Board Policy IFBG: Internet Acceptable Use

Status: DRAFT

Original Adopted Date: 01/01/1900 **| Last Revised Date:** 07/11/2011 **| Last Reviewed Date:** 09/24/2025

REDLINE VERSION

The DeKalb County School District provides ~~technologies, networks, and Internet~~ technology resources, including internet access to support the educational mission of the district ~~District~~ and ~~to~~ enhance the curriculum and learning opportunities for students and district ~~District~~ employees. ~~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 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. ~~Internet services;~~
4. ~~Telephone services; and~~
5. ~~Cellular telephone services.~~

~~Acceptable use agreements must be signed by all users of District technologies or networks.~~
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:Bullying. JCDAG: Bullying
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: Bullying. JCDAG: Bullying
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.

I. ~~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;
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. Are designed to prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
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 violate acceptable-use procedures.

II. 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.

III. **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. 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;
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.~~

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

~~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 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 or regulations.~~

~~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.~~
