Shelby County Board of Education

6031

Issued Date: 08/26/10
Revised Date: 03/25/14

INTERNET SAFETY AND USE

District-Provided Access to Telecommunication Networks

I. PURPOSE

To promote educational excellence, equity, efficiency and communications through the appropriate use of telecommunications and other technologies that have transformed the ways that information may be accessed and communicated.

II. SCOPE

This policy applies to all students, employees, board members, contractors, vendors and guests. Guests include parents, volunteers, and any other persons or agencies authorized to use or have access to Shelby County School (SCS) telecommunications network/equipment.

III. DEFINITION

Telecommunications - Communication over a distance by electronic transmission of impulses. Examples include internet, local area networks, television, radio, telephone, and mobile devices.

IV. POLICY STATEMENT

The Shelby County Schools Board of Education recognizes that electronic information resources have transformed the ways that information may be accessed and communicated. The Board generally supports access by students to rich information resources and believes it incumbent upon students to use this privilege in an appropriate and responsible manner. The Board encourages the development of appropriate skills to analyze and evaluate such resources.

Electronic information research skills have become a necessary part of the educational process. The Board expects that faculty will blend thoughtful use of the Internet throughout the curriculum and will provide guidance and instruction to students in its use. As much as possible, access from school to Internet resources

should be structured in ways which point students to those sources suited to learning objectives. While students will be able to move independently through resources, they shall be provided with guidelines defining acceptable use.

The Board authorizes the Superintendent to develop and implement procedures to provide guidance for students in the appropriate and ethical use of telecommunication networks such as the Internet.

Principles of Acceptable and Safe Internet Use

A. General

In accordance with federal law, SCS shall ensure the Internet safety of students through enforcement of acceptable use guidelines, and a filtered network that is monitored for unacceptable content pursuant to 47 USC section 254(h) and the Children's Internet Protection Act. The acceptable use guidelines include prohibitions on the access, creation, receipt, display or transmission of inappropriate material; monitoring Internet and e-mail traffic to prevent access to inappropriate material; restrictions on access to students' personal information; and prohibitions on "hacking" and other unauthorized access. The technology protection measures include computer software programs, or "filters," with respect to all Internet-enabled computers, that will block access to visual depictions or documents that are obscene, that contain child pornography**,** promote, encourage, or provide the skills to commit illegal, criminal activities**,** or, with respect to use of the computers by minors, that are harmful to minors.

The District shall educate students on appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response (6046-Harassment, Intimidation, or Bullying of Students (Sexual, Racial, Ethnic, Religious).

1. Students

   Students utilizing school-provided Internet access are responsible for appropriate behavior on-line just as they are in a classroom or other area of the school. Communications on the network are often public in nature. General school rules for behavior and communications apply in using the networked-communications system.

2. Employees, Board Members, Contractors, Vendors and Guests

   All employees, board members, contractors, vendors and guests are expected to conduct their use of the District’s telecommunication network with the same integrity as in face-to-face or telephonic business operations.

B. Rules for Use of the District's Telecommunication Network

All users, including students, employees, parents, contractors, and any other person using the District's network, shall comply with the following rules:

- The District's network may be used only for educational and professional purposes consistent with the District's goals. Commercial use (advertisements, business logos, etc.) of the District's network is prohibited, unless specifically permitted in writing by the Department of Communications. A list of school adopters is permitted.
- Users will only use District-approved e-mail applications.
- Users cannot use the Internet to create, access, or transmit information that is obscene or vulgar, that advocates dangerous or illegal acts or that advocates violence or hatred toward any group. Written approval by the teacher and the parent may be required when a research project involves accessing information on the Internet relating to dangerous or illegal acts or violence or hatred toward a group.
- Personal employee information must be given out only in an instructional context or in the performance of District business.
- Materials that are offensive, threatening or that otherwise are intended to harass or demean recipients must not be transmitted, including jokes that are intended to offend, harass or intimidate.
- Files, data or information of others must not be improperly accessed or misused.
- Plagiarizing is prohibited. Plagiarism means to steal and pass off the ideas or words of another as one's own. Users cannot use another's ideas or words without crediting the author.
- Copyright infringement is a violation of federal law. Users should be aware that most of what is on the Internet is protected by copyright. Copyrighted materials include, but are not limited to, writings, articles, web pages, designs, music, videos, and software. The illegal installation, use, or transmission of copyrighted materials is prohibited.
- Web sites cannot display photographs or videos of employees or individuals not affiliated with the District without the individual's prior consent, unless the individual is an historic figure or a public figure.

C. Prohibited Uses

1. Students

   Students shall not transmit personally identifiable or personal contact information about themselves or others, except the student's e-mail address, without prior consent by the parent and the teacher. Personally identifiable or personal contact information shall include name, address, telephone number, photograph, social security number, school name, and classroom.

   School web sites cannot include pictures or names of students without prior written consent of the parents and teacher. All other personally identifiable information (e.g., address and phone number) is strictly prohibited on a web site.

2. All Users

   The District prohibits the use of SCS's electronic system in ways that are inappropriate, disruptive, offensive to others, or harmful to morale. Examples of prohibited uses include but are not limited to:

   - Unauthorized transmission of confidential information pursuant to TCA 10-7-504 (Confidential Records).
   - Downloading, installation and use of programs that infiltrate computing systems and/or damage software components, including "viruses," "worms, trojan horses, trap door programs codes, or other malicious codes."
   - Downloading, installation and use of any program or software without prior written authorization of the Division of Information Technology.
   - Intentionally disrupting network traffic, crashing the network, or gaining unauthorized access to the files of another user.
   - Using inappropriate language in any type of communication on the SCS network. Inappropriate language includes, but is not limited to, language that is vulgar, profane, abusive and threatening.
   - Using the SCS network to personally attack, harass, or threaten another person or intentionally or recklessly publishing false information about another person
   - Private use of the District's network. Incidental personal use by employees during lunch and break times is permitted.
   - Illegal use of the SCS network.
   - Using the District's network for political lobbying.
   - Anonymous communications.
   - Mass e-mailing of unsolicited or unwanted messages ("spamming"), including text, software, video images, graphics.
   - Playing computer games, unless part of an educational program.

- Falsifying, concealing, or misrepresenting the user's e-mail identity ("spoofing").
- Forwarding messages without the knowledge and permission of the original user, except in circumstances in which forwarding is customary or expected.
- Downloading music and sound recordings without prior approval.
- Any action which violates existing Board policy, or local, state or federal law.

D. Authorization for Use

1. Students
   Use of the system's electronic resources will be permitted upon submission of agreement forms by students and parents. Violations of the terms and conditions stated in the agreement may result in disciplinary action up to and including expulsion for students.

2. Other Users
   Use of the District's telecommunications and electronic information sources network will be permitted upon submission and approval of agreement forms by employees, vendors, contractors and guests. Employees and other users must sign and return the authorization form to the appropriate staff member.

<u>Review and Monitoring</u>

1. The District reserves the right to review, monitor, and restrict at any time information stored on or transmitted via the District's network and to investigate suspected inappropriate use of resources.

2. The District reserves the right to monitor and read e-mail communications. USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN E-MAILS TRANSMITTED, RECEIVED AND STORED ON AND THROUGH THE SCS NETWORK.

3. Correspondence in the form of electronic mail may be a public record under the state of Tennessee's public records law and may be subject to public inspection.

4. The District may monitor or review user's Internet activity at any time. Users should have no expectations of privacy in their Internet traffic and activities.

Sanctions for Violations of this Policy

Violations of this policy or the required agreements may result in loss of access to the District's network. Additional disciplinary action may also be taken, including suspension/expulsion for students and termination of employment for employees. When applicable, law enforcement agencies may be involved.

V. RESPONSIBILITY

A. Principals are responsible for ensuring that school personnel are trained and have appropriate authorization to access SCS telecommunications networks, and for reviewing and approving all information published by their schools.

B. Executive staff is responsible for ensuring that all employees, vendors, contractors and guests within their jurisdiction are trained and have appropriate authorization to access the telecommunication networks, and for reviewing and approving all information published by their departments.

C. Teachers are responsible for ensuring that students are trained to use the district's telecommunication networks. Teachers are responsible for monitoring use of the Internet in their classrooms.

D. Users of the district's telecommunication networks, including contractors, consultants and parents, are responsible for complying with the provisions of this policy, the pertinent administrative rules and regulations, and the acceptable use policy agreement.

E. Any questions concerning this policy, the pertinent administrative rules and regulations, or the acceptable use policy agreement should be directed to the department responsible for Information Technology.

F. The Board is responsible for ensuring that board members comply with the pertinent provisions of this policy.

G. The Division of Internal Audits is responsible for determining if this policy is followed.

H. The Superintendent is responsible for ensuring that this policy is followed.

Legal References:

1. TCA 39-14-602
2. TCA 10-7-512
3. TCA 49-1-122
4. 47 U.S.C. § 254

Cross References:

1. 6046-Harassment, Intimidation, or Bullying of Students (Sexual, Racial, Ethnic, Religious

5. Children's Internet Protection Act