

	<b>MURFREESBORO CITY SCHOOL BOARD POLICY</b>		
	Descriptor Term:  <b>EMPLOYEE USE OF INTERNET/ ELECTRONIC MAIL</b>	Descriptor Number:  PER 44	Date Adopted:  9/09
	Revision Adopted:		

## I. POLICY

- A. The Board offers employees of the Murfreesboro City School System, who need it, access to the Internet and electronic mail (e-mail) as a business tool.
- B. Access to e-mail and the Internet will enable employees to explore thousands of libraries, databases and bulletin boards while exchanging messages with Internet users throughout the world. Although there is some degree of risk in offering Internet access, we believe that benefits to the school system exceed any disadvantages.

## II. INTERNET AND E-MAIL POLICY

The network is provided for authorized employees to conduct research and communicate with others for school related purposes. Access to network services is given to employees who agree to act in a considerate and responsible manner. Internet access and e-mail accounts are issued only after Board approved training has occurred. Access can be revoked at any time if network security or protocol is compromised.

## III. USE OF ELECTRONIC MAIL (E-MAIL)

- A. Electronic mail capability among board members and district staff exists for the purpose of enhancing communication to better perform tasks associated with their positions and assignments. Therefore all staff and board members who have access to the district network shall adhere to the following guidelines when sending or receiving messages via system-wide-electronic mail (e-mail):
  1. Because all computer hardware and software belong to the school district, all data including e-mail communications stored or transmitted on school district computers shall be monitored. Employees/board members have no right to privacy with regard to such data. Confidentiality of e-mail communication cannot be assured. E-mail correspondence may be a public record under the public records law and may be subject to public inspection.<sup>1</sup>
  2. Messages shall pertain to legitimate board/district business; email shall not be used to circumvent requirements of the Open Meetings Act.<sup>2</sup>
  3. Staff/board members will be asked to sign an application for terms and conditions for Use of the Internet. Staff/board members shall not reveal their passwords to others in the network or to anyone outside of it. If anyone has reason to believe that a password has been lost or stolen or that e-mail has been accessed by someone without authorization, the employee shall contact the technology coordinator immediately.
  4. It is the responsibility of the sender not to violate copyright laws.

5. Messages shall not be sent that contain material that may be defined by a reasonable person as obscene or that are racist, sexist or promote illegal or unethical activity.
- B. 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. Employees 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.<sup>3</sup>

#### **IV. INAPPROPRIATE USES AND PRACTICES**

- A. The following practices are considered unacceptable, and may be subject to disciplinary action including written warnings, revocation of access privileges, and/or up to and including termination.
1. Visiting Internet sites that contain obscene, racist, sexist, discriminatory or otherwise objectionable materials; sending or receiving any material that is obscene or defamatory, or which is intended to annoy, harass or intimidate another person.
  2. Sending and receiving unusually large e-mails or attachments; sending or forwarding electronic chain letters.
  3. Spending time on non-school/non-school system business.
  4. Soliciting e-mails that are unrelated to school activities, or soliciting non-school business for personal gain or profit.
  5. Representing personal opinions as those of the Board, school or school system.
  6. Using the Internet or e-mail for gambling or other illegal activities.
  7. Making or posting indecent remarks, proposals or materials.
  8. Uploading, downloading or otherwise transmitting commercial software or copyrighted material in violation of its copyright.
  9. Intentionally interfering with normal operation of the network, including the propagation of computer viruses, or sustained high volume network traffic which substantially hinders others in their school business related use of the network.
  10. Revealing or publicizing confidential information regarding students or employees.
  11. Examining, changing or using another person's files, output, account or user name without explicit authorization from the Murfreesboro City Schools Technology Department.
  12. Other inappropriate uses of the Internet or network resources that may be identified by the network administrator.
- B. The Board reserves the right to report any illegal activities to appropriate authorities.

#### **V. USE OF INTERNET**

- A. Before any employee is allowed use of the district's Internet or intranet access, the employee shall sign an employee acknowledgement form, PER 44 Form A (see attached). Any employee who accesses the district's computer system for any purpose agrees to be bound by the terms of that agreement, even if no signed written agreement is on file.

B. The director of schools shall develop and implement procedures for appropriate Internet use which shall address the following:

1. Development of the Network and Internet Use Agreement.
2. General rules and ethics of Internet access.
3. Guidelines regarding appropriate instruction and oversight of student Internet use.
4. Prohibited and illegal activities, include but are not limited to the following:<sup>1</sup>

- 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 to any computer
- 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

## **VI. VIOLATIONS**

Violations of this policy or a procedure promulgated under its authority shall be reported immediately to the director and may result in the suspension and/or revocation of system access or if deemed necessary, appropriate disciplinary action may be taken.

## **VII. IMPLEMENTATION**

Administrative Directive 44 implements this policy.

---

## **REFERENCES:**

1. T.C.A. §10-7-512
2. T.C.A. §8-44-102
3. T.C.A. §10-7-512

**ACCEPTABLE USE, MEDIA RELEASE, AND INTERNET SAFETY PROCEDURES  
EMPLOYEE ACKNOWLEDGMENT FORM**

**SCHOOL OR DEPARTMENT:** \_\_\_\_\_

**JOB TITLE:** \_\_\_\_\_

**EMPLOYEE NAME:** \_\_\_\_\_

**I. PURPOSE**

The Murfreesboro City School District (MCS) provides employee access to the Internet as a means to increase learning and productivity toward achieving 21st Century literacy. The purpose of this contract is to assure that users recognize the procedures which the school imposes on their use of Internet, electronic media resources, and release of student information. In addition, this contract requires that users agree to 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. THE CONTRACT**

MCS has outlined the following guidelines as required for all technology users. The district has taken measures designed to protect students and adults from obscene information and restrict access to materials that are harmful to minors. 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, disciplinary action up to and including termination of employment, and/or criminal prosecution.

**A. Employee Compliance**

All employees must comply with the MCS Board policy. Users shall not attempt to make use of material or attempt to locate material which would not be acceptable in a school setting. Students shall be supervised by faculty during use of online resources.

**B. Internet Safety**

All students will participate in Internet safety instruction integrated into the district's instructional program in grades K-6. Schools will use existing avenues of communication to inform parents about Internet safety.

**C. Network Security**

1. Only users with valid MCS network accounts are authorized to use the MCS's

network and computer equipment. Employees must only use their assigned network account. Users are prohibited from giving anyone their network password or network account information other than to authorized personnel.

2. Employees are not to allow anyone to use a computer while logged in. Computer users should always logoff from the network before leaving their room or office.
3. 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.
4. 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 you inadvertently discover passwords or any other measure used to control unauthorized access you should report such discovery to IT personnel.
5. 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.
6. All network users may be monitored at any time by authorized personnel for the purpose and inspection of compliance to these guidelines.

#### **D. Workstation/Computer Use**

1. All employees 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.
2. All employees are prohibited from using any computer for illegal or commercial activity.
3. 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.
4. Changing or tampering with any computer's system configuration is strictly prohibited.
5. All computers must be turned off before 8:00 pm every evening in order to complete the backup of all files on the server and for server maintenance.
6. Computers found to be tampered with or computers with unapproved software or files will be re-formatted and restored to compliance.
7. Installing and using personal accounts is prohibited under all circumstances through any type of access or connectivity to include private phone lines.
8. No desktop computer shall be moved by anyone other than IT Department personnel unless approved by a member of the IT Department.

#### **E. Server Software**

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

#### **F. Saving Documents**

Employees must save all documents to the network. Employees should not save any applications to the network, only documents and data may be saved. Due to server storage limitations, any applications or executables residing in an employee's 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's faculty or staff.) Any documents residing solely on an employee's local computer are at risk.

It is the employee's responsibility to make sure important documents and data are saved to the network.

#### **G. Network Drives/Shares**

All users have access to a public directory on the server. All users' desktop and document data will be backed up on the server. Employees should make sure they have a backup of anything you have on the server and on their computer.

#### **H. Viruses and Virus Protection**

1. 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.
2. Employee should not open any e-mail attachments from anyone the employee does not know. An employee should never forward an email suspected of containing a virus. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted. If an employee feels a computer may contain a virus, the employee should contact the IT Department immediately.
3. There are many virus hoaxes. An employee should never delete system files from a computer in order to remove a potential virus without first checking with the IT Department to make sure the virus is valid and not a hoax.

#### **I. Copyright Policy**

All students and employees will comply with all applicable copyright laws in the use of all media and materials. All employees will model legal and ethical practice related to technology use as established in Murfreesboro City School Board Policy IS 21.

#### **J. E-mail**

1. The MCS e-mail system has been provided for the internal and external communication of employees and board members. Responsible and ethical use of the e-mail system is required. The e-mail system may not be used for personal gain, or political or religious views or in any illegal, offensive or unethical manner. The e-mail system is intended only for valid and legitimate MCS related communication.
2. MCS does reserve the right to access any e-mail for any business purpose, and also for inspection for disciplinary or legal actions.
3. Emails on the MCS network may be a public record according to the Tennessee Open Records Act.

### **III. ACCEPTANCE OF TERMS AND CONDITIONS**

These terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreement and understandings of the parties.

I have read this contract and all related policies cited within and understand that should I fail to honor all the terms of this contract, I may be subject to disciplinary action, up to and including termination, and future Internet and other electronic media accessibility may be denied.

**Employee Name (Please Print)**\_\_\_\_\_

**Employee Signature**\_\_\_\_\_ **Date**\_\_\_\_\_

