REGULATION   MONTGOMERY COUNTY PUBLIC SCHOOLS

Related Entries: AFA, BBB, EDC, EDC-RA, EGI-RA, EHA, EHC-RA, IGS, JFA, JFA-RA, JOA-RA, KBB

Responsible Office: Chief Operating Officer
Global Access Technology

User Responsibilities for Computer Systems and Network Security

I.   PURPOSE

A.   To ensure the security of all elements of MCPS computer systems, related technology, and electronic information

B.   To delineate appropriate uses for all users of MCPS computer systems

C.   To promote intellectual development through the use of computer systems, related technology, and electronic information in a safe environment

D.   To ensure compliance with relevant state, local, and federal law

II.   BACKGROUND

MCPS provides computer equipment, computer services, and network access to schools and offices for purposes consistent with the mission of MCPS. The wide array of information technology available to MCPS users introduces new risks and opportunities. The responsibility for appropriate behavior rests with all individuals who use MCPS information technology resources and computing facilities. Levels of access are provided depending on assignment, responsibility, and need to know. Users must protect information and resources against theft, malicious damage, unauthorized access, tampering, and loss.

III.   DEFINITIONS

A.   A *computer system* is hardware, software, and related technology including networks, wiring, and communications equipment.

B.   *Electronic data* are facts and information contained in any electronic form.

C. *Educational purposes* are those actions directly promoting the educational, instructional, administrative, business, and support services mission of MCPS and related to any instruction, project, job, work assignment, task, or function for which the user is responsible.

D. A *local security administrator* (*LSA*) is the individual at a site responsible for computer and network system security. This can be a principal, director, other head of an office, program, or facility, or the designee.

E. A *user* is any MCPS staff member, student, or other individual authorized to use MCPS computer systems. Other individuals may include parents, volunteers, and contract or temporary staff.

F. *Harmful to students* means any text, graphic, pictorial, or auditory representation that taken as a whole and with respect to students, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes or represents, in a patently offensive way with respect to what is suitable for students, actual or simulated normal or perverted sexual acts, or a lewd exhibition of genitals; and taken as a whole, lacks serious literary, artistic, political, or scientific value as to students.

G. *Inappropriate materials* consist of text, graphic, pictorial, or auditory representations of items that are inconsistent with the educational mission of the school system as set forth in the policies of the Board of Education, including material intended to teach skills that would enable an individual to engage in illegal activities, materials that promote discrimination against others based on race, religion, gender, nationality, sexual orientation, or advocate illegal use of any controlled dangerous substances or of alcohol.

H. A *technology protection measure* is Internet filtering software that is designed to limit access to selected portions of the Internet based on identified criteria. Its intended use in MCPS is to limit access to inappropriate material and/or material that might be harmful to students.

I. *Internet access* includes all methods used to connect to the Internet servers and users, and all methods for providing access regardless of funding or facilitating sources, including e-mail.

IV. PROCEDURES

The following section delineates appropriate procedures in the areas of electronic data security, physical security, systems and applications security, network security, conduct and use, and noncompliance. More specific responsibilities and procedures for computer

systems security are outlined in the *Manual of MCPS Computer Systems Security Procedures*, available from the Office of Global Access Technology.

A.   Electronic Data Security

Users may only access information and/or computer systems to which they are authorized and that they need for their assignments and responsibilities.

1.   Users are responsible for their own individual accounts.

a)   Users cooperate in the protection of their accounts by changing passwords as required and keeping passwords strictly confidential.

b)   Users are expressly prohibited from sharing of accounts and passwords.

c)   Any violations that can be traced to an individual account name will be treated as the responsibility of the account owner.

2.   Users must log off all systems before leaving a computer or workstation or allowing others to use it.

3.   It is the responsibility of every user to be aware of and follow security procedures in accordance with this regulation.

4.   Users must secure their electronic data. (Note: Sensitive files must be saved to a secure location such as an individual's network folder/directory or a removable disk that is then secured in a locked file cabinet.)

5.   MCPS is not responsible for information that may be lost due to system failures or interruptions. Users should make backup copies and ensure they are stored in a secure place.

B.   Physical Security

Computer systems equipment must be located and maintained in a secure physical environment. Users are responsible for cooperating with the following physical security provisions for computers and related technology.

1.   When staff members are not present to supervise the area, all areas (including permanent or temporary storage) housing valuable computer equipment must be secured.

2. Computer or related equipment may not be removed from MCPS property without appropriate authorization.

3. Users must employ local accountability procedures to sign in or out any computer or related equipment. This equipment must be returned to the school, department, division, or unit that owns it prior to the user leaving MCPS or transferring to another school or office.

4. The local equipment inventory will be maintained as accurately as possible. New and donated equipment will be added when acquired. Users may not remove the inventory markings or tags from computers.

5. Lost and stolen equipment should be handled in accordance with MCPS Regulation EDC-RA: *Control of Furniture and Equipment Inventory*.

C. Systems And Applications Security

1. Users should not install software or hardware, or disable or modify security settings or measures (such as anti-virus software) installed on any computer for any purpose without the permission of the appropriate staff as outlined in the *Manual of MCPS Computer Systems Security Procedures*.

2. Users must not change the system settings without the permission of the appropriate staff as outlined in the *Manual of MCPS Computer Systems Security Procedures*.

3. MCPS software and applications may not be installed or copied to a non-MCPS computer except as specified by licensing agreements.

D. Network Security

MCPS is not responsible for all of the information found on networks outside of the MCPS organization, including the World Wide Web. MCPS does not have control over information residing on other systems or internet sites to which there is access through MCPS. Some sites and systems outside of MCPS may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

1. Users are responsible for ensuring that access to or importation of material on networks is for educational purposes.

2. Any material or information purposefully posted or linked from an MCPS system or internet site must be consistent with the educational purpose as defined in this regulation.

3. Users are responsible for abiding by the rules applicable to the computer system(s) they use, including those accessed over the Internet from MCPS equipment.

4. The only remote access approved for all users is to MCPS web pages through the Internet and to the MCPS e-mail system. Remote access to all other MCPS computer systems is not permitted except by express written authorization from the Office of Global Access Technology.

E. Conduct And Use

1. All use of computer facilities, networks, and other technology resources must be for educational purposes as defined in Section III.C. and are subject to MCPS review and may be logged and archived.

2. MCPS e-mail is for educational purposes only. All actions are subject to MCPS review and may be logged and archived. All student use of MCPS e-mail must be authorized for purposes of supporting or facilitating the learning process.

3. Students are prohibited from using unauthorized e-mail, instant messaging and chat rooms.

4. Although it is impossible to document all inappropriate conduct and use of computer facilities, the following guidelines provide examples of computer and network use infractions that are prohibited:

   a) System tampering (any unauthorized alteration of operating systems, individual accounts, software, networking facilities, and/or other programs) and/or equipment damage

   b) Decrypting passwords and/or gaining unauthorized higher level access or privileges or attempting to do so

   c) Interfering deliberately with other users

   d) Making statements or actions that are libelous, slanderous, or that harass others

e)   Using language, pictures, or other material that is obscene, vulgar, abusive, or otherwise harmful to students

f)   Knowingly introducing viruses or attempting to do so

g)   Reading, deleting, copying, forging, or modifying the e-mail of other users or attempting to do so

h)   Permitting others to use one's personal e-mail address, account, or password

i)   Using commercial advertising, chain letters, or non-educational games on MCPS systems

j)   Copying or transferring copyrighted materials and software without authorization

k)   Posting personally identifiable information about students or staff without authorization

l)   Using MCPS networks or computer systems for personal gain or any illegal activities

5.   Students are prohibited from knowingly accessing or attempting to access inappropriate material or material that is harmful to students. Student use of the Internet will be monitored by a variety of methods including, but not limited to, technology and direct supervision.

6.   All users are prohibited from knowingly accessing or attempting to access portions of the Internet that do not promote the educational, instructional, administrative, business or support services purposes of MCPS or is not related to any instruction, project, job, work assignment, task, or function for which the user is responsible.

7.   In order to prevent the unauthorized disclosure, use and dissemination of personal identifying information regarding students, students are to be educated on appropriate use of the Internet, particularly personal safety practices including, but not limited to, release of personal identifying student information and meetings with anyone to whom a student corresponded online.

8.   Any student who identifies a portion of the Internet that contains inappropriate material or material that is harmful to students which has not

been filtered through the technology protection measure is required to notify instructional staff immediately.

9. Any staff who identifies or is informed of a portion of the Internet that contains inappropriate material or material that is harmful to students which has not been filtered through the technology protection measure is required to follow the procedures as outlined in the *Manual of MCPS Computer Systems Security Procedures*.

F. Noncompliance

1. Noncompliance with the procedures and standards stated in this regulation is proper cause for disciplinary action.

   a) Disciplinary actions for employees may include a conference, warning, letter of reprimand, loss of privileges, suspension without pay, demotion, dismissal, and/or criminal prosecution.

   b) Disciplinary actions for students may include, but not be limited to, a telephone call to parents or guardians, loss of privileges, restitution, suspension, and/or expulsion, and/or criminal prosecution. (See Regulation JFA-RA and school discipline policies)

   c) Disciplinary actions for other users may include loss of privileges, and/or criminal prosecution.

2. Anyone who becomes aware of suspicious or inappropriate use of data, computer system abuse, or possible breaches of security should alert his/her instructional staff, immediate supervisor and/or the LSA. Serious infractions as set forth in the *Manual of MCPS Computer Systems Security Procedures* should also be reported to the Office of Global Access Technology.