

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

I. Purpose

The DeKalb County School District (“DCSD” or “District”) provides technology resources, including internet access, to support the district’s educational mission and enhance teaching, learning, and operational efficiency. The district is committed to safeguarding its students, employees, 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 will be used only for educational, research, and official district purposes consistent with the district’s mission and goals.
- B.** All users must sign an Acceptable Use Agreement acknowledging understanding of this policy and its accompanying regulations.

IV. Internet Safety

The Superintendent or designee will:

- A.** Implement and maintain technology protection measures to block or filter internet content that is obscene, pornographic, or harmful to minors, as required by law and Board Policy JCDAG.
- B.** Provide instruction on appropriate online behavior, including social networking, chat room interaction, and cyberbullying prevention, consistent with CIPA and Board Policy JCDAG.

- C. Develop and enforce regulations to monitor network use, prevent unauthorized access, and ensure data security.
- D. Implement technical and administrative safeguards to protect the integrity of district networks and user data.
- E. Educate students, employees, and contractors on emergent technologies, ethical use, and information security risks.
- F. Establish disciplinary consequences for violations of this policy and supporting regulations.

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.
- D. All suspected security breaches or misuse shall be reported immediately to the Chief Information Officer and the Director for Information and Network Security.
- E. The district retains ownership, control, and supervisory rights over all technology resources and may monitor usage at any time. Users have no expectation of privacy in their use of district technology, including email and stored files.
- F. Employees must exercise sound judgment when using technology and ensure the confidentiality of student and staff personally identifiable information.
- G. Teachers, staff, and volunteers supervising student technology use will ensure compliance with this policy and promptly report violations to the principal or appropriate administrator.
- H. Employees may be held financially responsible for losses or damages resulting from misuse.

VI. Student Use of Technology

- A. Students will use district technology for 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 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 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)