INFORMATION TECHNOLOGY RESOURCES/ STUDENT AND STAFF ACCEPTABLE USE AND INTERNET SAFETY

Code **IJNDB** *Issued* **7/16**

Purpose: To establish the board's vision and the basic structure for the use of technology resources in instruction.

Student access

Students are encouraged to use telecommunications to explore educational topics and conduct research related to the student's assigned curriculum. Students are to abide by acceptable use and network etiquette definitions any time they are accessing network resources. Any communication with others via the Internet is prohibited unless this communication is directly related to the student's current course of study. Student access to the Internet makes available material that may not be appropriate for student's age or course of study. The district will provide a technology protection measure (filter) in an attempt to restrict minor's access to inappropriate materials, materials harmful to minors and monitoring of online activities of minors.

The district will require parental consent prior to students accessing the Internet. The acceptable use agreement IJNDB-E(1) must be signed yearly and kept on file in the media center of the student's school prior to a student's use of any network information resources. The media specialist at each school is responsible for making sure that each student's AUP is current and on file. Schools will include instruction on acceptable use of computer technology including networks and the Internet. This instruction will include rules, rights and privileges of network/Internet use. Schools will provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response. Students and parents/legal guardians must agree to comply with these rules, rights, privileges, appropriate online behavior and any other local school rules prior to students being granted computer access.

All student use of computer technology within the district must support the district's curriculum. The district's technology center, as well as the South Carolina CIO office, will monitor all network/Internet traffic. The technology center is required to block any network traffic on the network it deems as inappropriate. Use of the Internet by any student without a current signed AUP is strictly prohibited.

Reporting

District and school computer technicians who are working with a computer and come across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

Off-campus conduct

Students, parents/legal guardians, teachers and staff members should be aware that the district may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying.

No student will engage in the following activities while using the Internet.

 (see next page)

- accessing Proxy servers (those web sites designed to bypass the district's web filter)
- sending, displaying or requesting offensive message or pictures
- using obscene language
- harassing, insulting, or attacking others (cyberbullying)
- physically damaging computers or any vandalism of computer systems or computer networks
- violating copyright laws
- using others' passwords
- trespassing in others' folders, work or files
- intentionally wasting limited resources
- intentionally using the Internet for non-instructional purposes
- employing the network for commercial purposes
- purchasing something which obligates the school or another party without prior approval
- any other activities prohibited by the district, school or teacher

Sanctions may include the following.

- loss of access to computers
- removal from a class/course which requires computer access
- disciplinary action for inappropriate language or behavior consistent with school board policies
- notification of law enforcement agencies when criminal conduct is suspected

Employee access

Employees are encouraged to use telecommunications to explore educational topics, conduct research and communicate with others in a professional capacity. Employees are to abide by acceptable use and network etiquette definitions any time they are accessing network resources. Access to networked information resources is a privilege extended to employees. The district requires that each employee sign an acceptable use agreement form IJNDB-E(2) prior to using any networked information resources or being granted Internet access. This form must be signed each year and kept on file at the staff members work site. Use of the Internet without a current signed AUP is strictly prohibited. Staff members directly responsible for students are required to monitor students closely while they are on the Internet, to prohibit surfing of the Internet unless it is directly related to the district's curriculum and to monitor for safety/security of minors when using email, chat rooms or other direct electronic communication.

Employees will not engage in the following activities while using networked information resources.

- sending, displaying or requesting offensive message or pictures
- using obscene language
- harassing, insulting or attacking others
- physically damaging computers or any vandalism of computer systems or computer networks
- violating copyright laws
- using others' passwords
- trespassing in others' folders, work or files
- intentionally wasting limited resources
- employing the network for commercial purposes
- any other activities prohibited by their supervisor
- unauthorized disclosure, use and dissemination of personal information regarding minors

Employees are required to immediately report any breach of this policy by any student or staff.

 (see next page)

Sanctions may include the following.

- disciplinary action to be determined by their supervisor or the superintendent
- notification of law enforcement agencies when criminal conduct is suspected

Adopted 8/19/08; Revised 6/12/12, 7/19/16

Legal references:

A. Federal Law:
   1. Children's Internet Protection Act of 2000, 47 U.S.C.A. Section 254(h).
   2. The Digital Millennium Copyright Act of 1998, 17 U.S.C.A. Section 512 - Limitations on liability relating to material online.

B. S.C. Code, 1976, as amended:
   1. Section 10-1-205 - Computers in public libraries; regulation of Internet access.
   2. Section 16-3-850 - Encountering child pornography while processing film or working on a computer.
   3. Section 16-15-305 - Disseminating, procuring or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.