Board Policy IFBG: Internet Acceptable Use

Status: PROPOSED

Original Adopted Date: 01/01/1900 **| Last Revised Date:** 07/11/2011 **| Last Reviewed Date:** 07/11/2011

The DeKalb County School District provides technologies, networks, and Internet access to support the educational mission of the District and to enhance the curriculum and learning opportunities for students and District employees. In an ever-changing world, the District is committed to protecting its students, employees, partners, and its information technology infrastructure from intentional or unintentional harm arising from internet use and emerging technology.

Applicable Definitions

1. Users**:** all individuals, including students, employees, administrators, contractors, parents, visitors, etc. who use, connect to, or access the District's technology or digital infrastructure.
2. Emergent and or emerging technology: includes artificial intelligence engines, chatbots, automated decision-making software, and any other technology that might come into being and could impact the District's Network and equipment.

These technology resources may be used only in support of education and research and consistent with the educational objectives of the District.

All guidelines set forth in this policy and any relevant regulations or rules are applicable to all telecommunication services, equipment, and activity on equipment provided by the District including, but not limited to, the following:

1. Computer workstations and notebook computers;
2. Smart phones, tablets, e-readers, and other devices within the Internet of Things (IoT);
3. Internet services;
4. Wi-Fi Networks
5. Telephone services; and
6. Cellular telephone services.
7. District Networks, Local Area Networks;
8. Electronic messages or transmissions via internet, Bluetooth, Near Field Communication (NFC), Radio-frequency identification (RFID), etc.; and
9. emerging technologies.

Acceptable use agreements must be signed by all users of District technologies or networks.

I. **INTERNET SAFETY**

A. The Superintendent shall, with respect to any computer or other technology connecting to the District network and having access to the Internet:

1. Ensure that a qualifying "technology protection measure," as that term is defined in section 1703(b)(1) of the Children's Internet Protection Act of 2000 ("CIPA"), is installed and in continuous operation;

2. Ensure that minors are educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and about cyber bullying awareness and response, as required by CIPA and as set forth in Board Policy JCDAG; and

3. Implement, maintain, and enforce procedures or guidelines that provide for monitoring of the online activities of users and of the use of "technology protection measures" to prevent access to visual depictions that are (i) "obscene," (ii) "child pornography," or (iii) "harmful to minors," as those terms are defined in section 1721(c) of CIPA.

4. Ensure that sufficient information, cyber, and network security measures are in place to protect the integrity of the network; to safeguard employee and "student data" as that term is defined in Section 12 of the Georgia Student Data Privacy, Accessibility, and Transparency Act (O.C.G.A. §20-2-661-20-2-667).

5. Ensure that minors, students, and employees are educated about appropriate use of emergent technology, the ethics of emergent technology usage, fallacies associated with the technology, and information security risks posed by emergent technology usage on District devices, networks, and credentials.

B. The Superintendent shall, with respect to access to the Internet by or through computers, networks or other devices belonging to the District network, implement, maintain and enforce procedures or guidelines that

1. Provide for monitoring the online activities of users to limit, to the extent reasonably feasible, access by minors to inappropriate matter on the Internet, and other unauthorized activities by minors online; and

2. Are designed to promote the safety and security of minors when using electronic mail, social media, emerging technology, and other forms of direct electronic communications;

3. Are designed to prevent unauthorized access, intentional or unintentional, including so-called "hacking," by employees, students, or other threat actors;
4. Are designed to prevent the unauthorized disclosure, use, and dissemination of personal identification information regarding minors;

5. Are designed to restrict minors' access to materials "harmful to minors," as that term is defined in section 1721(c) of CIPA; and

6. Establish consequences for students and employees who willfully or inadvertently violate acceptable-use procedures.

II. **EMPLOYEE USE OF TECHNOLOGY**

District employees are to utilize the District's technologies, networks, and Internet services only for District-related purposes and performance of job duties. In the event an emerging technology is deemed appropriate for District employee use, such use must comply with the District's policies, information security protocols, and applicable laws. Incidental personal use of District technologies, meaning use by an individual employee for occasional personal communications, is permitted only if such use does not interfere with the employee's job duties and performance, with

District operations, or with other District users. Employees are reminded that such incidental personal use must comply with this policy and all other applicable policies, regulations, procedures, and rules. Each employee is responsible for his or her actions and activities involving District technologies, networks, and Internet services, and for his or her computer files, passwords, and accounts. Examples of prohibited unacceptable uses include, but are not limited to, the following:

1. Any use that is illegal or in violation of other Board of Education policies, including, for example, harassing, discriminatory, or threatening communications and behavior, or violations of copyright laws;

2. Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive;

3. Any inappropriate communications with students or minors;

4. Any use for private financial gain or for commercial advertising or solicitation purposes;

5. Any use as a forum for communicating by e-mail or other medium with other District users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-District sponsored organization; to solicit membership in or support of any non-District sponsored organization; or to raise funds for any non-District sponsored purpose, whether for-profit or non-profit. No employee shall knowingly provide District e-mail addresses to outside parties whose intent is to communicate with District employees, students, or their families for non-District or non-school related purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from their immediate supervisor;

6. Any communication that represents an individual's personal views as those of the District or any school unit or that could be misinterpreted as such;

7. Downloading or loading software or applications without permission of the Department of Management Information Systems;

8. Opening and forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses;

9. Sending or facilitating mass e-mails to school users or outside parties for any purpose, unless prior permission has been granted;

10. Any malicious use or disruption of the District technologies, networks, and Internet services or breach of security features;

11. Any misuse or damage to District technology arising from any direct or indirect action, including unauthorized use of an emergent technology;

12. Misuse of computer passwords or accounts, including providing personal passwords to non-District personnel;

13. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;

14. Any attempt to access unauthorized websites;

15. Any use of emergent technology in a manner counter to the District's Policies;

16. Using District technologies, networks, or Internet services after such access has been denied, revoked or suspended; or

17. Any attempt to modify, delete, erase, or otherwise conceal any information stored on District technologies or networks that violates this policy.

District employees should report all known breaches of technology use or security to the Chief Information Officer and Director of Information and Network Security.

The District retains control, custody, and supervision of all technologies, networks, and Internet services owned or leased by the District. The District reserves the right to monitor all technology and Internet activity by all system users. Users have no expectation of privacy in their use of school technologies or networks, including e-mail messages and stored files. Employees are expected to use appropriate judgment and caution in communications concerning students and employees, as well as interactions with emergent technology, to ensure that personally identifiable information remains confidential.

Teachers, staff members, and volunteers who utilize school technology for instructional purposes with students have a duty of care to supervise such use. Teachers, staff, and volunteers are expected to be familiar with the District's policies and rules concerning student computer and Internet use and to enforce them. When, in the course of their duties, employees and volunteers become aware of student violations, they are expected to stop the activity and inform the building principal or other appropriate administrator.

Employees shall be responsible for any losses, costs, or damages incurred by the District related to violations of this policy and other rules, regulations, or applicable laws.

The District assumes no responsibility for any unauthorized charges made by employees, including but not limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers or other technologies.

Policy Reference Disclaimer:
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.

Note: ***To access the policy references, CLICK HERE:*** **State of Georgia Terms and Conditions** ***and close the LexisNexis tab, which will return you to the policy. Click on the links below to be taken to each specific code. You should only have to do this one time per session.***

State	Description
O.C.G.A. 10-01-0912	Notification required upon breach of security regarding personal information
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	Computer Crimes: 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. 16-09-0122	Attempting or conspiring to attempt identity fraud
O.C.G.A. 16-11-0037.1	Dissemination of information relating to terroristic acts
O.C.G.A. 16-12-0100.1	Electronically furnishing obscene material to minors
O.C.G.A. 16-12-0100.2	Computer or electronic pornography and child exploitation prevention
O.C.G.A. 20-02-0324	Internet safety policies in public schools
O.C.G.A. 20-02-0666	Activities by operators; limitations
O.C.G.A. 20-02-0660	Georgia Student Data Privacy, Accessibility, and Transparency Act
O.C.G.A. 20-02-0662	Georgia Student Data Privacy, Accessibility, and Transparency Act - Definitions
O.C.G.A. 39-05-0002	Subscriber's control of minor's use of internet
O.C.G.A. 39-05-0003	Immunity
O.C.G.A. 39-05-0004	Internet safety report of certain information

Federal	**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 info from and about children
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