ADMINISTRATIVE REGULATION AND PROCEDURE

Title: TECHNOLOGY USAGE	Code: EE0202

Policy Reference: E0202, Policy Statement Governing Technology Use by Faculty and Staff; C0201, Harassment; C0700, District Employee Code of Ethics

1.0 BACKGROUND AND PURPOSE

This procedure is intended to allow for the proper use of all MATC computer technology resources, effective protection of individual users, equitable access, data security, and proper management of those resources (also referred to herein as the "Network" or "System"). This procedure also applies to MATC Network usage even in situations where it would not apply to the computer(s) in use. This procedure is intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to these resources.

Access to networks, computer systems, and software owned, licensed, or operated by MATC is a privilege and imposes certain responsibilities and obligations and is granted subject to MATC policies and local, state, and federal laws. Appropriate use should always be legal and ethical, reflect academic honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property, ownership of data, system security mechanisms, and individual rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance. Appropriate use of technology resources includes instruction, independent study, authorized research, communications appropriate to a district board member, college staff or student user, and official work of the offices, departments, divisions, recognized student and campus organizations, and agencies of MATC. The proper use of technology assets will be in compliance with data regulatory mandates (FERPA, HIPAA, Sarbanes-Oxley, etc.) data security and data privacy.

2.0 USAGE/WARRANTIES/LIABILITIES

2.1 Authorized Use

Authorized use of MATC owned or operated technology resources is consistent with the mission of the college and consistent with this procedure.

2.2 Authorized Users

Authorized Users are: (1) current district board members, faculty, staff, and students of the college; (2) any individuals connecting to an MATC-sponsored public information service; (3) others whose access furthers the mission of MATC and whose usage does not interfere with other access to resources. In addition, a User must be specifically authorized to use a particular technology resource by the campus division responsible for operating the resource.

2.3 Disclaimer of Warranty

The User acknowledges that the services provided under this agreement, including access to the System, are provided by MATC and the information providers on an "AS IS" basis. MATC and the information providers make no representation or warranties, express or implied, with respect to the System and access thereto, including, warranties of merchantability or fitness for a particular purpose. MATC and the information providers do not represent or warrant that access to the System will be uninterrupted, or that there will be no failures in transmission of information, errors or omissions in transmission, or loss of information.

2.4 Limitation of Liability

User assumes all risks of loss or damage in connection with their use of the System, including, but not limited to, any loss or damage arising from the selection of the uses to which it will put the System and the adequacy of the System to meet the User's need.

2.5 Disclaimer of Liability

MATC and the information providers are not liable to User with respect of any claim made based on copyright, trade secrets, or other intellectual property or other proprietary rights in regard to any information or the use of which any information is put by User.

2.6 Indemnification

User shall indemnify, hold harmless, and defend MATC, its officers, employees, and agents, from and against any claims, liabilities, losses, costs, damages, or expenses (including attorney's fees) arising out of the User's use of the System or the information contained thereon.

2.7 Assignment

User may not assign or transfer, in whole or in part, his/her rights to use the System, including the use of the User's password, without the prior written consent of MATC.

2.8 Hardware or Software Access

MATC shall not be responsible in any way for any User hardware or software required or used by User to access or communicate with the System or to upload or download Information or for the telecommunication cost of accessing the System.

3.0 INDIVIDUAL PRIVILEGES

The following privileges, all of which currently exist at MATC, empower each User to be a productive member of the campus community. It must be understood that privileges are conditional upon acceptance of the accompanying responsibilities. (This includes compliance with all applicable MATC Policies and Procedures).

3.1 Privacy

To the extent possible in a public setting and subject to Section 5 hereof, MATC wants to preserve the individual's privacy. Electronic and other technological methods must not be used to infringe upon privacy. However, users must recognize that MATC computer systems and networks are public and subject to the Wisconsin Open Records Law and their contents are subject to public scrutiny. MATC data is subject to FERPA and HIPAA security controls. Individuals utilize such systems at their own risk.

According to Wisconsin State Statute 19.32(2), Definitions, "record" means any material on which written, drawn, printed, spoken, visual or electromagnetic information is recorded or preserved, regardless of physical form or characteristics, which has been created or is being kept by an authority. "Record" includes, but is not limited to, handwritten, typed or printed pages, maps, charts, photographs, films, recordings, tapes (including computer tapes), computer printouts and optical disks. "Record" does **not include** drafts, notes, preliminary computations and like materials prepared for the originator's personal use or prepared by the originator in the name of a person for whom the originator is working; materials which are purely the personal property of the custodian and have no relation to his or her office; materials to which access is limited by copyright, patent or bequest; and published materials in the possession of an authority other than a public library which are available for sale, or which are available for inspection at a public library.

3.2 Freedom of Expression

The constitutional right to freedom of speech applies to all members of the campus regardless of the medium used.

3.3 Ownership of Intellectual Property

People creating intellectual property using MATC resources, including but not limited to software, should consult the MATC policy governing copyright ownership and other related MATC policies.

3.4 Freedom from Harassment and Undesired Information

All members of the campus have the right not to be harassed through a technology resource by others. (See 4.1.3.) This includes, but is not limited to, written messages, downloading or transmission of pornography or other similar inappropriate communication.

4.0 INDIVIDUAL RESPONSIBILITIES

Just as certain privileges are given to each member of the campus community, each User is held accountable for his/her actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each individual situation and across MATC engenders the trust and intellectual freedom that form the heart of our community. This trust and freedom are grounded in each person developing the skills necessary to be an active and contributing member of the community. These skills include awareness and knowledge about information and the technology used to process, store, and transmit it.

4.1 Responsible Use of Information

Responsible use of information is detailed in 4.1.1 to 4.1.3.

4.1.1 Privacy of Information

The fact that a User has the ability to access a file or other information does not constitute permission to do so. Users are to limit their use of computer equipment, software, and network access to the performance of their job duties or other Authorized Use. Users may be subject to criminal prosecution if they access or release information/data without authorization, intentionally disclose their password to another who uses it to gain unauthorized access to information, and/or fail to exercise adequate care in maintaining system security.

The User shall not use the System to gain access to personnel and other confidential MATC information which is not being used by the User to perform his or her job duties.

No one should access, look at, copy, alter, or destroy anyone else's files without explicit permission (see 5.3) (unless authorized or required to do so by law or regulation). Remember, simply being able to access a file or other information does not imply permission to do so.

4.1.2 Intellectual Property

Users are responsible for recognizing and honoring the intellectual property rights of others.

4.1.3 Harassment

No person may, under any circumstances, use MATC's technology resources to libel, slander, or harass any other person in any manner. Harassment through computer or e-mail use is subject to the MATC Harassment Policy (CO201). Student users may be subject to disciplinary action for any violations under the Student Life Code of Conduct (including loss of system privileges).

4.2 Responsible Use of Resources

Users are expected to refrain from all acts that waste or prevent others from using information resources. Details regarding available resources are available in many ways, including conferring with other users, examining on-line and printed references maintained by Information Technology (IT) Division by contacting the IT Division Help desk (297-6541).

4.3 Information Integrity

It is the responsibility of MATC users to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information that they compile or use. Users must not depend on information or communications to be correct when they appear contrary to their expectations and should verify it with the person whom is believed to have originated the message or data. **All users are required to use appropriate names and language in the name spaces, address spaces and other areas on the network.**

4.4 Use of Desktop Systems

Users are responsible, in coordination with the IT Division, for the security and integrity of MATC information stored on their personal desktop system. This responsibility includes making regular backups, controlling physical and network access to the machine, and using virus protection software.

4.5 Access to Facilities and Information

Access to facilities and information is detailed in 4.5.1 to 4.5.4

4.5.1 Sharing of Access

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Individual users are responsible for any use of their accounts. Sharing of passwords with others may result in the loss of network access privileges.

4.5.2 Permitting Unauthorized Access

Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. (See section 2.2.)

4.5.3 Use of Privileged Access

Special access to information or other special computing privileges is to be used in performance of official duties only. Information obtained through special privileges is to be treated as private.

4.5.4 Termination of Access

When users cease being a member of the MATC community (graduate or terminate employment), or if they are assigned a new position and/or responsibilities within MATC, their access authorization will be reviewed and if appropriate, terminated. Users must not use facilities, accounts, access codes, privileges, or information for which they are not authorized in the new circumstances.

4.6 Attempts to Circumvent Security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by IT personnel. The Director of Technical Services, has the responsibility for technology security.

4.6.1 Decoding Access Control Information

Users are prohibited from using any computer program or device to intercept or decode passwords or similarly access control information.

4.6.2 Denial of Service

Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any MATC technology resource are prohibited. The Director of Technical Services, in conjunction with the CIO, will make a joint decision affecting technology access by a user under this provision.

4.6.3 Harmful Activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software, or data belonging to MATC or other users, and the like; making or importing unauthorized and/or unlicensed copies of data or software; and conveying software or data to any outside third party.

4.6.4 Unauthorized Access

Users may not:

- damage computer systems or deployed software services
- obtain extra resources not authorized to them
- deprive another user of authorized resources
- gain unauthorized access to systems
- access personnel or confidential institutional information which they do not need to carry out their tasks or duties
- transmit or import any material or data in violation of any federal, state, or local law or regulation
- install software not under license or prior approval of the IT Governance Committee
- faculty and staff are not permitted to purchase software or cloud services with a PCard, or without the prior approval of the IT Governance Committee after approving a Business Case submission

by using knowledge of:

- a special password
- loopholes in computer security systems
- another user's password
- access abilities used during a previous position at MATC
- authorized access to obtain information not necessary to carry out appropriate uses (such as personnel records, or student information).
- Attempt to alter Endpoint Detection and Response (EDR) security software

4.6.5 Unauthorized Monitoring

Users may not use technology resources for unauthorized monitoring of electronic communications.

4.7 Academic Dishonesty

Users should always use computing resources in accordance with the high ethical standards of the college community. Plagiarism and cheating are violations of those standards.

4.8 Use of Copyrighted Information and Materials

Users are prohibited from using, inspecting, copying, and storing copyrighted computer programs and other material in violation of copyright law.

4.9 Copyright Complaints

MATC respects the intellectual property of others, and we ask our users to do the same. MATC may, in appropriate circumstances and at its discretion, terminate the accounts of users who infringe the intellectual property rights of others.

If you believe that your work has been copied and is accessible on the MATC service in a way that constitutes copyright infringement, you may notify MATC by providing MATC's copyright agent the following information:

1. An electronic or physical signature of the person authorized to act on behalf of the owner of the copyright interest;

2. A description of the copyrighted work that you claim has been infringed, including the URL (i.e., web page address) of the location where the copyrighted work exists or a copy of the copyrighted work;

3. Identification of the URL or other specific location on the MATC site where the material that you claim is infringing is located;

4. Your address, telephone number, and e-mail address;

5. A statement by you that you have a good faith belief that the disputed use is not authorized by the copyright owner, its agent, or the law;

6. A statement by you, made under penalty of perjury, that the above information in your Notice is accurate and that you are the copyright owner or authorized to act on the copyright owner's behalf.

MATC's agent for notice of claims of copyright infringement on this Web site can be reached as follows:
Vice President and General Counsel
Milwaukee Area Technical College
700 West State Street
Milwaukee, WI 53233-1443
Telephone: (414) 297- 7307
E-mail: generalcounsel@matc.edu

4.10 Use of Licensed Software

No software may be installed, copied, or used on MATC assets except as permitted by existing software licensing (Google, Microsoft, Adobe, etc.) or software approved by the IT Governance Committee. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, and number of simultaneous users,

term of license, etc.) must be strictly adhered to. No software or cloud service is to be installed or accessed on any MATC asset without the authorization of the Director of Technical Services, IT Security, or the IT Governance Committee.

4.11 Personal Use

Computing facilities, services, and networks may not be used in connection with compensated outside work nor for the benefit of organizations not related to MATC except in connection with scholarly pursuits (such as faculty publishing activities) in accordance with the MATC Ethics Policy and Student Code of Conduct. Computing facilities, services and networks are not to be used to obtain information regarding MATC employees, board members, or students for which is not necessary to carry out an authorized employee or student duty or task.

5.0 SYSTEM MONITORING

5.1 Imposition of Sanctions

MATC may impose sanctions and punishments, including loss of user privileges, on anyone who violates the policies and procedures of MATC regarding computer, and network. Employees may be subject to disciplinary action up to and including discharge. Students may be subject to disciplinary action up to and including dismissal through the Student Life Code of Conduct.

5.2 System Administration Access

A System Administrator (i.e., the person responsible for the technical operations of a particular machine) may access others' files for the maintenance of networks and computer and storage systems, such as to create backup copies of data. However, in all cases, all individuals' privileges and rights of privacy are to be preserved to the greatest extent possible.

5.3 Monitoring of Usage, Inspection of Files

MATC Information Technology division ("IT") may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, network loading, authorized investigation, etc. IT may review this data for evidence of violation of law or policy.

IT Security upon alert status regarding Endpoint Detection and Response, will stop a computer from network access when malware is detected. Upon mitigation the network access will be restored. In all cases, all users' privileges and right of privacy are to be preserved to the greatest extent possible.

5.4 Suspension of Individual Privileges

A user's computer and network may be suspended or terminated for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and well-being of other members of the campus community, or college property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the Office of Student Life (for students) or the employee's department in consultation with Human Resources. Members of the bargaining units are entitled to due process as outlined in their respective contracts.

6.0 MATC RESPONSIBILITIES

6.1 Security Procedures

MATC has the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, isolate workstations until mitigated, and to impose appropriate penalties when privacy or security is purposefully abridged.

6.2 Individual Department Responsibilities

Each department has the responsibility to:

- Enforce this policy
- Provide for security in their areas

If warranted by the importance and sensitivity of information stored and processed in their facility, a department must also:

- Verify the integrity of regular media backups
- Employ appropriate security-related software and procedures
- Guard confidentiality of Personally Identifiable Information (PII), including user files and system access codes
- Monitor and provide physical access to equipment
- Provide proper physical environment for equipment
- Provide safeguards against fire, flood, theft, etc.
- Provide proper access administration; e.g., prompt and appropriate adjustment of access

6.3 Procedural Guidelines

The CIO is responsible for developing and issuing general procedural guidelines for use of resources, etc.

7.0 PROCEDURES AND SANCTIONS

7.1 Responding to Security and Abuse Incidents

All users and divisions have the responsibility to report any discovered unauthorized usage or access attempts of MATC computers, networks, or other information processing equipment. If users observe, or have reported to employees, a security or abuse problem with any college computer or network facilities, including violations of this policy, employees should:

- Take immediate steps as necessary to ensure the safety and well-being of users and of information resources. For example, if warranted, an Information Technology representative should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 5.4).
- Ensure that the user's immediate supervisor and the Director of Technical Services are notified.

The Director of Technical Services will coordinate the technical and administrative response to such incidents. Reports of all incidents will be forwarded to Student Life/ Judicial Affairs (for apparent policy violations by students) or the division head (for employees), and to the CIO.

7.2 Appeal of Termination of User Access

An authorized user may appeal termination of his/her technology or usage access. A written statement detailing reasons why access should be reinstated must be submitted no later than ten (10) calendar days from written notification of access termination. Any and all correspondence will be sent to the CIO. He/she will have five (5) calendar days to respond from the date of receipt of the written appeal. If the CIO decision is not satisfactory to the user, that decision may be appealed to the Executive Vice President . His/her decision will be issued no later than five (5) calendar days from receipt of the decision of the CIO. **The decision of the Executive Vice President is final.**

7.3 Range of Disciplinary Sanctions

Persons in violation of this procedure are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the college, and legal action. Some violations may constitute criminal offenses, as outlined

in the local, state, and federal laws; the college will carry out its responsibility to report such violations to the appropriate authorities.

8.0 WEB SITE POLICY/PROCEDURE

The following standards in the development and maintenance of MATC Web Site connected web content must be followed by all Users:

1. Appropriate Copyright laws must be followed in all Web Site development.
2. All Web maintenance will be done using MATC's Content Management System unless authorized in writing by MATC's Communication and Events Director.
3. External links to non-MATC content must be approved in writing via e-mail by MATC Marketing before the links can be added to an MATC Web Site page.
4. All web content will adhere to the MATC Web Site Style Guide.
5. All web page changes will be automatically submitted to Marketing for review prior to a page going "live" unless Marketing grants a department an exemption from such reviews.
6. All web content will adhere to all of MATC's Policies and Procedures.
7. As users change content which does not currently comply with the MATC Style Guide, users will bring the content into compliance with Style Guidelines.
8. MATC faculty or staff who desire to create a web link directly off MATC's home page, such as www.matc.edu/times, must send such a request, in writing, to the MATC Communication and Events Director. Such links must represent a significant MATC-Community partnership.

Office of Responsibility: Information Technology
Last Reviewed: August, 2021