Mountwest
Community & Technical College

Office of the President

Mountwest Administrative Procedure

Information Technology Acceptable Use

This procedure sets standards of acceptable use of the information technology environment at Mountwest Community & Technical College (MCTC). MCTC has contracted with West Virginial Network (WVNET) to provide certain IT services and solutions to MCTC students, faculty, staff and MCTC affiliates. Therefore, all information technology related services provided by WVNET are incorporated within this procedure.

Procedure:

Introduction Information technology is playing an increasingly important role in the life of each individual, and consequently to the Mountwest Community & Technical College (MCTC) community. Access to these finite resources is a privilege and is provided with an expectation of responsible and acceptable use. In addition to the principles and guidelines provided in this procedure, institutional policies along with certain federal, state and local regulations apply to the use of the information technology environment (ITE).

General Principles and Guidelines The basic premise of this procedure is that responsible and acceptable use of the MCTC ITE does not extend to whatever an individual is capable of doing. Instead, certain principles provide a guide to users regarding responsible and acceptable behaviors and users are responsible for knowing and understanding them. These principles and guidelines include, but are not limited to:

- The MCTC ITE was funded and developed for the sole purpose of promoting and supporting the mission of the College.
- Authorized users of the MCTC ITE, or College sponsored IT resources including Microsoft, Zoom, ConnectYard, and various enterprise software solutions, are those individuals who have been granted a username and password. The username and password combination is your identity and license to access and use the components of the MCTC information technology environment for which you are specifically authorized.
- Authorized users will abide by institutional policies and procedures along with applicable local, state and federal regulations.
- The resources of the MCTC ITE are finite and shared. Appropriate and responsible use of these resources must be consistent with the common good. The ITE may NOT be used for commercial or profit-making purposes.
- The College reserves the right to limit access to the MCTC ITE when investigating cases of suspected abuse or when violations have occurred.
- The College does not monitor or generally restrict the content of material stored on or transferred through the components of the ITE. Use of the ITE is a privilege and not a public forum, therefore MCTC reserves the right to restrict or deny usage of the ITE when such usage does not promote or support the mission of the College.
- Users must adhere to the ethical standards governing copyright, software licensing, and intellectual property.
- Personal web pages and/or social media channels may NOT contain the official MCTC logos.

- Unauthorized interaction with ITE components is prohibited; unless pre-approved for College Staff related duties and responsibilities or for College Faculty/Student related educational activities; Including but not limited to:
    - Scans of ports, computers, and networks.
    - Attempts to uncover security vulnerabilities, circumvent data protection schemas, or alter computing/network components or configurations.
    - Use of College resources, networks, system identification numbers, or names that are not assigned for one's specific use to gain unauthorized access to any network device, computer system, or software solution.
    - Use of computers to run software or services that may negatively impact management, reliability or integrity of the network and/or one of its components. The College is permitted to disconnect any computer from the network should this activity occur.

Enforcement Violation of these guidelines constitutes unacceptable use of information resources, and may violate other institutional policies and/or state and federal law. Suspected or known violations should be reported to the appropriate MCTC Administrator and/or Information Services department. MCTC is authorized to engage in investigations and apply certain penalties to enforce this policy. The appropriate authorities and/or law enforcement agencies will process violations. Violations may result in revocation of computing resource privileges to any or all of the components of the ITE, academic dishonesty proceedings, faculty, staff or student disciplinary action, or legal action.

The maintenance, operation, and security of computing resources require responsible MCTC and/or WVNET personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to the West Virginia Access to Public Records Act, other applicable state and federal laws, and the needs of the College to meet its administrative, business, and legal obligations.

Commentary: Introduction and analogies

The Information Technology Environment discussed above consists, not only, of the superficial wires, equipment and devices of the data, voice, video, and more conventional information networks on our campuses and the world but also the setting created by the integration of these technologies into our everyday life situations. In this respect the whole is much greater than the sum of the parts and thus the effect of inappropriate use of this resource can be much greater than might be imagined. This should not be a cause for hesitation about its use but merely a call for thoughtful consideration of action.

In describing the responsibilities and acceptable behaviors related to the Information Technology Environment, certain analogies can be drawn. Social norms, behaviors, and responsibilities associated with the use of electronic communication, publication, media, and access authorization are no different than the conventional mediums with which we are all familiar, i.e.,

- Email or electronic mail is just another form of mail or communications,
- Posting to social media sites is the same as posting a notice or comment on a bulletin board, newsletter, letter to the editor, call to a talk show, etc.,
- Participating in a chat group is the same as participating in discussions anywhere a group might congregate face-

to-face e.g. in a class, the student center, recreation room, lounge, church group, etc.,

- Creating a WWW or World Wide Web presence is publishing (i.e., making public) your own magazine, memoirs, diary, biography, press release, newsletter etc. Consequently, you are not only, typically, the author but also, perhaps more importantly, you become the editor and publisher and are responsible for your publication from a legal standpoint. Even though MCTC is not the publisher, editor, or author it is the provider of the resource and, as such, is associated with your publication. Therefore, MCTC maintains the right to restrict or deny use of this resource when usage does not promote or support the mission of the College or the State of West Virginia.
- MCTC User ID and password combinations are your identity and license to use and access limited portions of the IT environment. In this sense they are like your MCTC identification card or a driver's license. Impersonating another individual, or allowing another to impersonate yourself is not acceptable behavior.
- The computing systems used for mail, **WWW,** and other technologically augmented services are similar to a classroom, or assigned work or office space. The space (and some of the content) belongs to MCTC and the State of West Virginia but other personal items in the room belong to you. In this sense MCTC has an obligation to provide a reasonable amount of security to protect your personal property but cannot assume full responsibility for it nor guarantee full privacy (if you are concerned about the inadvertent disclosure of information you should protect these items in another way).

Similarly, as in your classroom or office space, in the course of normal maintenance of the IT environment, certain information may be seen by those attending to the maintenance. All employees are instructed that the disclosure of this information is a punishable offense (as is the willful intrusion without cause).

Also, in a similar manner, you are allowed the use of certain space and accouterments and are expected to utilize them in a responsible manner by taking proper care, providing reasonable security, and respecting the property and privacy rights of others occupying similar spaces and their assigned, and private resources.

Common Forms of Violations Although most users strive for acceptable and responsible use of the ITE, inexperienced users may unwittingly engage in behaviors that violate the principles and guidelines of responsible and acceptable use. To that end, this section outlines some of the more common forms of violations that occur. These examples should not be interpreted as an exhaustive list of violations. Questions regarding the appropriateness of specific behaviors should be directed to the Chief Information Officer.

- Furnishing false or misleading information or identification in order to access another user's account
- Using another person's username/password or letting someone else use your username/password
- Investigating, reading or attempting to access another user's files without permission
- Attempts to access or manipulate certain components of the information technology environment without authorization
- Alteration of software, data, or other files without authorization
- Disruption or destruction of equipment or resources
- Using subterfuge to avoid being charged for computer resources or deliberate, unauthorized use of another user's account to avoid being billed for services

- Copying or attempting to copy data or software without authorization
- Sending email or a software program which will replicate itself or do damage to another user's account
- Interfering with the legitimate work of another user
- Sending abusive, harassing, or obscene messages
- Viewing or listening to objectionable, obscene, pornographic, or harassing material in public areas
- Excessive recreational use of resources
- Sending chain letters or unauthorized mass mailings or transmitting a crippling number of files across a network
- Sending hoax messages or forged messages, including messages sent under someone else's username
- Any activity or action that violates the MCTC Student Code of Conduct or Policies, faculty/staff policies and regulations, or federal, state, or local laws.

Effective Date: November 12, 2009
Date Updated: March 11, 2011
Date Updated: April 30, 2020
Approved by: Mr. Michael Sellards, Interim President