REGULATION MONTGOMERY COUNTY PUBLIC SCHOOLS

Related Entries: BBB, EDC, EDC-RA, EGI-RA, EHC-RA, IGS, JFA, JFA-RA, JHF-RA, JOA-RA, KBA-RB**,** 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. In schools, the online activities of minors are monitored by staff, and through systemwide technology protection measures. 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 of schools 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. *Cyberbullying and/or electronic harassment or intimidation* means intentional conduct using electronic communication such as e-mail, instant messaging, social sites, blogs, mobile phones, or other technological methods to create a hostile educational environment by substantially interfering with a student's educational benefits, opportunities, or performance, or with a student's physical or psychological well-being, and is:

- Motivated by an actual or perceived personal characteristic including race, national origin, marital status, sex, sexual orientation, gender identity, religion, ancestry, physical attributes, socioeconomic status, familial status, or physical or mental ability or disability

- Threatening or seriously intimidating

- Occurs on a school property, at a school activity or event, or on a school bus

- Substantially disrupts the orderly operation of a school

D. *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.

E. *Electronic data and information* are facts or figures in any electronic or digital form. Examples include e-mail, instant messaging, chat rooms, texting, documents, databases, files, websites, and any other electronically stored information.

F. 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.

G. 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.

H. *Inappropriate materials* are materials that are obscene or pornographic and thus harmful to minors/students, including websites related to adult/sexually prurient content, materials that are not age appropriate, and materials with no educational purpose, as defined in this regulation or that are inconsistent with system security or MCPS policies and regulations. Inappropriate materials also may include those that promote or advance hacking, the use, distribution, and production of drugs, alcohol, and tobacco, bullying, harassment, and intimidation, criminal skills, violence or unlawful use or possession of weapons. Where the need for bona fide research or other lawful purpose is identified by staff, appropriate access may be granted.

I. *Internet access* includes all authorized methods used to connect to the Internet servers and users, and all authorized methods for providing access.

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 designed to limit or prevent access to inappropriate material.

K. *Unauthorized equipment* is any device that is not approved by the Office of the Chief Technology Officer (OCTO) and/or his designee to be connected to an MCPS computer or MCPS network, including, but not limited to, computers, tablet devices, 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 procedures required for cybersafety, cybersecurity, and cyberethics for electronic data and information security, electronic transactions and signatures, physical security, systems and applications security, network security, and conduct and use. More specific user responsibilities and procedures for computer systems security are outlined in the *Manual of MCPS Computer Systems Security Procedures* available on the MCPS website.

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 must change passwords as required and keep 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 Transactions and Signatures

Where Maryland state law, federal law, or MCPS policies or regulations require that a transaction have the signature of an authorized person, that requirement is met when the electronic record has associated with it an electronic signature using an approved electronic signature method. Procedures for authorization and use of electronic transactions and signatures are outlined in the *Manual of the MCPS Computer Systems Security Procedures*.

C. Physical Security

Computer systems equipment must be located and maintained in a secure physical environment. Users are responsible for 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. Equipment will be added to the inventory 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 must not install software or hardware, or disable or modify security settings or measures (such as antivirus software) installed on any computer or other authorized digital/electronic devices 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

All access to the MCPS network and information requires approval from an authorized MCPS authority in OCTO. User accounts or access may be removed, suspended, or revoked if it is determined the network or information access is used in violation of this or any other applicable MCPS policy or regulation.

F. Conduct and Use

Student and staff use of the Internet will be monitored by a variety of methods including, but not limited to, technology and direct supervision.

1. Users are responsible for ensuring that access to or importation of material on networks is for educational purposes as defined in this regulation.

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. MCPS does not have control over and cannot be responsible for 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.

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

6. 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.

7. Students are prohibited from using unauthorized e-mail, instant messaging, or chat rooms.

8. 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 (also known as hacking) 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, key logging, or 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 such as through denial of service (DoS) or distributed denial of service (DDoS).

d) Making statements or actions that are libelous, slanderous, or that constitute cyberbullying, harassment, or intimidation of others.

e) Knowingly accessing or attempting to access inappropriate material, as identified in III. H. above.

f) Introducing malicious codes/software 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 the MCPS network without authorization from OCTO 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, through the use of proxies, applications, or other methods.

j) Deleting, forging, modifying or reading or copying without permission 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 of schools 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 or disseminating by electronic means personally identifiable information without authorization or posting false information about students or staff, using MCPS equipment or resources.

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

9. All users are prohibited from knowingly participating in the unauthorized disclosure, use, and dissemination of personal information about minors.

10. Students are to be educated about appropriate online behavior including interactions with other individuals on social networking sites and in chat rooms, and about cyberbullying awareness and response.

11. Any user of MCPS computer systems who identifies a portion of the Internet that contains inappropriate material 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* which is available on the MCPS website.

V. NONCOMPLIANCE

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

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

2. 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 Responsibilities,* and school discipline policies.)

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

B. 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 of schools and/or his designee. Serious infractions, as set forth in the *Manual of MCPS Computer Systems Security Procedures*, also should be reported to OCTO.

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; revised July 27, 2012.