blogs**" (short for Web Logs) means dynamic web sites consisting of regularly updated entries displayed in reverse chronological order. They read like a diary or journal, but with the most recent entry at the top. Blogs can allow for open comments meaning other individuals can respond to a posted entry. Open comments is an optional feature for most blog Web sites.

"**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.

"**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.

"**External site**" means Web sites and materials not hosted on the District's Web server.

"**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.

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

"**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 Administrative Rule IJNDB)
Conforming Changes: 5/31/13
Revised: 7/24/13**; ?/?/16**

Legal Reference

O.C.G.A. 16-9-90	Georgia Computer Systems Protection Act
O.C.G.A. 16-9-91	Computer Related Crime
O.C.G.A. 16-9-92	Definitions
O.C.G.A. 16-9-93	Computer crimes defined
O.C.G.A. 16-9-93.1	Misleading transmittal
O.C.G.A. 16-9-94	Violations
O.C.G.A. 20-2-149	Online internet safety education
O.C.G.A. 39-5-2	Subscriber's control of minor's use of internet
O.C.G.A. 16-11-37.1	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