CODE OF CONDUCT FOR USERS OF MCC COMPUTER SYSTEMS

Individuals who use MCC computer facilities and systems must assume the responsibility for using these resources in an appropriate manner for college related work only. Misuse of computer facilities is considered a violation of College policy and may also be a violation of state and federal law. Please note that MCC computers are public access computers where you should have no expectations of privacy.

Individuals using MCC's computing facilities are NOT permitted to:

- Copy, download, change, distribute or modify any computer programs (in part or whole), subroutines, graphics, etc… from a website, textbook or another individual without the written consent or permission of the author. This may be considered plagiarism and/or a violation of copyright and patent laws. Examples include: MP3, DVD, WAV, WMA, AVI, ASF, VIV etc…
- Use MCC facilities and systems for the purpose of advertising or running an organization or business
- Sending, viewing and/or printing lewd or pornographic materials or other related activities unless directly authorized, in writing, by an instructor and the coordinator of the learning environment.
- Participate in any form of chat room, unless otherwise authorized by your instructor or the coordinator of the learning environment.
- Play or download any type of computer games or entertainment activities.
- Reveal your password to anyone including faculty and staff, or let another person use their account. You are responsible for what is done with your account.
- Change, copy, delete, distribute, read, or otherwise access files without the permission of the owner. If it's not yours, don't touch it.
- Prevent others from accessing systems or unreasonably slow down a system by deliberately running wasteful jobs. Examples include disabling or crashing the system, playing games, sending mass mailings, creating unnecessary or multiple jobs and process names, etc.
- Bypass accounting or security mechanisms, attempt to circumvent data-protection or system consistency schemes, or attempt to uncover security loopholes.
- Provide others with programs or files that cause damage to their files or the operation of their computer system, compromise the security of their accounts, or disable their account.
- Harass others by sending annoying, obscene, libelous, or threatening messages.
- Disobey the rules of any computer system or network that you remotely access through MCC's computer systems.
- Aid or abet another person in violating any part of this Code of Conduct.

The above list is not exhaustive. This Code of Conduct is intended to require compliance with all local, state, and federal laws. Individuals who violate any part of the Code of Conduct will be subject to college disciplinary action, criminal prosecution or civil action.

LAPTOP BEST PRACTICES IN THE MCC CYBER SECURITY POLICY

Portable Devices

When using mobile computing resources such as notebooks, PDA’s, laptops, and mobile phones, special care must be taken to ensure that information is not compromised.

- Individuals are required to use a unique, secure username and password to avoid the unauthorized access to, or disclosure of, the information stored and processed by these devices.
- Precautions must be taken to avoid the risk of unauthorized persons viewing information on-screen.
- Procedures to prevent the introduction or execution of malicious software shall be developed and implemented and be kept up to date.
- Equipment carrying important, sensitive and/or critical business information must not be left unattended and where possible, must be physically locked away, or special locks must be used to secure the equipment.
- Training must be provided to staff using mobile computing resources to raise their awareness of the additional risks resulting from this way of working and the controls that must be implemented.
- Employees in the possession of portable, laptop, notebook, netbook, and other transportable computers must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler as hand luggage unless other arrangements are required by federal or state authorities.

GUIDELINES FOR APPROPRIATE USE AND RESPONSIBILITY

Monroe Community College provides portable computers (laptops, notebooks and netbooks, etc.) collectively known as 'laptops' to faculty and staff members whose professional responsibilities and personal preferences conform to the guidelines in this document. A decision to provide a laptop is based upon identifiable need and available budget. The purpose of the laptop program is to enhance and enrich teaching and learning at the College, to facilitate the conduct of administrative duties, and to support communication. While the laptop program enables employees of Monroe Community College to conduct college business from various off-campus locations, the program does not change College expectations about attendance or other work practices.

Appropriate Use Issues

The laptop assigned to you with the property ID noted above is intended for use for college-related business as a productivity tool, curriculum tool, and for research and communication. It is not intended as a replacement for any computers you may own personally. Use of the laptop for college-related or personal purposes should be within the standards of good judgment and common sense, in compliance with the College's published Code of Conduct for Users of College Computer Systems as required through the terms and conditions of applicable software license agreements, and in compliance with practices set forth in the MCC Cyber Security Policy.

Physical Asset and Inventory Issues

- The laptop computer is provided for your use, but remains the property of Monroe Community College. Under the direction of the Controller the College conducts an annual physical inventory of all College assets. The laptop computer you are taking responsibility for is considered an asset of the College regardless of the funding source used to purchase the unit and as such must be inventoried as part of the annual College-wide physical inventory. Each unit is labeled with a unique property ID. The property ID allows College Property Control and ETS to manage unit assignments, coordinate reports, and maintain inventory systems. Do not remove the property ID tag from the laptop assigned to you.

- ***You will be required to physically bring the laptop to a designated campus location once per year for inventory purposes.*** Multiple dates and locations will be announced in the Tribune to facilitate this process. Generally these dates will be during the Spring semester of any given year. If you are unavailable during the announced dates, you may make special arrangements to present the laptop for inventory by contacting Property Control at 585-292-3247.

- Failure to provide the laptop for physical inventory will result in the item being listed on our inventory as 'unlocated.' You will be responsible to reimburse the College from personal funds for the replacement cost of the item, unless otherwise determined.

Setup, Maintenance and Repair Issues

- The laptop computer will be configured with a standard suite of programs that are appropriate for the type of computer you received based upon the campus software standards. It is also possible that other applications will be provided you by the College, based upon your professional needs or the requirements of the laptop. You should keep in mind the college policies for appropriate use of software, including the requirement to demonstrate legal license to a program before it can be installed on a college-owned computer. The Code of Conduct for Users of the College Computer Systems applies to all laptop activities.

- The laptop assigned to you will be configured with Ethernet. These will allow the laptop to connect to the Internet from locations other than campus, such as through an Internet service provider (ISP) at your home. However, the College will not provide Internet access to you from off-campus nor will ETS configure the laptop assigned to you to work with your ISP. It will be up to you and your ISP to make remote connections work.

- The College and ETS will secure, via warranty extension or other means, the services needed to repair the laptop should its operation be impaired by a component failure or normal wear and tear. The coverage for these items will be borne by the College. However, it is your responsibility to take appropriate precautions to prevent damage or loss/theft of the laptop assigned to you. You may be responsible for certain costs to repair or replace the computer if the damage or loss is due to negligence or intentional misconduct.

- Should you have problems with the laptop assigned to you, you will need to bring it to your office or the ETS offices for hardware repair, software installation or program diagnosis. ETS staff will not visit your home or go to off-campus locations to provide services.

Security Issues

- If the laptop assigned to you is lost or stolen you must report the disappearance to the proper authority immediately. Theft or loss that occurs on campus should be reported to Public Safety. For theft or loss off campus, you should report the disappearance to the local police. The police report should include the serial number for the lost computer. You will need to provide ETS with a copy of the police report within 48 hours of the discovery of the loss.

- You are responsible for maintaining an appropriate backup of the data on the laptop assigned to you, especially of the work-related documents and data files you create that cannot be retrieved by reinstalling the operating system or programs. Depending upon how you intend to use the laptop, you will probably need to store some of your documents and data files on the laptop's hard disk drive, however, this should not include identifying files you use on the laptop to the College 'M' Drive as an added precaution against data loss. You should not use the 'M' drive to backup personal documents or data files.

- Laptops will be set-up to automatically receive Microsoft and Symantec antivirus updates.