Department: Technology
Policy Number: TCH-A002
Effective Date: 4/17/06

ADMINISTRATIVE POLICY

The online version of this policy is official. Therefore, all printed versions of this document are unofficial copies.

TECHNOLOGY ACCEPTABLE USAGE

Clarksville-Montgomery County School System (CMCSS) has developed an extensive technology infrastructure, including hardware, software and connectivity equipment toward the purpose of improving the District's educational, administrative and clerical functions. The significant ongoing investment in technology is in part justified by two promises:

To better prepare students for life and work in an ever-changing environment filled with technology.

To increase the productivity of district personnel.

This investment must be protected from potential misuse and abuse. CMCSS uses a Children's Internet Protection Act (CIPA) compliant solution to prevent student access to materials the district deems harmful and to block internet access to inappropriate sites, including child pornography and obscenity. This policy clarifies roles and responsibilities in the use of CMCSS technology, both hardware and software, to preserve the integrity and usability of these resources to benefit and serve all clients. Failure to comply with this policy may result in the suspension of privileges, internal investigation, disciplinary action, and/or criminal prosecution. CMCSS must be strict in these matters, not only because of the value of the resources, but also to ensure a safe and productive learning and working environment for our students, faculty, and staff. These rules apply to all CMCSS computing resources.

The intent of this policy is to raise awareness about what is an appropriate, ethical, legal and professional use of a valuable shared resource, not to enumerate all uses that are or are not appropriate.

Acceptable use of CMCSS technology resources is based on common sense, common decency, and civility applied to the networked computing environment. There is no expectation of privacy by users when using the internet or electronic communications. The district reserves the right to monitor, inspect, copy, review, and store (at any time and without any prior notice) all usage of district computers, computer systems, and electronic communications, with the exception of personal banking/health information. The district may access district-owned devices for maintenance, upgrades, and at any time there is suspected abuse of district policy. Appropriate use of these resources must be consistent with the purpose for which the computer/security accounts (log-ins) were originally requested and provided. Privately owned devices connected to a CMCSS network, whether wired or wireless, are subject to monitoring, inspection, confiscation, and investigation. Attaching privately owned devices to a CMCSS network is a privilege and is subject to all provisions within the Technology Acceptable Usage Policy.

Expressly prohibited are any uses, which may result in cancellation of user privileges:

Which benefit any political, religious, or commercial organization.

Which are illegal, obscene, or for profit.

That adversely affect the reputation or image of CMCSS.

Of unauthorized attempts to log in to any network as a system administrator.

Of unauthorized disclosure of personal information (social security number, tax identification number, credit card information, medical information, etc).

Of any malicious attempt to harm or destroy CMCSS data, data of another user, or other CMCSS computing facilities or equipment.

Downloading, installation, or use of programs that infiltrate computing systems and/or damage software components.

Intentionally disrupting network traffic, crashing the network, or gaining unauthorized access to the files of another user.

Use of the network to personally attack, harass, threaten, bully another person, or publish false information.

Use of inappropriate language in any type of communication, including, but not limited to, language that is illegal, vulgar, profane, abusive, or threatening.

Any access to the network through false identity including anonymous communication, falsifying, concealing, or misrepresenting the user's identity or sharing network accounts.

Mass e-mailing of unsolicited and unwanted messages ("spamming"), including text, software, video, and images.

Network Security and Internet Connectivity

Network passwords and account information are only given to authorized personnel.

Employees and students with valid CMCSS credentials are required to use only the appropriately assigned CMCSS network and equipment. Users without valid CMCSS credentials requesting network connectivity are authorized only to use the CMCSS guest network. CMCSS devices designated for use of guest services is required to maintain guest network connectivity.

Non-CMCSS contracted personnel performing approved services for CMCSS should request network access to the contracted WiFi network. This request should be placed through the work order system by a CMCSS staff member.

All users must always secure their computer(s) and network log-in before leaving their room or office. Do not allow anyone to use your computer, account, or credentials (with the exception of CMCSS Technology Department personnel). The individual assigned an account is responsible for any and all transactions entered under that account login.

Use of software designed to gain passwords or access beyond the rights assigned to a user or computer is strictly prohibited. The intent to obtain unauthorized access is a violation of State and Federal law. Violators will be prosecuted.

Any violation of the above must be reported immediately to supervisory personnel in the room (in case of students) or the Chief Technology Officer (in case of staff).

Workstation/Computer Use

All employees and students are prohibited from installing any software on any computer unless authorized in writing by the Technology Department management. Illegal download or use of copyrighted software, music, videos, pictures, or other files is prohibited.

Any application designed to limit access to students or staff, other than those used by the Technology Department is prohibited.

Changing or tampering with any computer's system configuration is prohibited.

Any action which violates Board or Administrative policies, local, state, or federal law is prohibited.

Computers found to be tampered with or computers with unapproved software or files will be re-formatted and restored to compliance.

All computer equipment loans must comply with the district Equipment Loan Agreement (BUS-F012).

Viruses and Virus Protection

The CMCSS Technology Department will provide all virus protection and related software for all CMCSS devices. Virus protection and related software will be installed by authorized Technology Department personnel.

Do not open any suspicious e-mail attachments. Never send anyone e-mail you suspect may contain a virus. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted.

There are many virus hoaxes. Never delete system files from a computer in order to remove a potential virus without first checking with the Technology Department.

If you suspect your computer may contain a virus, contact the Technology Department immediately.

Copyright Policy

All students and employees will comply with all applicable copyright laws in the use of all media and materials and model legal and ethical practices related to technology. CMCSS students may create work in the classroom individually and with the assistance of CMCSS employees. Such work is owned by the student upon creation. Students and their legal guardians agree that any and all such student created work may be used by CMCSS in its publications, including but not limited to websites and other distributed materials promoting CMCSS, provided that such original student work will be reported as having been created by the student. Any student who desires not to authorize CMCSS to publish his/her work or to publish his/her name as the owner of such work, shall provide written notice to

CMCSS that such authorization is not granted (Added from Ownership of Student Created Work, INS-A070).

E-mail

The CMCSS e-mail systems have been provided for the communication of employees, board members, and students. Responsible and ethical use of the e-mail system is required and should reflect professional standards. The e-mail system may not be used for personal gain, expressing political, religious views, in any illegal, offensive, or unethical manner, (to include bullying-related acts). Personal e-mails should be limited. All e-mail is the property of CMCSS and should not be considered private or confidential and is subject to review at any time by authorized CMCSS personnel.

All district employee emails must adhere to the signature guidelines provided by the Technology Department. The only valid email signatures are those created using the following webpage: https://employees.cmcss.net/Home/EmailSignature

Cell Phones

This policy is meant to ensure the safe operation of both company vehicles and private vehicles while an employee is conducting business on work time. The use of a cell phone while driving may present a hazard to the driver, other employees, and the general public.

CMCSS employees are not permitted to use cell phones while operating a CMCSS vehicle, except as referenced in administrative policy OPS-A006.

In addition, employees must adhere to all local, state, or federal rules, regulations, laws or other ordinances regarding the use of cell phones while driving personal vehicles. Employees should check with local authorities if they are unsure whether the use of a cell phone while driving is prohibited in a particular area. It is recommended that employees not use hand held cell phones for business purposes while driving personal vehicles. Employees may use hands-free cell phones to make business calls in accordance with the law.

CMCSS provides cell phones to some employees for district business purposes. Any personal use of the device should be limited in both time and nature so as not to interfere with work responsibilities. If any employee abuses this privilege, the employee will be responsible for reimbursement to the school system. Individuals assigned a CMCSS cell phone are accountable for any and all activity on the device. Any action that is deemed for commercial gain or that violates Board or Administrative policies, local, state, or federal law is prohibited.

Server Software

Only CMCSS Technology Department or authorized personnel will install, modify, or access software on servers.

When a suspected violation of the above statement becomes known, the incident should be reported to the appropriate supervisor and the Chief Technology Officer.

Technology Abuse

In the event a CMCSS employee becomes aware of the misuse or abuse of CMCSS technology, they should act in accordance with the district's Computer Abuse Discovery Procedure (TCH-P026).

Associated Documents: Internet Usage Agreement (TCH-F018)
Equipment Loan Agreement (BUS-F012)
Computer Abuse Discovery Procedure (TCH-P026)
Children's Internet Protection Act
User Password Policy (TCH-A003)Use of Portable Digital/Electronic Devices While Operating CMCSS Vehicles (OPS-A006)
Employee Handbook (HUM-M001)
Harassment, Intimidation, Hazing, and Bullying (INS-A016)
Student Code of Conduct (STS-M001)
Ownership of Student Created Work (INS-A070)

Revision History:

Date:	Rev.	Description of Revision:
4/17/06		Initial Release
6/30/08	A	Add "computer systems, and electronic communications" to fourth paragraph, third sentence.
9/17/08	B	Second sentence in second paragraph added to comply with TN Senate Bill No. 3702, obscene added to second sentence under Expressly prohibited are any uses, add associated documents
10/23/08	C	Add fifth sentence under Expressly prohibited are any uses, add second paragraph under Internet Connectivity and add Children's Internet Protection Act to Associated Documents.
07/08/09	D	Add Computer Abuse Discovery Procedure reference.
12/10/09	E	Change form number in associated documents from TCH-F021 to BUS-F012.
09/27/10	F	Added last sentence to "Internet Connectivity" section.
7/18/11	G	Added Children's Internet Protection Act to second paragraph. Inserted "value of the resources" in place of "real value of the facilities" in second paragraph. Changed wording of last sentence in second paragraph. Added last two sentences in fourth paragraph. Deleted "will result in cancellation of privileges" from first paragraph on page 3. Inserted "could result in cancellation of privileges". Under Network Security, changed 2nd paragraph. Miscellaneous grammatical changes. In #2 under prohibited network activities, added "not listed on CMCSS software approval list is prohibited". Added reference to BUS-F012 in Workstation/Computer Use. Internet Connectivity – added "wired and wireless network" in second sentence. Cell Phones – Changed third paragraph.
3/5/12	H	Updated Cell Phone section to reflect the attached information, added OPS-A006 and HUM-M001 to Associated Docs.
7/1/14	I	Update email section to student email accounts; Add bullying-related acts to Internet Connectivity section and Harassment, Intimidation, Hazing, and Bullying (INS-A016) to Associated Documents
1/5/15	J	Additional wording added under Copyright Policy and Email; minor grammatical changes
11/30/15	K	Added link to valid email signature template under Email section.

9/18/18		Updated hyperlinks. Not a revision.
12/10/18	L	Changed IT to Technology throughout. Added disciplinary actions to list of possible consequences. Replaced employee with personnel throughout. Added fourth paragraph under cell phone section.
8/30/21	M	Added examples of unauthorized disclosure of personal information on page 2.
4/14/22	N	Changed "a future filled with technology-laden changes and use" to " an ever-changing environment filled with technology use" on page 1 Changed "current and future staff" to "district personnel" on page 1 Added ",with the exception of personal banking/health information" on page 1 Changed "of suspected abuse of district policy" to " there is suspected abuse of district policy" on page 1 Added section about Non-CMCSS contracted personnel access to the wifi on page 2 Deleted extra spacing Deleted " for voice communications, e-mail communications, or text communications" on page 4 Deleted "motor" on page 4 Changed "(Ref. OPS-A006)" to "except as referenced in administrative policy OPS-A006 on page 4 Changed "The Clarksville Montgomery County School System" to "CMCSS" on page 5. Deleted "due to the nature of one's position" on page 5. Changed "authorized Technology Department personnel" to "CMCSS Technology Department or authorized personnel" on page 5. Changed " install software to servers" to "install, modify, or access on servers" on page 5. Changed "he or she" to "they" on page 5.
3/17/23	O	Grammatical/spacing errors, updated expressly prohibited uses, updated network security, combined internet connectivity with network security, updated workstation/computer use, added INS-A070 as referenced document, updated email section, updated server software section.

*****End of Policy*****