

Mott Community College Acceptable Use Administrative Policy for Computers, Computer Networks, and Communication Systems Effective July 1, 2009

As an employee of Mott Community College, heretofore referred to as "The College," all college employees are required to adhere to the following Acceptable Use Policy regarding the use of our computer, network, communications, and telephone equipment, heretofore referred to as "The Network". This document functions in conjunction with related College Policy.

- I. Employees' right to privacy of communications when using The Network is not guaranteed. The College reserves the right to monitor all communications that use or are stored on The Network as it deems necessary.

- II. All data, software programs, and information stored on The Network is the sole property of The College. Users must respect the legal protection of applied programs, data, photographs, music, written documents and other material as provided by copyright, trademark, patent, licensure and other proprietary rights, unless otherwise specifically excluded or modified in a collective bargaining agreement or written agreement between The College and The Employee.

- III. College employees will not use The Network to transmit any material (via e-mail, uploading, posting or otherwise) that does the following:
 - a. Intentionally or unintentionally, violates any applicable local, state, national or international law, or conducting any activity that exposes The College to potential litigation or expenses or violates any other College rule or regulation
 - b. Threatens or encourages bodily harm or destruction of property
 - c. Harasses or discriminates against another person in any way or is harmful to students, employees, agents, or minors
 - d. Is malicious, fraudulent or misrepresentative in purpose, including, but not limited to, spreading false information about a student, employee, agent, or minor
 - e. Is related to pornography of any type or uses profanity, obscenity, discriminatory language, vulgarities or other inappropriate language or graphics.
 - f. Is related to gambling

- IV. The College is not responsible for damages or loss of personal files stored on The Network. Additionally, while attached to a College-owned computer, personal equipment may be subject to incidental access while the College is

maintaining College-owned devices. For example, The College has the same authority to access a non-College-owned hard drive attached to College-owned equipment as they have for accessing College-owned equipment.

- V. Employees must not use The Network or any other resources owned by The College for personal commercial purposes or financial gain. Employees must not excessively use the communications or telephone system for personal transactions.
- VI. Employees are expected to take all necessary steps to safeguard Proprietary and Confidential Information that resides on the network from release to unauthorized parties. Proprietary Information includes, but is not limited to, College financial information and/or other information that could damage The College's business should it be released to an unauthorized party. Confidential Information includes, but is not limited to, customer information, student information, employee information, and information relating to The College. This includes securing and safeguarding data stored on portable devices used to transport data, such as flash drives.
- VII. Employees must not use The Network to knowingly distribute spam, chain letters or other mass unsolicited mailings.
- VIII. Employees must not use The Network for any activity which adversely affects the ability of other people or systems to use The Network. This includes, but is not limited to:
 - a. Denial of service attacks against another network by routing or relaying traffic between unknown third parties, worms, viruses or other intrusive services
 - b. Interference with or disruption of other network users, services or equipment
 - c. Through action or inaction, to allow The Network to be configured in such a way that gives a third party the capability to use their network in an illegal or inappropriate manner
 - d. Attempts to penetrate security measures of The Network via computer software, hardware or other systems whether or not the intrusion results in the corruption or loss of data
 - e. Employees must not install or use game software, entertainment software, screen saver or any other software that interferes with The Network or their desktop computer unless necessary for their job function at The College
- IX. Employees must respect the privacy of others and shall not intentionally seek information on, or represent themselves as another employee unless explicitly authorized to do so by that employee or supervisor.
- X. Employees must not disclose any Login IDs or passwords to any person except as directed by their supervisor. The authorized user of the account is responsible for all activities associated with the account.

- XI. Employees are allowed to disseminate information using The Network under the following conditions:
 - a. For Proprietary Information, employees must get permission from their supervisor before communicating this information to any third party, including verbal, written, or through The Network.
 - b. For Confidential Information, employees must get permission from their supervisor before communicating this information to any third party, including verbal, written, or through The Network.

- XII. Violations of the policies set forth in this document will result in disciplinary action in accordance with the appropriate Collective Bargaining Agreement clause(s) regarding disciplinary procedures. The resulting action may include but is not limited to the following: termination of use, written discipline, suspension, or termination of employment from The College and/or legal action taken against the Employee by The College. All investigations shall be conducted under the jurisdiction of the Office of Human Resources and/or an independent investigator if necessary.

Questions Related to Acceptable Use Policy

Q. Will administrative access take place without just cause? If no, is the individual notified?

A. Employees' computers and files will only be accessed when there is a cause for doing so identified by HR via the person's supervisor. Files are not randomly accessed.

Q. Define "Just Cause."

A. Just cause is a "term of art" in labor relations. It refers to the standards that must be present when a supervisor disciplines an employee under a labor agreement that provides for just cause. This is explained in detail in the following document:
http://www.mcc.edu/hr_protected/pdf/supervisors_investigations.pdf.

Q. Will an individual be warned if their usage inadvertently breaks the usage policy?

A. Yes.

Q. Who will be responsible for reporting games, personal software, etc., on other's computers?

A. Employees who discover inappropriate use of College resources or violations of any College policy should report it to their supervisor or another manager.

Q. Will all e-mail be read? If so, by whom?

A. No, unless there is a cause for doing so which has been validated by the CHRO or another member of the Executive Cabinet.

Q. Does the Acceptable Use Administrative Policy (AUAP) prohibit sending/receiving jokes via e-mail?

A. All faculty and staff are expected to exercise discretion when it comes to the sending/receiving of e-mails. Because of their nature, it would be inappropriate to send certain types of jokes. The occasional tasteful joke shared with a close circle of work friends is not an issue, however inappropriate materials, multi-forwarded e-mails that could be interpreted as spam, etc., are examples of the types of actions that are prohibited under the acceptable use policy.

Q. Are we accountable for e-mails we receive that may be in violation?

A. You will not be held responsible for unsolicited e-mails you receive.

Q. If I check my Yahoo or other personal e mail account on a Mott computer, can/will the College read my e-mail?

A. The College is unable to access or view e-mails retrieved from remote or web-based access.

Q. What are acceptable and non-acceptable sites?

A. As stated in the AUAP, sites (including but not limited to) related to pornography of any type or uses profanity, obscenity, discriminatory language, vulgarities or other

inappropriate language or graphics would be considered non-acceptable. All employees are expected to exercise common sense and good judgment.

Q. If we stumble across an inappropriate website that we don't know about, what are the ramifications?

A. You will not be held responsible for websites that you open accidentally.

Q. What is the status of incoming web information such as washingtonpost.com, nytimes.com, or politics1.com?

A. Those are considered acceptable when access is related to your job or little or no work time is spent keeping informed of current events.

Q. Can you download music via iTunes on your lunch hour?

A. The purchasing of music via download will be acceptable within reason, provided it does not interfere with the functionality of your computer or place a burden on the network.

Q. Will I be able to listen to satellite or internet-based radio (XM Radio, Sirius, etc.) while at work?

A. All computers are equipped with a limited and prioritized amount of Internet bandwidth. While the streaming of music is not prohibited, employees should be aware that it can cause a drain on that bandwidth, resulting in slower network access, especially during the Fall and Winter semesters when usage is at its highest.

Q. Does the AUAP include my home computer since I access my e-mail from home?

A. While the AUAP does not apply to your personally owned hardware, the access and/or utilization of College resources (i.e., College network drives, Intranet, Datatel, MCC-provided dial-in or VPN tunnel capabilities, etc.) is subject to the AUAP. If you are using dial-up service, you will automatically be subject to the Merit Acceptable Use Policy. You may also be subject to any rules or guidelines set forth by your personal Internet Service Provider.

Q. Is my desktop considered part of the Network?

A. Yes, if it is College-issued it is therefore College-owned and subject to the AUAP.

Q. My college-issued laptop is kept at home, where my children sometimes use it to check e-mails or instant message their friends? Is this okay?

A. College-issued equipment should be viewed as an employee resource rather than for family use. Employees are strongly advised against allowing family members equipment access, as it may result in the downloading of viruses or inappropriate material(s), or the damaging of the equipment.

Q. Will employees be required to sign an acceptable use document?

A. No but you are obligated to be aware of the policy and to follow it.

Q. Who does the supervisor report the violations of this policy to?

A. Reports of possible violations are to be reported to the Office of Human Resources. If a possible violation involves HR staff, it should be reported to the President

Q. What assurance do we have that Union business will be secure on the computer?

A. In terms of physical safety, all data remains as safe as it was before the implementation of the AUAP, therefore no assurances can be given that any file cannot be altered, corrupted, or deleted in some way. The intention of the AUAP is not to grant supervisors or administrators the right to access computers without a valid reason. Should any individual and/or group feel their confidential information is in potential jeopardy, they may want to create backup files or utilize portable memory devices, such as flash drives.

Q. Does Article XI, Section (b) [obtaining permission from a supervisor before communicating confidential information to a third party] include attorney contacts in reference to matters such as student situations that are under litigation or where legal expertise is indicated? Does every contact have to be cleared by supervisor even when the supervisor is aware of the situation?

A. No to both questions. To elaborate on the first question, an attorney would not be considered a third party if operating as an agent of the College.

Q. What is considered "excessive use" for personal transactions?

A. Again, employees are asked to use proper judgment. While there is no exact time limit that would qualify as "excessive," common sense would dictate that a disproportionate time spent tending to personal transactions as opposed to work could be considered a violation, excluding any emergency or extenuating situation. Supervisors are expected to investigate possible infractions and make an appropriate judgment call about the situation, given all of the facts, including extenuating circumstances.

Q. Is there a definition of "false information," as referenced by Article III, Section (d) [prohibiting College employees from using the Network to spread false information about a student, employee, agent, or minor]? Students going through the academic complaint process often misrepresent their situation and claim we have "false information" about their situation then go on to litigation.

A. In this particular instance, there is a difference between malicious dissemination of information known by the sender to be untrue, and a difference in perception of the details surrounding an incident. The section of the AUAP that this question refers to deals with the former, not the latter.

Q. I have an employee who frequently sends huge floods of e-mail to one or more individuals* throughout the course of a day (15-60 messages). Some may consider this as harassment. Does this type of activity fall under the acceptable use policy?

(*These individuals are other MCC employees.)

A. If the received e-mails are unsolicited, it could be viewed as harassment under the AUAP, however it is hoped that a situation such as this can be resolved by simple conversation with the sender, rather than by lodging a complaint.

Q. Will there be a maximum number of e-mails per person – sent, received or stored?

A. Each employee possesses a specific amount of space for e-mails. You will be notified if you begin to reach your limit, which is based on volume as a whole, rather than a specific count.

Q Am I allowed to send/receive e-mails from my children who live out of state?

A. Yes.

Q. Can employees use live chat mechanisms (like MSN Messenger or Yahoo Messenger) to communicate with employees in the College?

A. Live chat and instant messaging programs are allowed, however employees are reminded to use common sense and good judgment, as transcripts from messaging conversations may be copied and forwarded like any other text document. Use of such programs should also not interfere with any employee doing his/her job.