REGULATION MONTGOMERY COUNTY PUBLIC SCHOOLS

Related Entries: BBB, EDC, EDC-RA, EGI-RA, EHC-RA, IGS, JFA, JFA-RA, JOA-RA, KBB
Responsible Office: Superintendent of Schools

User Responsibilities for Computer Systems, Electronic Information, and Network Security

I. PURPOSE

A. To ensure the security of all elements of Montgomery County Public Schools (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; and

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. An *approved electronic signature method* is one that has been approved by the superintendent and/or his designee, in accordance with this regulation and all applicable state and federal laws, and which specifies the form of the electronic signature, the systems and procedures used with the electronic signature, and the significance of the use of the electronic signature.

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

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

D. *Electronic data and information* are facts or figures contained in any electronic form.

E. An *electronic record* is information generated, sent, received, or stored in digital form in connection with the conduct of MCPS business, communicated between parties as evidence of a transaction, and preserved for MCPS documentation purposes. A record does not include information that is so transitory in character that it is not ordinarily preserved.

F. An *electronic signature* is an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign a record.

G. *Harmful to students or staff* 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.

H. *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.

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.

J. A *technology protection measure* is an Internet filtering technology 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.

K. *Unauthorized equipment* is any device that is not approved by the superintendent and/or his designee to be connected to an MCPS computer or MCPS network, including, but not limited to, personal communication and organization devices such as wireless access points, smart phones, or cell phones; gaming devices; photographic equipment; and entertainment devices such as MP3 players or iPods™.

L. 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.

IV. PROCEDURES

The following section delineates appropriate procedures in the areas of electronic data and information security, electronic signatures, 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*.

A. Electronic Data and Information 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 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. Electronic Signatures and Electronic Records

1. Electronic Signatures

Where Maryland state law, federal law, or MCPS policies or regulations require that a record have the signature of a responsible person, that requirement is met when the electronic record has associated with it an electronic signature using an approved electronic signature method.

2. Electronic Records

Where Maryland state law, federal law, or MCPS policies or regulations require a written document, that requirement is met when an electronic record has associated with it an electronic signature.

3. The signing of a record using an approved electronic signature method means that the record has been signed by a person authorized to sign or approve that record. Appropriate procedures must be used to confirm that the person signing the record has the appropriate authority to do so.

4. MCPS may make rules that do the following:

a) Identify specific transactions that the school system is willing to conduct by electronic means.

b) Identify specific transactions that the school system will never conduct by electronic means.

c) Specify the manner and format in which electronic records must be created, generated, sent, communicated, received, and stored, and the systems established for those purposes.

d) Specify control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records.

e) Identify any other required attributes for electronic records that are specified for corresponding nonelectronic records or that are reasonably necessary under the circumstances.

5. Any individual or party who makes inappropriate or illegal use of electronic signatures and/or records is subject to noncompliance sanctions as described in Section IV.G.

C. 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*.

D. Systems and Applications Security

1. Users should not install software or hardware, or disable or modify security settings or measures (such as antivirus 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.

E. 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 Information and Organizational Systems (OIOS).

F. 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 or assisting others to cause tampering by providing instructions or information on how to tamper with any MCPS system (any unauthorized alteration of operating systems, individual accounts, network-shared folder, software, networking facilities, and/or other programs) and/or equipment damage.

   b) Decrypting passwords, unauthorized capturing of passwords by using hardware devices or software applications, and/or gaining unauthorized higher-level access or privileges or attempting to do so.

   c) Interfering deliberately with other users' network access or computer use.

   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) Introducing malicious codes such as viruses or worms that cause harm or subvert the intended function of MCPS computer systems.

   g) Attaching unauthorized equipment to any MCPS computer or MCPS network without authorization from the superintendent and/or his designee.

   h) Using e-mail to harass or defraud others by sending threatening or unsolicited bulk and/or commercial messages over the Internet, or using fraudulent e-mail messages to obtain personal information for purposes of identity theft.

i) Circumventing technology protection measures, also known as network security or filtering technology.

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

k) Reading, deleting, copying, forwarding, printing, sharing, or modifying the data files of other users without authorization of the superintendent and/or his designee.

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

m) Permitting others to use one's personal MCPS network account, network folders, or password.

n) Using commercial advertising, chain letters, or noneducational games on MCPS systems.

o) Copying or transferring copyrighted materials and software without authorization.

p) Posting on the Internet personally identifiable information or false information about students or staff without authorization, using MCPS equipment or resources.

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

5. All users are prohibited from knowingly accessing or attempting to access inappropriate material or material that is harmful to students or staff. Student and staff 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 are 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 with whom a student corresponded online.

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

G. 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, restitution, 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 MCPS Regulation JFA-RA, *Student Rights and Responsibiliies,* and school discipline policies.)

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

2. Any user of MCPS computer systems should report suspicious or inappropriate use of data, computer system abuse, or possible breaches of security. School-based users should alert the principal or the principal's designee responsible for information technology. Non-school-based users should alert their immediate supervisors and the superintendent and/or his designee. Serious infractions, as set forth in the *Manual of MCPS Computer Systems Security Procedures*, also should be reported to OIOS .

Regulation History: New Regulation, August 22, 1995; revised December 13, 1999; updated office titles June 1, 2000; revised June 10, 2002; revised May 23, 2007.