APPROPRIATE USE POLICY

Table of Contents

1. OVERVIEW

This policy applies to all users of IT systems, including but not limited to students, faculty, and staff. It applies to the use of all IT systems. These systems, networks, and facilities administered by the IT Department, as well as those administered by individual departments, laboratories, and other college-based entities.

2. PURPOSE

The purpose of this policy is to ensure that information technology infrastructure promotes the basic mission of the college in teaching, learning, research, and administration. In particular, this policy aims to promote the following goals:

- To ensure integrity, reliability, availability, and superior performance of IT systems.
- To ensure that IT systems are used for their intended purposes.
- To establish processes for addressing policy violations and sanctions for violators.
- To ensure the users have the appropriate access for remote work and distance learning.

3. SCOPE

Use of institutional computers, network, and internet services is a privilege, not a right. All users are required to comply with this policy and the accompanying rules.

4. POLICIES

A. UNACCEPTABLE USE

Use of institutional computers, network, and internet services is a privilege, not a right. All users are required to comply with this policy and the accompanying rules. The following rules are intended to provide general guidelines and examples of prohibited use. Failure to comply with these rules may result in loss of computer and internet access privileges, disciplinary action, and/or legal action.

- All users shall have no expectation of privacy regarding computer files, email, or internet usage. Turtle Mountain Community College reserves the right to monitor all computer files, email, and internet usage without prior notice.
- All users may not attempt to gain unauthorized access to any other computer system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of “browsing."
- All users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.

- All users are not allowed to download, copy, or install any games or unauthorized software on college computers. Any unauthorized software and games, if found in the college computers, will be removed by college IT Department.
- All users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. Restrictions against inappropriate language apply to public messages, private messages, and material posted on social media sites. Please see Title IX Policy.
- All users will not post private information about another person.
- All users will not use College resources (including, for example, e-mail, web pages, or newsgroups) to defame, harass, intimidate or threaten any other person(s), or to promote bigotry or discrimination.
- All users will not knowingly or recklessly post false or defamatory information about a person or organization.
- Use information systems to solicit for commercial ventures, religious or political causes, or for personal gain.
- Any attempt to negate or circumvent security controls, policies and procedures (e.g., disabling virus protection or tunneling a protocol through a firewall).
- Use that violates local, state or federal laws.

B. EMAIL

Use of email by staff, faculty, and students is permitted and encouraged where such use supports the goals and objectives of the institution. Users of TMCC's email services are expected to act in accordance with the following policies and with professional and personal courtesy and conduct.

- Email is an official means of communication at TMCC. Account holders are responsible for accessing their email in a timely manner.
- The Information Technology personnel will assign all users an official institution e-mail address. It is to this address that the institution will send all official email communications.
- Any emails that discriminate against employees by virtue of any protected classification including race, color, gender, religion, national origin, sexual orientation, age, or disabilities, will be dealt with according to the harassment policy.
- You cannot send or attempt to send spam of any kind. 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).
- Once an employee has resigned or been terminated; or a student has withdrawn or graduated, they will have two weeks to save any email. After the two weeks the account will be deleted.
- Sending mass email that is unrelated to an individual's administrative or academic activity is completely prohibited. Mass e-mails are defined as messages sent to all students, all staff, all faculty, or when individual recipient addressees are not defined. IT manages e-mail distribution lists

of current staff, faculty, and students. There is no opt-out provision for these lists. If you need to attach a large file please contact the IT Department for alternate methods of distribution.
- Users that sign a contract to use TMCC equipment including but not limited to laptops, tablets and other electronic devices are responsible for the replacement of damaged, lost or stolen equipment.
- While the College makes a good faith effort to reduce the amount of spam delivered to individual mailboxes, it accepts no responsibility for the content of email received by account holders.
- Forgery (or attempted forgery) of email messages is prohibited.
- Attempts to read, delete, copy, or modify the email of other users are prohibited.

C. PRIVACY AND CONFIDENTIALITY

Communication via e-mail is subject to all of the same public information, privacy, and records retention laws as other forms of communication. While TMCC e-mail affords some measure of privacy, the redirecting of e-mail by students to outside accounts and the sharing of messages with third parties can negate the privacy protection rights afforded by students to the College.

D. SOCIAL MEDIA

Purpose:

Turtle Mountain Community College encourages the use of social media to connect with others, including students, employees, alumni, fans, and the College. Social media sites are excellent venues to communicate and encourage engaging discussions about College current events, issues, accolades, organizations and people. This policy defines the rules and procedures for the use of social media.

Policy:

- Think first, post second. The things that can get you in trouble and subject you to discipline with the College can do the same in the realm of the internet and social media. Some examples include: sexually harassing a colleague, inappropriate interactions with students, derogatory statements, threatening or intimidating others, violating privacy policies/laws, or defamation. Please refer to the TMCC Title IX Policy.
- Generally, employees should manage their personal social media accounts on their own time. There may be minimal personal use of social media while utilizing College resources but only to the extent such use does not hinder an employee's job productivity, the productivity of other employees, or College programs/activities.
- Computers, hardware, information technology accounts, and information technology infrastructure are property owned and operated by the

College. As a result, the law does not grant you an expectation of privacy in your usage of them. Conduct personal matters on your personal devices and refrain from doing so on property owned by the college.
- You are prohibited from using the College name or image to endorse an opinion, product, cause, business, or political candidate or otherwise holding yourself out as a representative of the College when you are not.
- Be mindful of copyright and intellectual property rights of others and the college and of college policies regarding those rights. A common example would be posting a video with copyrighted music attached to it. All videos are subject to review by Facebook, Twitter, Instagram, etc., and they reserve the right to remove content and even possibly suspend your account if copyright infringement is in play.

Non-Compliance/Breach of Policy

Violations of this policy will result in a review of the incident and may include action under appropriate College discipline processes. Corrective action may involve but are not limited to: a verbal or written warning, suspension or dismissal and/or termination of employment or privileges with Turtle Mountain Community College. This section does not preclude disciplinary action for conduct that involves social media and that also violates other College policies.

Best Practices:

- Be confidential. Be careful not to reveal confidential or proprietary information about TMCC students, employees or alumni. Adhere to all applicable College, Tribal and federal privacy and confidentiality policies. All employees of TMCC are subject to FERPA, and other laws mandating the nondisclosure of personal information.
- Respect TMCC. Remain professional and in good taste, and protect TMCC's institutional voice. As a representative of TMCC, avoid pranks and postings that could be misinterpreted. Ask your supervisor if you are unsure. Respect College time and property—TMCC computers and time on the job are reserved for College-related business.
- Be respectful: Understand that content contributed to social media could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the poster and/or the college and its institutional voice. You are more likely to achieve your goals or sway others to your beliefs if you are constructive and respectful while discussing a bad experience or disagreeing with a concept or person. In addition, the Acceptable Use Policy prohibits threats or harassment by using TMCC's computing resources to "transmit material or data that causes or encourages physical or intellectual abuse or that causes or encourages harassment, explicit or implied."
- Create accounts with your departmental tm.edu email address. If you are setting up social media accounts on behalf of your department then be

sure to add your shared departmental tm.edu address as an administrator. This will ensure a successful transfer of administrative power if and when you no longer are responsible for updating the account.

- Assign responsibility. When possible, identify a full-time appointed employee responsible for social media content and monitoring. If responsibility is not assigned, new content might not be posted, and the site will wither and die. As your site grows, you will also need someone familiar with the site to attest what is and isn't working for your audience.
- Finally, remember anything you post can resurface in the future. Anyone can screenshot and save any content that you post. Since you deleted a post after realizing it was inappropriate doesn't mean that it went unnoticed by even one individual. Always remember, think first before posting.

Guidelines for Handling Negative Posts

- When you've developed a vibrant social media community, it's inevitable that you'll get some negative posts. Most of these posts, handled well, create an opportunity to strengthen your community by solving a problem or generating a good discussion. Some may require a team response.
- Here's an overview of what to do:
- It's important to be calm, thoughtful and strategic when dealing with a negative post. Take the time to consider whether and how to respond.
- Confirm facts. Make sure you know the facts and current college policies and procedures related to the post.
- Sympathize. Consider whether to apologize. Often people who are upset simply want to know their complaint has been heard.
- Consider going offline. In many cases, the person who wrote the post will be willing to talk with.
- Say "Thank You." Social media depends on conversations to thrive. It's good practice to thank people for their posts, even if their post is a complaint or otherwise negative.
- Clarify. Sometimes social media posts are so brief that they can be misunderstood. Make sure your intent is clear.

5. NETWORK

Individuals who are eligible to receive access to network services.

The following users are identified as eligible to receive network services from TMCC. Any applicant for network not described below should be referred to the IT Department, who will coordinate a decision on that particular case.

- **Students:** All full-time and part-time students may receive network privileges without restriction.

- **Faculty:** All full-time faculty without restriction. Part-time faculty, faculty with temporary or cyclical appointments, and visiting faculty may receive limited network privileges.
- **Full-time regular part-time staff:** All regular, non- faculty, college employees may receive network privileges without limitations.

The campus community and its guests have access to the network provided they adhere to all established policies regarding network usage and are in compliance with applicable local, state, and federal laws. TMCC's network policies prohibit disruptive or abusive behavior, which includes but is not limited to using the network in the following ways:

Responsibilities

- **Account Responsibility:** Access to the TMCC's Network is through individual accounts with password protection. Accounts and passwords are not to be shared. All violations of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account.
- **Network Degradation:** The running of programs, services, systems, processes, or servers by a single user, or group of users, that may substantially degrade network performance or accessibility will not be allowed. Electronic chain letters, mail bombs, malware, spamming, and excessive recreational use of the TMCC Network are prohibited.
- **Copyrights:** Network users must respect all copyrights and intellectual property laws, and always provide proper attributions of authorship. Commercial software licensed to TMCC may be installed only on equipment and devices expressly covered by the licenses. Upon request from a network administrator, individuals who have software licensed to them and installed on a TMCC computer shall produce original disks and/or documentation to verify compliance.
- **Printing:** Network users are expected to use network printing in a responsible manner by printing only those materials essential to educational, academic, or College needs and by printing selected text rather than full text when possible.
- **Business Transactions/Personal Use:** The conduct of occasional private business or financial transactions when such uses are de minimus and sporadic in nature is permitted, provided such use does not degrade the TMCC Network performance.

Prohibited Activities

- **Spreading Computer Viruses and Worms:** Deliberate attempts to degrade or disrupt the system performance of the TMCC Network or any other computer system or network on the Internet by spreading computer viruses, worms, and malware. As a precondition for network attachment and use, all personal computers and devices capable of running antivirus

software must have up-to-date virus protection software installed and operating.

- **Impersonation:** Impersonation, false representation, forgery, pseudonyms, spoofing, deception, and other methods of hiding or cloaking the true identity of a user in order to mislead or avoid detection is prohibited.
- **Unauthorized Access:** Gaining or attempting to gain unauthorized access to, or make unauthorized use of, accounts, files, records, equipment, or networks is prohibited. Violating the privacy of others is also prohibited.
- **Business Transactions**: The use of the TMCC Network and/or personal web pages to offer goods or services of a business or commercial nature is not permitted except for those consistent with the College's educational or business mission.
- **Illegal Activities:** Use of the TMCC Network for any activity contrary to Federal, state, or local laws is prohibited. Illegal activities include, but are not limited to, tampering with computer hardware or software, unauthorized entry into computer systems or computer data, willful vandalism or destruction of computer data or files, or any attempt to defeat the TMCC Network security systems.

Any violations of policy may lead to TMCC's Information Technology Department employing network filters and possibly terminating network access in order to protect the integrity and security of the campus network.

A. PASSWORD

All TMCC staff, faculty, and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

- All system-level passwords must be changed on at least a 120-day basis.
- All production system-level passwords must be changed on at least a 120-day basis.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines:

- It must be at least ten characters in length.
- It must contain at least one alphabetic, one numeric character and one special character.
- It must be significantly different from previous passwords.
- It cannot be the same as the user ID

- It cannot include the first, middle, or last name of the person issued the user ID.
- It cannot be a common word or name.
- It should not be information easily obtainable about you. This includes license plate, social security, telephone numbers, or street address.

B. WIRELESS

The purpose of this policy is to provide reliable and secure wireless network access.

This policy applies to all wireless network users at Turtle Mountain Community College

- TMCC is solely responsible for providing wireless networking services on campus. No other department may deploy wireless network access points or other wireless service on campus. Private wireless access points in the departments or offices are strictly prohibited.
- TMCC is responsible for maintaining a secure network and will deploy adequate security procedures to support wireless networking on campus.
- TMCC will provide temporary use of a wireless access point to support campus events.
- A "TMCC Staff" wireless network and a "TMCC Student" wireless network have been created. For a user to be able to access these wireless networks, the user must have an active, valid Turtle Mountain domain user account.
- Any "TMCC Guest" wireless network is created for public use. Any guest needing to connect a device via wireless network access shall first contact the Information Technology department in order for the device to be properly configured for accessing the campus network via wireless connection. Guest network access is offered for temporary use to guests of the Turtle Mountain community; it offers limited bandwidth and restricted access to TMCC services. TMCC Guest access should not be used by TMCC students, faculty or staff, except as needed for short term Internet access while resolving authenticated network access problems.
- A "TMCC Admin" wireless network is created for Information Technology use only.
- All wireless networks are controlled using policies and firewall rules, which prevent Internet/network activities not permitted

Consideration:

Wireless networking has bandwidth limitations compared to the wired network. The wireless network should be viewed as augmenting the wired network, to provide more flexible network use. Applications that require large

amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for wireless access.

6. ENFORCEMENT

Users who violate these policies may be denied access to institution computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the institution disciplinary procedures applicable to the user. The institution may suspend, block, or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of institution or other computing resources or to protect the institution from liability. The institution may also refer suspected violations of applicable law to appropriate law enforcement agencies.

7. ACKNOWLEDGEMENT

I acknowledge that I have received, read, and understand the Information Technology Appropriate Use Policy and agree to comply with said policy.

8. POLICY VERSION HISTORY

Version	Date	Description	Approved By
1.0	3/4/2022	Updated Draft	Technology Committee