Manhattan Area Technical College
Institutional Policy and Procedure Manual

Policy No. 9.1.1

Title: Computer Usage Policy	
Originated by: CISO	
Originated Approver: Board of Directors	Originated Date:
Revised by:	Revised Date: 3/2019
Reviewed on:	

Policy Statement:

Manhattan Area Technical College intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to MATC's established culture of openness, trust, and integrity. MATC is committed to protecting employees, partners and the college from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of MATC. These systems are to be used for business purposes in serving the interests of the company, and of our customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every MATC employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Rationale:

Employees, students, and guests are responsible for maintaining an environment free of malicious, inappropriate, and illegal acts. MATC is not responsible for unacceptable or unethical use of the information technology systems including internet access, network usage, and electronic mail. However, policies and best practices will be employed to protect the institution, authorized users and electronic data stored on MATC systems. Unacceptable uses of the computer system will result in the revoking of computer access. Faculty and staff may utilize laptop computers or portable computing devices in the performance of their duties including but not limited to traveling to conferences, workshops, or other off-campus activities. Due to the mobile nature of such items, additional measures must be taken to secure College property and data.

Scope:

This policy applies to the use of information, electronic and computing devices, and network resources to conduct MATC business or interact with internal networks and business systems, whether owned or leased by MATC, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at MATC and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with MATC policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at MATC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by MATC.

Procedure:

1.1 General Use and Ownership

1.1.1 MATC's proprietary information stored on electronic and computing devices whether owned or leased by MATC, the employee or a third party, remains the sole property of MATC. You must ensure through legal or technical means that proprietary information is protected by the *Data Protection Standard.*

1.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of MATC's proprietary information.

1.1.3 You may access, use or share MATC's proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

1.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

1.1.5 For security and network maintenance purposes, authorized individuals within MATC may monitor equipment, systems, and network traffic at any time.

1.1.6 MATC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.2 Security and Proprietary Information

1.2.1 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended. Unauthorized access is prohibited.

1.2.2 Postings by employees from an MATC email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of MATC unless posting is in the course of business duties.

1.2.3 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

1.3 Portable or Remote Computing

1.3.11.3.1 Laptop computers and/or portable computing devices will be under the control of the IT Department. The IT Department will check out the equipment for use by faculty and staff in conducting college business. Please notify Helpdesk@manahattantech.edu at least one week before needing the laptop or portable-computing device. Include in the request any software that will need to be loaded.

1.3.2 No personal or student information should be saved to the laptop or portable-computing device.

1.3.3 Staff members that have checked out laptop computers and/or portable-computing devices will take all reasonable measures to secure the device and data contained therein including but not limited to the following.

- Keep the device within your immediate control while traveling
- Do not leave the device in an unlocked car, residence or hotel room
- Use the case provided to protect the device from accidental damage
- Do not loan the device to any other individual including another staff member
- In the event the device has been damaged, lost, or stolen, report the incident to the IT Department immediately.

1.3.4 Failure to take reasonable measures to protect MATC-owned portable-computing devices may result in the employee being responsible for any financial loss.

1.4 Student E-mail Accounts

1.4.1 Email as official communication

Emails are to be considered an appropriate mechanism for official communication by MATC with faculty, staff, and students. MATC has the right to send official communications by email to faculty, staff, and students with the full expectations that those communications will be received and read in a timely fashion. The same expectation may be held for faculty, staff, and students communicating via email.

1.4.2 Use of college account

Official email communication will be sent to the recipients' official college email address. Faculty, staff, and students are expected to check their email frequently and consistently to stay current with MATC and faculty-student related communication. It should be recognized that certain communications may be time-critical. Faculty, staff, and students will not be held responsible for an interruption in their ability to access an email message due to a College system-related problem that may prevent timely delivery or access to the message.

1.4.3 Forward email

Setting up auto-forward rules from your MATC email account to a private, unofficial email address outside matc.net or manhattantech.edu is prohibited.

1.4.4 Communicating confidential information

Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form is not secure and is, therefore, vulnerable to unauthorized access and modification by third parties. Confidential information, such as student grades or social security numbers should not be sent to a student with a private, unofficial, non-College email account (i.e., aol.com, yahoo.com, hotmail.com, cox.net, etc.). Faculty may require students to provide their official College email address (matc.net or manhattantech.edu) to receive a reply. A recommended step is to provide general replies directing students to College tools that require authentication, such as MATCOnline.

1.4.5 Passwords

Users are responsible for protecting their own passwords and should not share their login information.

1.4.6 Student email account standards

The account of any faculty, staff, or student who deliberately violates this or other relevant College policies, such as the non-tolerance policies, using the College email account, may be terminated immediately. A member of Administration will be responsible for determining if such a violation has occurred and subsequently notifying the IT Department to terminate the account. Certain types of email, including but not limited to harassing messages, may also incur civil or criminal penalties.

1.5 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of MATC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing MATC owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

1.5.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by MATC.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which MATC or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting MATC business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using an MATC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any MATC account.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to MATC is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Introducing honeypots, honeynets, or similar technology on the MATC network.

14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

16. Providing information about, or lists of, MATC employees to parties outside MATC is strictly prohibited without written consent from MATC administration.

1.5.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation with the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within MATC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by MATC or connected via MATC's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

1.5.3 Blogging and Social Media

1. Blogging by employees, whether using MATC's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of MATC's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate MATC's policy, is not detrimental to MATC's best interests, and does not interfere with an employee's regular work duties. Blogging from MATC's systems is also subject to monitoring.

2. MATC's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any MATC's confidential or proprietary information, trade secrets or any other material covered by MATC's Confidential Information policy when engaged in blogging.

3. Employees may also not attribute personal statements, opinions or beliefs to MATC when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of MATC. Employees assume any and all risk associated with blogging.

   Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, MATC's trademarks, logos, and any other MATC intellectual property may also not be used in connection with any blogging activity.

Policy Compliance:

1.6 Compliance Measurement

MATC administration will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

1.7 Exceptions

Any exception to the policy must be approved by the MATC administration team in advance.

1.8 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.