Board Policy IFBG: Internet Acceptable Use **Status:** DRAFT - 1st Reading

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

CLEAN VERSION

The DeKalb County School District provides technology resources, including internet access, to support the educational mission of the district and 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 technology infrastructure from harm. Employees who are uncertain whether particular activities are acceptable must seek further guidance from their immediate supervisor. Students who are uncertain whether activities are acceptable must seek further guidance from their teacher or school administrator.

Applicable definitions:

1. Artificial Intelligence: Artificial intelligence (AI) encompasses generative artificial intelligence (Gen AI), automated decision-making software (ADMS), and large-language models (LLMs). Generative Artificial Intelligence (AI) refers to computer systems that are capable of generating creative or original content, such as written or visual materials, with minimal human input. Examples include, but are not limited to, ChatGPT, DALL-E, Microsoft Copilot, and Gemini.
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.
3. School equipment: any computer or computer networking equipment, technology or technology related device or service, or communication system or service that is operated, owned, leased, and made available to students by a local board of education, local school system, or public school and that is used for transmitting, receiving, accessing, viewing, hearing, downloading, recording, or storing electronic communication.
4. Social Media: means any internet-based technology or website that facilitates or promotes interactive communication, participation, collaboration, or the submission of user-generated content. Examples of Social Media include, but are not limited to: blogs, wikis, microblogging sites, such as Twitter™/ X; social networking sites, such as Facebook™, Instagram™, SnapChat™, TikTok™, and LinkedIn™; video sharing sites, such as YouTube™; and the interactive tools and functions they provide to users.
5. Student data: students' names, addresses, social security numbers or other identifying numbers, telephone numbers, email addresses, and other personally identifiable information.
6. Threat actors: any unauthorized party with malicious intent. These include, but are not limited to national governments, terrorists, organized crime groups, hacktivists, and hackers.

7. Users: all individuals who connect to or access the district's technology or digital infrastructure.

Technology resources must only be used in support of education and research and be consistent with the educational objectives of the district. This policy, regulations and guidelines apply to all technology resources. All district technology users must sign agreements acknowledging allowable and acceptable use of district technology.

I. INTERNET SAFETY

With respect to any computer or other technology with internet connectivity, the superintendent or the superintendent's designee will:

1. Install and operate “technology protection measures,” to block or filter internet "obscene", "pornography", or content that is harmful to minors as defined in law and Board Policy JCDAG which is available on the district website at https://shorturl.at/zpi8U.

2. Educate users about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, and about cyberbullying awareness and response, as required by CIPA and as set forth in Board Policy JCDAG which is available on the district website at https://shorturl.at/zpi8U.

3. Create and enforce supporting regulations to monitor users’ online activities, “technology protection measures,” and to prevent unauthorized access.

4. Implement sufficient technology security measures to protect the integrity of networks; and to safeguard employee, contractor, and student data.

5. Educate minors, students, employees, and contractors about:
    I. Emergent technology
    II. Ethical concerns about emergent technology (for example plagiarism, bullying, etc.)
    III. Information security risks associated with emergent technology use on district technology resources and credentials.
6. Establish consequences for students and employees who violate this policy and supporting regulations.

II. EMPLOYEE USE OF TECHNOLOGY

District employees will only use the district’s technology resources for district-related 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, the district's operations, other district users, the law, or the district's ethical obligations. Employees are responsible for their own actions and activities involving district technologies, and for their computer files, passwords, and accounts. IFBG (R)(1) discusses specific employee uses.

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

The district retains control, custody, and supervision of all technology resources owned or leased by the district. The district reserves the right to monitor all technology and internet activity of 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 student and staff 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. If, 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 may be held responsible for any losses, costs, or damages incurred by the district related to violations of this policy and other rules, regulations, or applicable laws.

III. STUDENT TECHNOLOGY USE

Students are expected to use district technology for educational purposes during hours as defined by the student's teacher and under appropriate adult supervision. Students may not use technology at any time to violate the code of conduct including, but not limited to plagiarism, cheating, harassment or bullying. Students are required to comply with the general guidelines and restrictions applied to all users.