**ICSS ACCEPTABLE USE POLICY**

**I) Introduction**

The Irwin County School District believes that using computer resources should be an enjoyable and educational experience. Therefore, the school district provides computing facilities to faculty, students, and staff for educational activities. This policy mandates responsible behavior by individuals given access to these facilities and recognizes the district's responsibility to promote the safety and security of these users.

Since the Internet opens up the world to unrestricted access, the district cannot assume the responsibility for monitoring every document to which a user may gain access. Therefore, the district is not to be held accountable for what the user may access through the Internet beyond instructional directives.

To the extent practical, the Irwin County School District shall take steps to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

*In order for students to use the available technology and access the Internet, parents must read this policy with their child(ren) and indicate acceptance of the policy by their signature on the Internet Usage Permission Form. Students in grades four through twelve must also sign the permission form.*

**II) Definitions**

A. Computing resources include computers, as well as peripherals, networks, software, data, labs, computer-related supplies and the Internet
B. Technology Protection Measure means a specific technology that blocks or filters Internet access to visual depictions that are: (1) Obscene, as that term is defined in section 1460 of title 18, United States Code; (2) Child pornography, as that term is defined in section 2256 of title 18, United States Code; or (3) Harmful to minors.
C. Harmful to Minors means any picture, image, graphic image file, or other visual depiction that: (1) Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (2) Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (3) Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
D. Sexual Act and Sexual Contact have the meanings given in section 2246 of title 18, United States Code.

**III) General Policies Regarding Use of Technology**

A. The use of technology and access to the Internet is a privilege, not a right. Inappropriate use will result in a cancellation of those privileges. In addition to the following guidelines, the administration will deem what constitutes inappropriate use.
B. Intentional abuse of computing resources, intentional interference with the operation of computing resources or wasting of computer resources is prohibited. This includes, but is not limited to, the uploading or creation of computer viruses.
C. Intentional interference with or destruction of the work of other users is prohibited.
D. Users shall not violate confidentiality, copyrights, or license agreements.
E. Actions that attempt to circumvent prescribed channels of obtaining computer privileges and resources are prohibited.
F. Changing wiring, connections, or placement of computing resources is prohibited.
G. Modifying any system configuration, startup files, or applications without the explicit permission of the lab supervisor, teacher, media specialist or technologist is prohibited.
H. Reporting improperly working equipment or software is highly encouraged so that computing resources can be better maintained for efficient availability.
I. Using computing resources for commercial purposes is prohibited.
J. A user may not use or download any software to school computers without permission of the school's technologist.
K. All external storage devices (CDs, floppies, etc.) brought to the lab or library to be used in the computers must first be scanned for viruses by the teacher/librarian.
L. Under no circumstances shall students, employees of the school system, or any individual exhibit or disseminate obscene/offensive materials on school property by computers or any other means.
M. Under no circumstances shall students, employees of the school system, or any individual communicate by way of threatening material in a manner that could be construed as cyberbullying or directly threatening bodily harm and/or illegal activity.

**IV) Terms and Conditions for Use of Internet**

A. Internet access has been made available to students and staff. This access offers vast, diverse, and unique resources to both students and staff. The goal of providing this service is to promote educational excellence by facilitating resource sharing, production, innovation, and communication.
B. Internet users are personally responsible for their use of the Internet. These guidelines are provided so that users are aware of these responsibilities.
C. All students must have an Internet Usage Permission Form, signed by their parents, that authorizes them access to the Internet.

D. Students are to notify the teacher/librarian immediately of any security problem or inappropriate material they may encounter on the web or in e-mail. Inappropriate material should not be demonstrated to other users.
E. Students are not to give out their own or others' personal information like telephone numbers, full names, addresses, etc. to anyone on the Internet.
F. Students should not give anyone their password or allow another person to use their account to access the Internet or school network.
G. Students must gain clearance from the teacher/librarian before downloading any programs from the Internet.
H. Students must gain permission from the teacher/librarian to utilize personal devices brought to campus. All supplementary activities involving the use of personal devices, social media, chat rooms, etc. must be conducted under the permission and supervision of system personnel.
I. Adherence to generally accepted rules of network etiquette (netiquette) is required. This includes but is not limited to the following:
    1. Be polite. Abusive messages to others will not be tolerated.
    2. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
    3. Illegal activities are strictly forbidden. Messages relating to or in support of illegal activities, cyberbullying, and other equally offensive activities should be reported to system personnel and proper authorities.
    4. Electronic mail (e-mail) is not private. System administrators have access to all mail.
    5. All communications and information accessible via the network should be respected as private property.

**V) Access to Inappropriate Material**

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter access to inappropriate information received through the Internet or other forms of electronic communication. As described in the district's technology plan, the district currently uses blocking and filtering software and hardware to ensure the safety and protection of the users.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled; or, in the case of minors, minimized only for bona fide research or other lawful purposes.

**VI) Enforcement**

Violating any of the guidelines of this policy can result in:

A. Restricted access to computing facilities and equipment.
B. Temporary or permanent loss of access to computing facilities and equipment.
C. Disciplinary or legal action including, but not limited to, criminal prosecution under appropriate state and federal laws.
D. Users being held responsible for the replacement costs of hardware or software due to damage through misuse or abuse.
E. In addition to local policy requirements, Georgia law O.C.G.A. 16-9-90, which may be cited as the Georgia Computer Systems Protection Act, also provides definitions, criminal liability and penalties for the crimes related to computer theft, computer trespass, computer invasion of privacy, computer forgery and computer password disclosure. Commission of a computer crime under O.C.G.A. 16-9-90 carries the possible penalty of a fine not exceeding $50,000 and/or incarceration for a period not to exceed one year. Property laws covering theft, vandalism, destruction and copyright also apply to computing resources.
F. Violation of state law and/or federal law can be reported to proper enforcement authorities. Irwin County School District's internal procedures for enforcement of its policies are independent of possible prosecution under the law.

**VII) Adoption**

The CIPA-Compliant Internet Safety Policy and the Acceptable Use Policy were adopted by the Irwin County Board of Education at a public meeting following normal public notice.

**VIII) CIPA Compliance**

In compliance with the Children's Internet Protection Act (CIPA) and as outlined in the district's technology plan, Irwin County is currently using software and hardware for filtering/blocking measures to ensure the safety and protection of the users. (See Irwin County School District's CIPA-Compliant Internet Safety Policy and the Irwin County School District Technology Plan.)