



Department: Human Resources
Policy Number: HUM-A034
Effective Date: 11/3/09

ADMINISTRATIVE POLICY

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

SCHOOL DISTRICT COMMUNICATION SYSTEM USAGE

This policy covers employee use of Clarksville-Montgomery County School System communication systems, including computers, computer-based communication software and peripherals, facsimile, e-mail, internet, telephone, and voice mail.

- 1. Official use.** CMCSS communication systems, including all peripherals and software, are intended for official use. Use of all technology hardware, software and connectivity equipment is detailed in CMCSS Technology Acceptable Use Policy (ref. [TCH-A002](#)). Employees may not use a password, access a file, or retrieve any stored communication without authorization. While intended for official use, CMCSS recognizes there are instances where private communication through school district communication systems may be desirable and/or necessary. However, such private communication must be held to a minimum and must be of a nature as to contribute to the employee's performance of his or her job. For example, a brief phone call to the employee's home to pass information would be appropriate while a social conversation with one's friend would not be appropriate. Employees may not connect to "chat rooms," message boards or other similar public forums using CMCSS communication systems for personal purposes.
- 2. No offensive language.** CMCSS maintains a workplace free of harassment and is sensitive to the diversity of its employees. Employees are prohibited from using computers, the internet, facsimile, voice mail and the e-mail system in any way that is disruptive, harmful to morale, or offensive to others on the basis of race, sex, religion, ancestry, disability, or any other basis protected by law. Misuse of these facilities also includes but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.
- 3. Solicitation.** CMCSS communication systems may not be used to solicit others to promote personal events or causes, commercial ventures, religious or political causes, outside organizations, or other unofficial matters. Employees may not upload promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation. Employees may not transmit insubordinate messages, or messages that are contrary to CMCSS policies. Employees may not access CMCSS communication systems from a remote location without authorization, and must do so solely for official purposes.
- 4. Official Employer Records.** All data that are composed, transmitted, or received via CMCSS communication systems are considered to be the property of CMCSS, and are subject to monitoring, and as such, are also subject to disclosure to law enforcement or other third parties. Additionally, all correspondence in the form of e-mail may be a public record under the public records law and may be subject to public inspection under TCA § 10-7-512, as amended.
- 5. Duplication or downloading of software.** CMCSS purchases and licenses the use of various communication systems software programs solely for official purposes and does not own the copyright to this software or its related documentation. Employees are prohibited from illegally duplicating software and its related documentation, and downloading software from the internet without the authorization of CMCSS (ref. [TCH-A002](#)).



Department: Human Resources
Policy Number: HUM-A034
Effective Date: 11/3/09

6. **Employer access to data.** CMCSS reserves the right to read the contents of e-mail messages or listen to the contents of voice messages for any purpose. Communication systems may be monitored, searched and reviewed by CMCSS or its agents at any time.
7. **Publication of e-mail addresses.** Employees may not publish e-mail addresses outside CMCSS unless it is necessitated by the employee's job function. Under no circumstances should an employee publish the e-mail address(es) of other employees without the employee's expressed consent.
8. **Passwords.** Employees should notify their respective supervisors of all passwords and password changes associated with CMCSS communication systems.
9. **Authorization to monitor, search, and review personal communications required.** 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 (ref. [TCH-A002](#)). Requests for such activities should be submitted in writing and undertaken only upon receipt of written authorization. The Chief Human Resources Officer is the authorizing authority to approve requests to monitor, search, and review personal communications on CMCSS communication systems not covered by the CMCSS Technology Acceptable Usage Administrative Policy (ref. [TCH-A002](#)).
10. **Notification of violations.** Employees should notify their respective supervisors of any known violations of these provisions. Violations involving technology equipment should be handled per Computer Abuse Discovery Procedure (ref. [TCH-P026](#)). Failure to disclose known policy violations may subject the employee to disciplinary action.

Associated Documents: Technology Acceptable Use Policy ([TCH-A002](#))
Computer Abuse Discover Procedure ([TCH-P026](#))

Revision History:

<u>Date:</u>	<u>Rev.</u>	<u>Description of Revision:</u>
5/09/05		Initial Release
11/3/09	A	Reference CMCSS Technology Acceptable Use Policy in 1, 5 & 9 and Computer Abuse Discovery Procedure in 10, clarify 9.

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