Board Policy IFBG: Internet Acceptable Use **Status:** DRAFT

Original Adopted Date: 01/01/1900 **| Last Revised Date:** 07/11/2011 **| Last Reviewed Date:** 09/17/2025

REDLINE VERSION

I. Purpose

The DeKalb County School District ("DCSD" or "District") provides ~~technologies, networks, and Internet~~technology resources, including internet access, to support the district's educational mission ~~of the District~~ and ~~to~~ enhance ~~the curriculum and~~ teaching, learning ~~opportunities for~~ , and operational efficiency. The district is committed to safeguarding its students ~~and District~~, employees~~. These~~, partners, and technology infrastructure. Employees and students uncertain about appropriate technology use must seek clarification from their supervisor, teacher, or school administrator.

II. Definitions

A. **Artificial Intelligence (AI):** Includes generative artificial intelligence, automated decision-making software (ADMS), and large language models (LLMs) capable of generating original content with minimal human input (e.g., ChatGPT, DALL·E, Microsoft Copilot, Gemini).

B. **Emergent Technology:** Includes AI engines, chatbots, ADMS, or other technologies that may impact the district's network, equipment, or data.

C. **School Equipment:** Any computer, network, or communication system owned, leased, or provided by the district for instructional or administrative use.

D. **Social Media:** Internet-based platforms that facilitate communication, collaboration, or user-generated content (e.g., X/Twitter, Facebook, Instagram, TikTok, LinkedIn, YouTube).

E. **Student Data:** Personally identifiable information, including names, addresses, identification numbers, contact information, or other data protected by law.

F. **Threat Actors:** Unauthorized individuals or entities with malicious intent, including but not limited to governments, criminals, or hackers.

G. **Users:** Any individual who accesses or uses district technology or digital infrastructure.

III. General Use

A. District technology resources ~~may~~will be used only ~~in support of education and~~ for educational, research, and official district purposes consistent with the ~~educational objectives of the District~~district's mission and goals.

B. All ~~guidelines set forth in~~ users must sign an Acceptable Use Agreement acknowledging understanding of this policy and ~~any relevant~~its

accompanying regulations ~~or rules are applicable to all telecommunication services and 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 mobile devices;~~

~~3.~~**IV. Internet** ~~services;~~**Safety**

~~4. Telephone services; and~~

~~5. Cellular telephone services.~~

~~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~~or designee will:

Implement and maintain 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;~~

A. ~~Ensure~~protection measures to block or filter internet content that is obscene, pornographic, or harmful to minors ~~are educated about~~, as required by law and Board Policy JCDAG.

~~2.~~**B.** Provide instruction on 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~~room interaction, and cyberbullying prevention, consistent with CIPA and ~~as set forth in~~ Board Policy JCDAG~~; and~~.

~~3. Implement, maintain,~~Develop and enforce ~~procedures or guidelines that provide for monitoring of the online activities of users and of the use of "technology protection measures"~~regulations 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.~~

~~B. The Superintendent shall, with respect to access to the Internet by or through computers, networks or other devices belonging to the District~~monitor 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;~~

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

~~3.~~**C.** ~~Are designed to~~ use, prevent unauthorized access, ~~including so-called "hacking," and other unauthorized activities by minors online;~~and ensure data security.

D. ~~Are designed to prevent the unauthorized disclosure,~~Implement technical and administrative safeguards to protect the integrity of district networks and user data.

~~4.~~**E.** Educate students, employees, and contractors on emergent technologies, ethical use, and ~~dissemination of personal identification~~ information ~~regarding minors;~~security risks.

~~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.~~**F.** Establish disciplinary consequences for ~~students and employees who willfully violate acceptable-use procedures~~violations of this policy and supporting regulations.

~~II. EMPLOYEE USE OF TECHNOLOGY~~

~~District employees are to utilize the District's technologies, networks, and Internet services only for Districtrelated purposes and performance of job duties. 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~~

V. Employee Use of Technology

A. Employees will use district technology resources primarily for job-related duties.

B. Limited incidental personal use is permitted only if it does not interfere with job performance, district operations, or legal and ethical obligations.

C. Employees are responsible for the proper use, security, and confidentiality of their accounts, passwords, and files.

All suspected security breaches or misuse shall be reported immediately to the Chief 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 ofsecurity features;~~

~~11. Any misuse or damage to District 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. Using District technologies, networks, or Internet services after such access has been denied, revoked or suspended; or~~

~~16. Any attempt to modify, delete, erase, or otherwise conceal any information stored on District technologies or networks that violates this policy.~~

D. ~~District employees should report all known breaches of technology use or security to the Executive~~ Officer and the Director for ~~Management~~ Information ~~Systems or the Office of Internal Affairs~~and Network Security.

E. The ~~District~~district retains ownership, control, ~~custody,~~ and ~~supervision of all technologies, networks, and Internet services owned or leased by the District. The District reserves the right to monitor~~ supervisory rights over all technology ~~and Internet activity by all system users.~~ resources and may monitor usage at any time. Users have no expectation of privacy in their use of ~~school technologies or networks~~district technology, including ~~e-mail messages~~email and stored files.

F. Employees ~~are expected to use appropriate~~must exercise sound judgment ~~and caution in communications concerning students and employees to~~ when using technology and ensure ~~that~~ the confidentiality of student and staff personally identifiable information ~~remains confidential~~.

G. Teachers, staff ~~members~~, and volunteers ~~who utilize school~~ supervising student technology ~~for instructional purposes~~use will ensure compliance with ~~students have a duty of care to supervise such use. Teachers, staff,~~this policy 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~~promptly report violations~~, they are expected to stop the activity and inform the building~~ to the principal or ~~other~~ appropriate administrator.

H. Employees ~~shall~~may be held financially responsible for ~~any~~ losses~~, costs,~~ or damages ~~incurred by the District related to violations of this policy and other rules or regulations~~resulting from misuse.

VI. ~~The District assumes no responsibility~~Student Use of Technology

A. Students will use district technology for ~~any unauthorized charges made by employees~~educational purposes during designated instructional hours and under appropriate supervision.

B. Students may not use technology to engage in conduct that violates the Student Code of Conduct, including but not limited to ~~credit card charges, subscriptions, long distance telephone charges, equipment and line costs~~plagiarism, cheating, harassment, or bullying.

C. Students must comply with all provisions of this policy and related regulations.

VII. Authority and Responsibility

The superintendent or designee will:

A. Develop administrative regulations to implement this policy.

B. Ensure ongoing monitoring and evaluation of district technology use and internet safety measures.

C. Provide regular training for ~~any illegal use of its computers or other technologies~~staff and students on responsible technology use and emerging risks.

VIII. References

- Children's Internet Protection Act (CIPA)
- Board Policy JCDAG – Internet Safety and Cyberbullying
- Board Policy IFBG(R) – Acceptable Use Regulation
- Family Educational Rights and Privacy Act (FERPA)