

	MURFREESBORO CITY SCHOOL BOARD POLICY		
	Descriptor Term:	Descriptor Number:	Date Adopted:
	STUDENT USE OF INTERNET	STU 37	9/96
	Revision Adopted: 9/09; 8/10		

I. PURPOSE

The Board supports the right of students (regular or extended school students) to have reasonable access to various information formats and believes it incumbent upon students to use this privilege in an appropriate and responsible manner.

Electronic information research skills are now fundamental to preparation of citizens and future employees. The Board expects staff to blend thoughtful use of such information throughout the curriculum and to provide guidance and instruction to students in the appropriate use of such resources.

Students shall abide by MCS Board policies, and stipulations of the Children's Online Protection Act 47 USC Section 231 (COPPA), the Family Education Rights and Privacy Act (FERPA), and the Children's Internet Protection Act (CIPA) as well as laws pertaining to stalking and harassment. The policy is promulgated so as to be in compliance with the public records laws of the State of Tennessee.

II. STUDENT USE OF SCHOOL COMPUTER NETWORKS

- A. Students are responsible for appropriate behavior when using school computer networks just as they are responsible for appropriate behavior in all school settings. Communications on the network are often public in nature. General school rules for behavior and communications apply to all users of the networked communications system. The network is provided for students to conduct research, explore the world, and communicate with others. Access to network services will be provided to students who agree to act in a responsible manner.
- B. Independent student use of telecommunications and electronic information resources will be permitted upon submission of permission forms and agreement forms by parents of minor students.
- C. Access to telecommunications will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The Board believes that the benefits to student from access in the form of information resources and opportunities for collaboration exceed the disadvantages. Ultimately, however, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. The Murfreesboro City School Board supports and respects each family's right to decide whether or not to apply for independent access on computers used outside the system.

D. The Director of Schools shall develop and implement procedures for appropriate Internet use by students. Procedures shall address the following:

1. General rules and ethics of Internet use.
2. Prohibited or illegal activities, include, but are not limited to:¹
 - Sending or displaying offensive messages or pictures
 - Using obscene language
 - Harassing, insulting, defaming or attacking others
 - Damaging computers, computer systems or computer networks
 - Hacking or attempting unauthorized access
 - Violation of copyright laws
 - Trespassing in another's folders, work or files
 - Intentional misuse of resources
 - Using another's password or other identifier (impersonation)
 - Use of the network for commercial purposes
 - Buying or selling on the Internet

III. INTERNET SAFETY MEASURES

A. Internet safety measures shall be implemented that effectively address the following:

1. Controlling access by students to inappropriate matter on the Internet and World Wide Web
2. Preventing unauthorized access, including "hacking" and other unlawful activities by students on-line
3. Unauthorized disclosure, use and dissemination of personal information regarding students
4. Restricting students' access to materials harmful to them

B. The Director of Schools/designee shall establish a process to ensure the district's education technology is not used for purposes prohibited by law or for accessing sexually explicit materials. The process shall include, but not be limited to:

1. Utilizing technology that blocks or filters Internet access (for both students and adults) to material that is obscene, child pornography or harmful to students
2. Monitoring on-line activities of students²

C. The Board shall provide reasonable public notice of, and at least one (1) public hearing or meeting to address and communicate, its Internet safety measures.²

A written parental consent shall be required prior to the student being granted access to electronic media involving district technological resources. The required permission/agreement form, which shall specify acceptable uses, rules of on-line behavior, access privileges and penalties for policy/procedural violations, must be signed by the parent/legal guardian of minor students each year and shall be valid only in the school year in which it was signed unless parent(s) provide written notice that consent is withdrawn. In order to rescind the agreement, the student's parent/guardian must provide the director of schools with a written request. Such acknowledgment shall be incorporated into the parent/student handbook.

IV. E-MAIL

Users with network access shall not utilize district resources to establish electronic mail accounts through third-party providers or any other nonstandard electronic mail system. All data including e-mail communications stored or transmitted on school system computers may be monitored. Students have no expectation of privacy with regard to such data. E-mail correspondence may be a public record under the public records law and may be subject to public inspection.³

V. INTERNET SAFETY INSTRUCTION

Students will be given appropriate instruction in Internet safety as a part of any instruction utilizing computer resources. Parents and students will be provided with information to raise awareness of the dangers posed by the Internet and ways in which the Internet may be used safely.⁴

VI. NETWORK SECURITY

- A. For the protection and security of MCS data, all computers attached to the MCS physical network (a computer located at a MCS facility either wired or wireless), must be the property of MCS. It is prohibited to attach a computer that is not property of MCS to the network without first receiving approval from the IT Department management.
- B. Use of software designed to gain passwords or access beyond the rights assigned to a user or computer are strictly prohibited. Use of such programs risk the security of the network and is considered “hacking.” The intent to control unauthorized access is a violation of State and Federal law. Violators will be prosecuted. Should a student inadvertently discover passwords or any other measure used to control unauthorized access, the student should report such discovery to their teacher.
- C. No user shall encrypt files or folders or attempt to hide files or folders stored on a network server or local workstation. Any encrypted or hidden files will be deleted.
- D. All network users can be monitored at any time by authorized personnel for the purpose and inspection of compliance to these guidelines.

VII. WORKSTATION/COMPUTER USE

- A. All students are prohibited from installing any software on any computer unless authorized in writing by a member of the IT Department. Illegal downloads or use of copyrighted software, music, videos, pictures or other files is strictly prohibited
- B. All students are prohibited from using any computer for illegal or commercial activity.
- C. Any desktop applications designed to limit access to students or staff, other than those used by the IT Department for network security purposes, is prohibited.

- D. Changing or tampering with any computer's system configuration is strictly prohibited.
- E. Computers found to be tampered with or computers with unapproved software or files will be re-formatted and restored to compliance.
- F. Installing and using personal accounts is prohibited under all circumstances through any type of access or connectivity to include private phone lines.
- G. No desktop computer shall be moved by anyone other than IT Department personnel unless approved by a member of the IT Department.

VIII. SERVER SOFTWARE

Only authorized IT Department personnel will install software to the server.

IX. SAVING DOCUMENTS

Students must save all documents to a location away from the computer. Due to server storage limitations, any applications or executables residing in a user directory will be deleted. (Exception is given where individuals have created applications as part of a curriculum assignment and such activity has been approved by a member of the MCS faculty or staff.) Any documents residing solely on a local computer are at risk. It is each student's responsibility to make sure important documents and data are saved to a location away from the computer.

X. VIRUSES AND VIRUS PROTECTION

- A. The MCS IT Department will provide all virus protection and related software for all workstations and servers. Virus protection and related software will be installed by authorized IT personnel unless otherwise approved by the IT Department.
- B. There are many virus hoaxes. Students should never delete system files from a computer in order to remove a potential virus without first checking with their teacher to make sure the virus is valid and not a hoax.

XI. COPYRIGHT POLICY

All students and employees must comply with all applicable copyright laws in the use of all media and materials.

XII. VIOLATIONS

- A. Failure to follow all or part of these guidelines, or any action that may expose MCS to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure, or compromise the safety of users is prohibited and may result in disciplinary action up to and including loss of network privileges, confiscation of computer equipment, suspension and/or criminal prosecution.

B. Student Compliance

1. Students shall not attempt to make use of material or attempt to locate material which would not be acceptable in a school setting.
2. Students will be supervised by faculty during use of online resources.
3. Students must comply with the MCS Board policy.
4. Students shall report to school personnel any personal electronically transmitted attacks in any form made by others over the Internet or local network using any MCS' technology.
5. Students shall understand information obtained via the Internet may or may not be correct.

C. Violations of this policy or a procedure promulgated under its authority shall be handled in accordance with the existing disciplinary procedures of Murfreesboro City Schools.

XIII. IMPLEMENTATION

Administrative Directive 44 implements this policy.

Legal References:

1. T.C.A. §39-14-602 Use of Electronic Mail (e-mail) 1.805
2. 47 U.S.C. §254; *Federal-State Joint Board on Universal Service*, CC Docket No. 96-45 Report and Order (March 30, 2001)
3. T.C.A. §10-7-512
4. T.C.A. §49-1-221

Cross References:

Administrative Directive 44

