Jefferson County School System

Dr. Samuel D. Dasher, Jr., Superintendent

1001 Peachtree Street
Louisville, GA 30434
Telephone 478/625-7626
Fax 478/625-7459
E-Mail: dashers@jefferson.k12.ga.us

Board of Education
James E. Fleming, Jr. Chairman

Members
Teresa Brooks
Barbara Jordan
Steve Norton
Julia Well

Internet Acceptable Use

It is the belief of the Jefferson County School System that the use of telecommunications, including the Internet, in instructional programs is an educational strategy that facilitates communication, innovation, resource sharing, and access to information. Use of the Internet must be in support of education and research and consistent with the educational mission, goals, and objectives of the school system.

It shall be the policy of the Board of Education that the school system shall be compliant with the "Protecting Georgia's Children on Social Media Act of 2024" (The Act) and have in continuous operation, with respect to any computers belonging to the school having access to the Internet:

1. 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) and is compliant with The Act; and

2. Procedures or guidelines developed by the Superintendent and his/her designee(s), including administrators and/or other appropriate personnel, which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are
    i. obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are define in CIPA and The Act. Such procedures or guidelines shall be designed to:
    ii. Provide reasonable opportunities and procedures for parents/guardians of students to confer and collaborate with school administrators and teachers regarding appropriate internet access for such students;
    iii. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;
    iv. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
    v. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
    vi. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
    vii. Restrict minors' access to materials "harmful to minors," as that term is defined in CIPA and The Act.
    viii. Provide for students age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services, behaviors that may constitute cyber bullying, and how to respond when subjected to cyber bullying.
    ix. Establish appropriate enforcement measures in response to:
        1. Students against students and school employees who willfully intentionally violate the acceptable-use policy, whether or not such student or school employee was, at the time of such violation, on school property, on a school bus or other school vehicle, at a school-related function, or elsewhere, provided that such measures include disciplinary measures; and
        2. A person who is not a student or school employee who violates the acceptable-use policy, whether or not such person was, at the time of such violation, on school property, on a school bus or other school vehicle, at a school related function, or elsewhere;
    x. Provide for administrative procedures to: enforce the acceptable-use policy; for administrative procedures to address complaints regarding possible violations of the acceptable-use policy which, at a minimum, require that each complaint is responded to in writing by an appropriate school or local school system official; and provide for expedited review and resolution of a claim that the application of the acceptable-use policy is denying a student or school employee access to material that is not within the prohibition prohibitions of the acceptable-use policy.

3. Ensure that no Personally Identifiable Information (PII), sensitive personal data, or confidential information is entered, uploaded, processed, or included in any AI prompts, inputs, outputs, or generated content. All information must be anonymized or de-identified before use. Do not include names, addresses, phone numbers, email addresses, Social Security numbers, account numbers, or any other information that could directly or indirectly identify an individual. If PII is detected, stop processing and remove or redact the information before proceeding. Always follow applicable data privacy policies, security requirements, and organizational guidelines.