USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Code **IJNDB** *Issued* **10/05**

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

The Internet can provide a vast collection of educational resources for students and employees. It is a global network that makes it impossible to control all available information. Because information appears, disappears and changes constantly, it is not possible to predict or control what students may locate. The center makes no guarantees as to the accuracy of information received on the Internet. Although students will be under instructor supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students might encounter information that is not of educational value.

General system user responsibilities

Access to the Internet is a privilege, not a right. With this privilege, there is also a responsibility to use the Internet solely for educational purposes and not to access inappropriate materials not suitable for students.

The center does not condone the use of objectionable materials. Such materials are prohibited in the center environment.

Students knowingly bringing prohibited materials into the school environment will be subject to suspension and/or revocation of their privileges on the center's system and will be subject to discipline in accordance with the center's policy and applicable administrative rule.

Substitute instructors must be specifically certified to instruct in classrooms where students are accessing the Internet. Certification requirements will ensure that substitute instructors have a standard level of technical proficiency and understand Internet safety and responsible use issues, this policy and the obligations related to supervision of students in their use of the Internet.

Online conduct

The individual in whose name a system account is issued is responsible at all times for its proper use. The center's system will be used only for educational purposes consistent with the center's mission and goals. The center prohibits commercial and/or personal use of the center's system.

- System users will not submit, publish or display on the center's system any inaccurate and/or objectionable material.
- System users will not encourage the use of tobacco, alcohol or controlled substances or otherwise promote any other activity prohibited by center policy or state or federal law.
- Transmission of material, information or software in violation of any center policy or local, state or federal law is prohibited.
- System users identifying a security problem on the center's system must notify the appropriate instructor or the director.
- System users may not use another individual's system account without written permission from the director.

 (see next page)

- Attempts by a student to log onto the center's system as a center employee will result in cancellation of user privileges and may result in disciplinary action up to and including expulsion.

- System users will not write to directories other than their own as identified by the center.

- Instructors may require students to restrict access to course program files.

- Any system user identified as a security risk or having a history of violations of center and/or building computer-use guidelines may be denied access to the center's system.

- Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy or modify the electronic mail of other system users is prohibited, as is deliberate interference with the ability of other system users to send/receive electronic mail.

- Any software having the purpose of damaging the center's system or other user's system is prohibited.

- Copyrighted material may not be placed on any system connected to the center's system without the author's permission. Only the owner's or individuals the owner specifically authorizes may upload copyrighted material to the system.

- System users may download copyrighted material for their own use. System users may redistribute non-commercial copyrighted programs only with the express permission of the owner or authorized person. Such permission must be specified in the document or must be obtained directly from the author in accordance with applicable copyright laws, center policy and administrative rules.

- System users may upload public domain programs to the system. System users may also download public domain programs for their own use or non-commercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

Internet usage guidelines

- Prohibit transmission of any material in violation of any federal or state laws or regulations to include, but not be limited to, the following.

  - copyrighted material
  - threatening or obscene material
  - material protected by trade secret
  - sexual harassment
  - other forms of discrimination

- Require all users to accept the responsibility to safeguard their passwords.

- Prohibit the downloading of software, files, etc., without permission of the network administrator.

- Prohibit access/modification to any files to which the user has not been given appropriate authorization.

- Prohibit the posting of photos of students without administration approval and parental permission.

 (see next page)

- Allow the downloading of only material that is not a copyright violation; copyrighted photos and cartoons are not downloadable; QuickTime movie segments are not allowable if they are on the ALA approved list.
- Prohibit student participation in any form of electronic "chat" unless it is for specific educational purposes and directly supervised by staff.
- Require staff supervision when students access the Internet.
- Require "safe" and "valid" Internet searching.
- Provide Internet filtering software to decrease the ability of users to access websites displaying obscene material.

Accessing inappropriate sites

Student Internet activities will be monitored by the center to ensure students are not accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are harmful to minors. The center will use technology protection measures to protect students from inappropriate access.

The center will provide reasonable notice of and at least one public hearing or meeting to address and communicate its Internet safety measures.

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

Technology protection measure (filtering software)

The center has selected a technology protection measure (filtering software) for use with the center's Internet system and has specified the manner in which the technology protection measure will be configured. The technology protection measure will always be configured to protect against access to material that is obscene, child pornography and material that is harmful to minors, as defined by the Children's Internet Protection Act (CIPA). The center may, from time to time, reconfigure the technology protection measure to best meet the educational needs of the center and address the safety needs of the students.

The technology coordinator will conduct an annual analysis of the effectiveness of the selected technology protection measure (filtering software) and make recommendations to the director regarding the selection and configuration of such measure.

The technology protection measure (filtering software) may not be disabled at any time that students may be using the center Internet system, if such disabling will cease to protect against access to materials that are prohibited under CIPA. The technology protection measure may be disabled during non-student use time for system administrative purposes.

Unblocking filtering software

Authority will be granted to selected educators to temporarily or permanently unblock access to sites blocked by the technology protection measure (filtering software) in order to ensure that the

 (see next page)

implementation of the technology protection measure is accomplished in a manner that does not unduly restrict the educational use of the center Internet system by instructors or students and ensures the protection of students' constitutional rights of access to information and ideas.

To temporarily unblock a site, the authorized individual must review the contents of the site, outside of the presence of any student, prior to allowing access to the site by a student.

Reports of all instances of temporary unblocking will automatically be forwarded to the center technology coordinator.

If an authorized individual believes that the blocked site should be permanently unblocked, a recommendation will be forwarded to the center technology committee. The technology committee may make a decision to permanently unblock access to the site.

Vandalism of system, equipment or data

Vandalism is defined as any malicious attempt to harm or destroy center equipment or materials, data of another user of the center's system(s) or any of the agencies or other networks that are connected to the Intranet and Internet, and is prohibited. Deliberate attempts to compromise, degrade or disrupt system performance or operation will be viewed as violations of the center's policies and administrative rule and possibly as criminal activity under applicable state and federal laws. Vandalism includes, but is not limited to, the placement, transmission or creation of computer viruses or other data or programs that negatively impact the computer or system.

Vandalism will result in cancellation of system use privileges. Fines will be imposed for acts of vandalism.

Adopted 12/9/03; Revised 9/14/04, 10/25/05

Legal references:

A. Federal law:
   1. 47 USC Section 254(h) - Children's Internet Protection Act.

B. S.C. Code of Laws, 1976, as amended:
   1. Section 16-3-850 - Encountering child pornography while processing film or working on a computer.