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

As noted in MCPS regulation IGT-RA, User Responsibilities for Computer Systems, Electronic Information, and Network Security and the Manual of MCPS Computer Systems Security Procedures

Students have a right to use technology provided by MCPS for educational purposes only as defined in MCPS Regulation IGT-RA, *User Responsibilities for Computer Systems, Electronic Information, and Network Security*. Computer equipment, computer services, and network access to schools and offices are provided for purposes consistent with the mission of MCPS. All actions are subject to MCPS review and may be logged and archived. Students must protect information and resources against theft, malicious damage, unauthorized access, tampering and loss, and comply with relevant state, local, and federal laws. Students do not have a right or expectation of privacy in their use of school computers. Students have the responsibility to conduct themselves in accordance with the requirements of MCPS Regulation IGT-RA and other reasonable rules and restrictions regarding electronic communications. Internet use should support education and research and be consistent with the MCPS mission.

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.

Users may only access information and/or computer systems to which they are authorized and that they need for their assignments and responsibilities. Chromebooks remain in the school at all times.

The Internet may not be used for the following:

- Viewing information that is deemed inappropriate, violent, or otherwise potentially offensive and does not serve an educational purpose.
- Accessing or disseminating unauthorized information
- Sharing passwords, accounts, and e-mail addresses
- Illegal activities
- Sending unsecured information that may be confidential or private

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. Users are responsible for their own individual accounts. Users must log off all systems before leaving a computer workstation or allowing others to use it. It is the responsibility of every user to be aware of and following security procedures in accordance with the MCPS regulation, IGT-RA. MCPS is not responsible for information that may be lost due to system failures or interruptions. Users can save information to a secure location such as student shared folder or removable disk.

Network Security

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.

Conduct and use

Student use of the internet will be monitored by a variety of methods including, but not limited to, technology and direct supervision. 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. Students are prohibited from using unauthorized e-mail, instant messaging, chat rooms, or web-based programs/apps.

Computer and network use infractions that are prohibited include:

- 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 and equipment damage.
- Interfering deliberately with the other users' network access.
- Making statements or actions that are libelous, slanderous, or that constitute cyberbullying, harassment, or intimidation of others.
- Knowingly accessing or attempting to access inappropriate material, not related to MCPS educational purposes.
- Using email 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.
- Deleting, forging, modifying, reading or copying without permission the e-mail of other users or attempting to do so.
- Permitting others to use one's personal MCPS e-mail address, account, or password.
- Permitting others to use one's personal MCPS network account, network folders, or password.
- Using commercial advertising, chain letters, or non-educational games on MCPS systems.
- 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.
- 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.
- Students are expected to use school technology devices such as computers with care. If a student break, crack or destroy school equipment such as a computer, the school may decide to request financial reimbursement from the child's family to purchase a new device.
- Downloading apps onto chromebooks without teacher permission.

Noncompliance

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

Infraction

Computer Abuse; examples include but are not limited to the following;

- Hacking into MCPS/CESC network
- Hacking into school network
- Intentional viewing/distribution of inappropriate material
- Misuse of the network privileges
- Misuse of e-mail privileges
- *Bullying, see JFA-RA*

Written electronic abuse/harassment or threats