INFORMATION TECHNOLOGY POLICIES

As Amended by the Tohono O'odham Community College Board of Trustees
On November 12, 2020

These policies supersede and replace prior IT policies. None of these policies may be amended or altered in any way by oral statements. Only written amendments by authorized management officials and approved by the TOCC Board of Trustees will constitute changes to the content in this document.

ACKNOWLEDGEMENT FORM

This Manual includes the authorized policies for Information Technology for TOCC. The policies provide clear standards for the appropriate use of IT resources, promote institutional efficiency and effectiveness, enhance individual accountability for ethical and lawful use, and help mitigate cyber security risks. The policies apply for all users of TOCC's IT Resources including faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, collaborators, and volunteers wherever located.

All Information Technology users must agree to comply with the IT policies and acknowledge knowledge and understanding of the policies by signing the following form.

Please fill out the form and return it to the TOCC Information Technology Department.

ACKNOWLEDGEMENT FORM
Tohono O'odham Community College Information Technology Policies

This is to acknowledge that I have received a copy of the Tohono O'odham Community College Information Technology Policies. I understand that I will be required to sign a new Acknowledgement Form each time it is updated.

_____ Hard Copy

_____ Electronic version.

I will immediately familiarize myself with the information in this policy. If I have questions or there are parts of these policies that I do not understand I will ask for clarification from my supervisor or from Human Resources.

_____

Print Name

_____ _____

Signature Date

NOTE: This page will be provided to employees as a separate document to fill out, sign and return to the TOCC Department. It may be submitted electronically or as a hard copy.

TABLE OF CONTENTS

INTRODUCTION

The Tohono O'odham Community College Information Technology (IT) Department is responsible for ensuring that TOCC students and employees have the electronic equipment and capacity to perform their academic work and employment responsibilities; to ensure that TOCC has adequate internet connectivity; to support programs for instructor online and in classroom instruction connectivity with students; to conduct ongoing maintenance of equipment and systems; and to plan for increased electronic technology capacity. This policy manual documents the policies and procedures for IT staff to administer, and for TOCC staff and students to use TOCC electronic equipment, systems, and programs.

1. Definitions and Purpose

a. "Technology" refers to any use of internet-based desktop, laptop, tablets, and smartphone applications that are connected to or associated with TOCC. The Information Technology Department policies encourage the use of internet-based services for TOCC related purposes for students and staff and on TOCC related web spaces.

b. TOCC provides a wide variety of computing and networking resources to all members of the community. Access to computers, computing systems, and networks owned by TOCC is a privilege which imposes certain responsibilities and obligations, and which is granted subject to TOCC policies and codes, and tribal, and federal laws. All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources, including wireless. The purpose of this policy is to promote the efficient, ethical, and lawful use of TOCC's computer and network resources.

c. "Social media" refers to any Web-based and mobile technologies that enable individuals or entities to disseminate or receive information, communicate, or otherwise interact. The term includes email, texting, messaging, social networking, blogging, micro-blogging, bulletin boards, Facebook, LinkedIn, Twitter, YouTube, Instagram, Snapchat, and other similar social media platforms and apps.

d. TOCC recognizes and embraces the power of social media, and the opportunity those tools provide to communicate with the TOCC community, including students, faculty, staff, parents, alumni, and other interested parties. It is important to recognize, however, that the use of social media at or concerning TOCC is governed by the same laws, policies, rules of conduct and etiquette that apply to all other activities at or concerning TOCC.

2. General guidelines for use of Information Technology

a. Individuals using computer resources belonging to TOCC must act in a responsible manner, in compliance with law and institutional policies, and with respect for the rights of others using a shared resource. The right of free expression and academic inquiry is tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, ownership of data, and security of information.

b. IT policies do not prohibit employees from using social media to discuss among themselves, even in terms that may be critical of the College, any protected activities relating to the terms and conditions of their employment.

c. Users of TOCC technology implicitly agree not to use technology to engage in harassment or intimidation or use computer and network resources for unlawful acts. Using TOCC's computer or network resources for illegal activities is strictly prohibited. Unlawful use of the College's computer and network resources can expose the individual user and the college to damages claims or potential criminal liability. Unlawful uses may include, but are not limited to, harassment and intimidation of individuals on the basis of race, sex, religion, ethnicity, sexual orientation, or disability; obscenity; child pornography; threats; theft; attempting unauthorized access to data; attempting to breach security measures on any electronic communications software or system; attempting to intercept electronic communication transmissions without proper authority; and violation of intellectual property or defamation laws. Do not use computer systems to send, post, or display slanderous or defamatory messages, text, graphics, or images. By using TOCC's computer and network services, each user accepts the responsibility to become informed about, and to comply with, all applicable laws and policies.

d. Use of TOCC technology use implies an agreement to use computer and network resources efficiently. Computing resources are finite and must be shared. Users may use the College computer and network resources for incidental personal purposes, provided that such use does not:
    - Unreasonably interfere with the use of computing and network resources by other users, or with TOCC's operation of computing and network resources;
    - Interfere with the user's employment or other obligations to the college; or
    - Violate this policy or other applicable policy or law. TOCC retains the right to set priorities on use of the system, and to limit recreational or personal uses when such uses could reasonably be expected to cause, directly or indirectly, strain on any computing facilities, to interfere with research, instructional, or administrative computing requirements, or to violate applicable policies or laws. Examples of inappropriate use include circumventing the editor or moderator to post messages to private (closed) list serves, sending "chain letters" or engaging in pyramid schemes, or engaging in unauthorized peer- to-peer file sharing. Sending "spam" or posting inappropriate promotional or commercial messages to discussion groups or bulletin boards, is not permitted.

A. INFORMATION TECHNOLOGY DEPARTMENT

1. Department Responsibilities

The responsibility of the IT Department includes but is not limited to:

- Maintaining and repairing computer systems to ensure business productivity in a timely manner.
- Securing information systems.
- Providing a backup system for data stored on the servers.
- Respecting the Confidentiality of information.
- Using Administrative system passwords on computers designated by the Systems Technician.
- Keeping doors locked to restricted areas.

- Accessing information only if it is necessary to resolve an issue, or investigate violations of the computer use policy.
- Reporting criminal activity to the appropriate authorities.
- Notifying users when making system changes that affect them. This will be done in a manner where the users have time to prepare and voice any concerns about the changes.
- Approving all requested TOCC software before purchase to ensure compatibility.
- Keeping an inventory of all information technology equipment including but not limited to: computers, monitors, printers, scanners, presentation systems, external drives, servers, software, computer accessories and telephone communication equipment.
- Preparation of a disaster recovery plan.
- Implementation of a disaster recovery plan when data cannot be retrieved from servers.

2. Software

The following software is supported by the TOCC IT Department.

- Microsoft Windows
- Microsoft Office 365
- Google G-Suite
- Jenzabar EX
- Canvas
- Paychex Flex
- Adobe

Other software needed for College operations may be added by the IT Department by request of a staff or faculty member and approval by the appropriate supervisor and IT Department.

3. Rights of the IT Department

To perform its duties, the TOCC IT Department reserves the right to perform the following activities:

- IT may routinely monitor and log computer traffic on the network as well as inspect files of specific users on their computers for evidence of violation of policy or law.
- IT has the right to control or refuse access to anyone who violates the computer use policies.

4. Individual Responsibilities

The following list includes responsibilities for which TOCC users are responsible. They are designed to ensure computing security, efficiency, and respect for other TOCC employees and for students.

- Respect the privacy and personal rights of others. Accessing files, directories, or email of others without authorization is prohibited.
- Respect the needs of others and only use a fair share of computing resources.
- Use printing resources responsibly, using two-sided options when feasible.
- Users shall report any violations of the computer use policy to the TOCC Information and Technology department
- Users who find security holes on the TOCC system are obligated to report them to the IT Department

- Flash drives, external hard drives, or other media with Confidential Information must be in a secured location.
- Flash drives, external storage drives, or other media that once contained confidential information must be properly erased or destroyed so that their information cannot be recovered by others.
- Screens must be oriented to prevent unauthorized people from reading sensitive information when possible.
- Documents should be saved to "My Documents" on TOCC computers as they are backed up into the Google Drive Backup Sync program. Documents created on the computer desktop should be saved in "My Documents" regularly to ensure that they are not lost if there is a computer malfunction.

5. Rules

The following is a list of rules relating to IT that TOCC users must follow.

- Theft of Computer Equipment, media, software, or data is prohibited.
- The act of deliberately attempting to degrade performance of the Computing system, damage it, or steal information is prohibited.
- Printers are to be used for College use only.
- All devices on the TOCC network must conform to the computer use policy.
- Use of the TOCC computing system is to be used for only TOCC related work. Personal use of software purchased by TOCC is prohibited unless approved by the appropriate supervisor and the IT department.

B. ACCOUNTS AND PASSWORDS

1. Accounts

Email account require a username and password to access resources on the computer network and on computers. For those employees hired under contract an email account will be created on the day the contract is signed. For those employees who are not hired under contract an email account will be established on the first day of employment. Employee accounts will remain active during the term of employment. When there is a separation from employment the Human Resources Department will notify the IT Department the date of separation, or in the case of termination just before the termination meeting, when to disable the email account.

For instructors including adjunct instructors if the instructor does not teach for two terms excluding summer sessions the account will be suspended until they resume teaching.

Student email accounts will be created when a student completes a TOCC application for enrollment and is accepted as a student. If a new student has not registered for classes after 60 days the account will be deleted. Student accounts will be closed after the student graduates, transfers, or has not registered for classes for 60 days.

Accounts with extensive permissions to the TOCC computing system or access to confidential information through the TOCC computing system are to be used only in the performance of job duties.

Interception, theft, and/or decryption of system or user passwords is prohibited.
Employees and students leaving TOCC shall discontinue use of TOCC technology upon termination of employment. Access to the Electronic Information System (EIS) will be removed.

Partners, affiliates, or other college collaborators may provide access to non-TOCC IT resources or services governed by third-party appropriate use policies, statements, or standards. Authorized Users shall comply with these requirements, unless doing so would violate applicable law or policy.

2. Passwords

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of TOCC resources. All users, (staff, students, guests, contractors, and vendors) with access to TOCC systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3. Securing email accounts

Employees and students must use the following practices to secure accounts:

- Avoid storing passwords around the office area where others can find and use the password for unauthorized access.
- Accounts with extensive privileges to the TOCC computer system shall choose passwords that are sufficient, meaning a mixture of letters and numbers of no less than eight characters. The use of symbols is also recommended.
- Password Length should be a minimum of 8 characters and a maximum of 20 characters in length and must contain special characters, all of which are may be used but are not required.
- Do not store passwords in unsecured locations.
- Computers must be to a point that requires a new log on whenever employees leave their work area.
- New passwords are required when the IT Department sets a regular schedule to change passwords.
- Avoid sharing of usernames and passwords, unless concluded necessary by the IT Department.
- Do not use a password that is the same or like one you use on any other websites/systems.
- Do not use a single word, for example, password, or a commonly used phrase like Iloveyou.
- Make passwords hard to guess and avoid names and birthdays of self, friends and family, favorite bands, and often used phrases for example.
- Avoid personal information including name, important dates, pets, context-specific words, such as the name of the service, the username, and derivatives thereof.
- Be aware that the IT Department sets the limit on the number of failed login attempts.

4. Third Party Vendors

Third Party vendors are only allowed access to production data to resolve problems with their own software or hardware. These parties are subject to the TOCC computer use policies where applicable.

C. DATA ACCESS AND USE

1. Guidelines for Data Usage

- The President's Office and the Finance Department must be consulted to ensure that appropriate contract language regarding protection of data is incorporated into any agreement.
- The IT Department will work with Operations to ensure that appropriate facilities are provided for protection of data equipment.
- Legally Restricted Information in paper form must be stored in locked or otherwise secured areas when not in active use. Legally Restricted Information in electronic form must be stored in secure designated data centers or, if authorized to be stored elsewhere, only in encrypted (or similarly protected) form. It must not be stored on desktop, laptop or other portable devices or media without encryption or similar protection.
- Reports and communications should not include Legally Restricted Information unless essential to perform the function for which the communication is made. Transmission of Legally Restricted Data must be by secure methods. If Legally Restricted Data is transmitted by e-mail or other electronic transmission, it must be encrypted or otherwise adequately protected. Contact the Information Technology Department for advice and assistance.
- When a record containing Legally Restricted Information is no longer needed, it must be disposed of in a manner that makes the Legally Restricted Data no longer readable or recoverable. Paper records containing Legally Restricted Data must be shredded. Destruction of electronic records containing Legally Restricted Data must include deleting from its storage location.

2. Restrictions

Access to information owned by TOCC is generally broadly consistent with the concept of academic freedom and the open nature of the institution. However, there are types of information where access must be restricted and caution in handling and storing the information is necessary. The disclosure and use of the following types of information is restricted by law.

- Social Security Numbers (SSN)
- Patient Protected Health Information (HIPAA)
- Student Information (FERPA)
- Financial Account, Credit and Debit Card Information
- Employee Personnel Records

Legally Restricted Information must be stored, used and disclosed to others only on a need to know basis to permit the individual faculty or staff member to perform their TOCC functions for which the information was acquired and for which it is maintained. Access to legally restricted information is carefully safeguarded. Protection of Legally Restricted Information from disclosure to or unauthorized access by anyone who does not have a legitimate need to access the information

is a primary responsibility of the staff person supervising the TOCC Division or Department that houses the information.

Alternatives to using Legally Restricted Information should be identified and used whenever possible. Disclosure of Legally Restricted Information to a third-party agent or vendor is permitted only if the agent or vendor assumes a legally binding obligation to safeguard the use and disclosure of the information. The electronic exchange of Legally Restricted Information outside of TOCC must have proper approval. In addition, the appropriate Administrators must be consulted to ensure appropriate security controls are employed. The Administrators include the TOCC President, Dean for Sustainability, and IT Manager.

D. EMAIL AND ELECTRONIC COMMUNICATION

1. Email Guidelines

When using TOCC email accounts, employees and students must conform to the following policies:

- Clearly and rightfully identify the user who sent it.
- Emails must be written in a professional manner and may not be used to send rude, obscene, harassing, or illegal materials.
- Mass mailings may only be used for business and for TOCC student activities. Chain letters and other types of non-business mailings are strictly prohibited.
- Users shall not use any means to alter, conceal, or misinform their true identity.
- Use of TOCC computing resources to obtain unauthorized access or intent to damage or disturb external computing systems is prohibited.
- Downloads from untrustworthy sources are prohibited. This includes “Freeware” such as games, organizer utilities, clock utilities, etc. If these programs are found on the computer of an employee or a student they will be removed by the IT Department. Only programs needed for productivity will be supported (see supported software section).
- The IT Department is the only TOCC entity authorized to repair or contract to repair computers and technology systems. Individuals authorized by the TOCC IT Department may perform basic troubleshooting.
- Authorized IT personnel may see the contents of emails while troubleshooting or performing maintenance work on the email system.

2. Conditions for Permitting Inspection, Monitoring, or Disclosure

TOCC may permit the inspection, monitoring, or disclosure of email, computer files, and network connections when:

- Required or permitted by law, including public records law, or by subpoena or court order.
- TOCC or its designated agent has reason to believe that a violation of law or policy has occurred.
- It is necessary to monitor and preserve the functioning and integrity of the e-mail system or related computer systems or facilities.

All computer users agree to cooperate and comply with TOCC requests for access to and copies of email messages or data when access or disclosure is authorized by this policy or required or allowed by law or other applicable policies.

3. Prohibition Against Activities Placing Strain on Facilities

Activities that may strain the e-mail or network facilities more than can be reasonably expected are not allowed. These activities include but are not limited to: sending chain letters; "spam," or the widespread dissemination of unsolicited e-mail; and "letter bombs" to resend the same email repeatedly to one or more recipients.

4. Personal Software

Software can only be installed on TOCC devices by the IT Department.
Personal software is not installed on TOCC device unless approved by the employee's supervisor and IT Manager for a work-related project. If it is approved the software must be installed by the IT Department. This policy is not intended to restrict the downloading of files from Internet sources or online services authorized by Instructors for courses and for employees in the performance of their job duties.

E. INTERNET USAGE

This policy and related regulation and exhibits define the acceptable uses of technology and technological education efforts. TOCC provides Electronic Information Services (EIS) to staff, instructors, students, and other users who acquire access privilege through association with TOCC. The use of these services shall be in support of instructional, informational, communication, research, administrative, and educational goals of the College

Electronic Information Services include, but are not limited to networks (e.g., LAN, WAN, Internet), telephone systems/voice mail, electronic mail, databases, hardware, software, Google Apps for G Suite, Microsoft 365, additional services, and any computer-accessible source of information. These include, but are not limited to hard drives, external drives, or other electronic sources/media (e.g., Universal Serial Bus [USB] flash drives, iPads), and similar equipment as it may become available.

To assure that the TOCC EIS are used in an appropriate manner and for the educational purposes intended, TOCC requires anyone who uses the TOCC EIS to follow this policy and related regulations for appropriate use.

The IT Department shall determine steps, including the use of firewall and/or proxy, that must be taken to promote the safety and security of the use of the College's online computer network when using electronic mail, social media hangouts, and other forms of direct electronic communications. Technology protection measures shall protect against Internet access by both staff and students to visual depictions that are obscene, child pornography or, with respect to the use of computers by minors, harmful to minors. Safety and security mechanisms shall include online monitoring activities.

It is the policy of TOCC to:

- prevent access to or transmission of inappropriate material via the EIS, the Internet, electronic mail, or other forms of direct communication;
- prevent unauthorized access and other unlawful online activity;

- prevent unauthorized online disclosure, use, or dissemination of personal identification information of students.

TOCC may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. TOCC is not responsible for any service interruptions, changes, or consequences. TOCC reserves the right to establish rules and regulations as necessary for the efficient operation of the electronic information services.
TOCC does not assume liability for information retrieved via the EIS nor does it assume any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

Internet Safety

Focus on the prevention of inappropriate network usage includes unauthorized access, including "hacking," and other unlawful activities; unauthorized disclosure, use and dissemination of personal identification information regarding minors.
Limits, controls, and prohibitions shall be placed on employees and students including:

- Access to inappropriate matters.
- Safety and security in direct electronic communications.
- Unauthorized online access or activities.
- Unauthorized disclosure, use and dissemination of personal information.

3. Education, Supervision and Monitoring
It is the responsibility of all TOCC employees to be knowledgeable of the College policies, regulations, and procedures. Further, it is the responsibility of all employees, to the extent prudent to an individual's assignment, to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy. The College shall provide for appropriate training for employees and students who use the EIS and have access to the Internet.

Training provided shall be designed to promote the commitment to:

- The standards and acceptable use of the College network and Internet services as set forth in policy;
- Student safety regarding use of the Internet, appropriate behavior while using, but not limited to, such things as social networking web sites, online opportunities, and chat rooms; proper use of personal devices; cyberbullying awareness and response.

4. Employees and Students are Strictly Prohibited from the Following Activities and Shall Not:

- Engage in unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications.
- Engage in unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications.
- Use College-owned or leased computer equipment “to access, download, print, or store any information, infrastructure, files, or services that depict nudity, sexual activity, sexual excitement, or sexual acts” unless the employee has written approval from the “agency head”

- Make personal use of the Internet and e-mail services in a way that impedes or interferes with the conduct of College business. In general, only incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—should be used to attend to personal matters.
- Use TOCC computer resources for private business or commercial activities, fund-raising, or advertising on behalf of non-TOCC organizations. Nor are they permitted to engage in the unauthorized reselling of TOCC computer resources or the unauthorized use of College trademarks or logos.
- Place links on the College website that generate or have the potential to generate revenue for TOCC or any private business (including click trade or banner advertising) without the approval of the TOCC IT Department.. This is not a general prohibition against links to commercial websites.
- Alter addresses, uniform resource locator (URL), or take other action that masks the tocc.edu domain as a host site.
- Intercept or attempt to intercept communications by parties not authorized or intended to receive them or general unauthorized anonymous and anonymous communications. Misrepresent or forge the identity of the sender or the source of an electronic communication; unauthorized acquisition, attempts to acquire, or use of another person's password or the computer account of others.
- Modify or delete another person's files or account or alter the content of a message originating from another person or computer with intent to deceive.
- Compromise the privacy or security of electronic information through an intentional or reckless manner or make TOCC computing resources available to individuals not affiliated with TOCC without approval of an authorized TOCC administrator.
- Deliberately interfere with or disrupt computer or network accounts, services, or equipment of others, propagate computer "worms" and "viruses," send electronic chain mail, or send "broadcast" messages to large numbers of individuals or hosts that are not College related.
- Disrupt electronic networks through negligent or intentional conduct; attempt to alter any TOCC computing or networking components (including, but not limited to, bridges, routers, and switches).

F. SOCIAL MEDIA

1. Guidelines for posting to social media sites

When posting to any TOCC social media site, or communicating with members of the TOCC community on *any* site, including through an employee's and student's own personal account or when using their own phone, computer, or other device, the lists of Best Practices and Prohibited Practices must be followed.

a. **Best Practices:**

- Treat past and present co-workers and other individuals with respect regardless of different opinions. Avoid posting materials or comments that may be perceived as offensive, demeaning, inappropriate, threatening, abusive, or a violation of TOCC's policies against discrimination, harassment, or hostility as it pertains to age, race, gender, sexual orientation,

and gender preference.

- Protect co-workers and students by refraining from sharing their confidential or proprietary information, including conversations, statements, photos, or videos, unless given written permission to do so. Employees must follow the applicable federal requirements such as Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA).
- When posting to social media sites, employees and students must honor the copyright and intellectual property rights of others, including the College.
- Remember that laws and TOCC policies governing inappropriate conduct such as sexual (or other) harassment, bullying, discrimination, defamation, infringement of copyright and trademark rights, and unauthorized disclosure of student records and other confidential and private information apply to communications by TOCC students, faculty and staff through social media.
- If, from a social media post, it is clear that a College employee or student is mentioning the College, or it is reasonably clear referring to the College or a position taken by the College, and also express a political opinion or an opinion regarding the College's positions or actions, the employee or student must specifically note that the opinion expressed is their personal opinion and not the College's position.
- Ensure that information posted is factual and accurate as the Internet archives everything. Even deleted postings can be searched, copied, and forwarded. It is virtually impossible to eliminate posted comments or pictures from the Internet. Employees and students must not post anything in anger that would deviate from best practices.
- Employees and students must identify their views on personal sites as their own and must not suggest that such views are those of TOCC. No one may represent themselves as a spokesperson for the College unless given direct permission to do so by the President or a designee.
- Employees and students must accurately disclose their relationship to the College if endorsing the College. When using TOCC sites or acting within the scope of College responsibilities employees may only endorse TOCC, its programs, or its services if authorized to do so by the College.
- Carefully consider the accuracy, clarity, length (brief is better) and tone of written comments before posting them. Posts on social media sites should protect the College's institutional voice by remaining professional in tone and in good taste. Remember, posts may last forever, and viewers will take screen shots as evidence.
- Employees and students must sign posts with their real name and indicate their relationship to TOCC. They may not use pseudonyms or post anonymously.
- All users should respect the views of others, even if they disagree.
- Be truthful, accurate and complete in describing TOCC programs and services.
- Strive to be accountable to TOCC audiences via regular updates and prompt responses when appropriate.
- Employees and students must obey the Terms of Service of any social media site or platform in which they participate.
- Whenever appropriate, share content directly from TOCC's social media pages rather than duplicating it. When content is directly shared, it is linked back to TOCC's social media accounts. This facilitates the efforts to analyze social media traffic and engagement (e.g. "likes" and comments). In addition, posts originating from TOCC will have the appropriate

links attached to bring the viewer back to the website or coordinating landing page.

- When TOCC faculty use social media as a means of student participation in course work, they also need to provide a practical and appropriate alternative for students who may be unable or reluctant to utilize that social media platform. For example, some students may not be comfortable with opening a Facebook account.
- TOCC cannot legally prohibit employees from interacting with students on social media. However, TOCC administrators encourage staff and faculty to exercise caution and good judgement if they choose to friend students on social media. Faculty and staff may choose to create a separate professional or course-focused Facebook page if they wish to connect with students on a social media platform to encourage discussions and dialogue. It is important for all staff and faculty to exercise sound judgment and to interact with students in a way that a reasonable person would find appropriate.

b. Prohibited Practices:

- Never use social media to harass, threaten, insult, defame or bully another person or entity and never use social media to engage in any unlawful act, including but not limited to gambling, identity theft and other types of fraud.
- Never post or store content that is obscene, pornographic, defamatory, racist, excessively violent, harassing, threatening, bullying or otherwise objectionable or injurious. In addition, do not attempt to compromise the security of any TOCC social media site or use such site to operate an illegal lottery, gambling operation, or other illegal venture.
- Do not post copyrighted content (such as text, video, graphics, or sound files) without permission from the holder of the copyright. Even information that is widely available to the public (such as text, photographs, or other materials posted on the Internet) may be subject to copyright restrictions that prohibit unauthorized duplication or dissemination.
- Do not post trademarked content (such as logos, names, brands, symbols, and designs) without permission from the trademark owner. The "®" symbol indicates that the mark is federally registered and the owner has the exclusive right to use it. The "TM and SM" symbols indicate that the owner may have common-law rights, but the mark is not federally registered.
- Do not use the TOCC name, logo or trademarks for promotional announcements, advertising, product-related press releases or other commercial use, or to promote a product, cause, or political party or candidate.
- Do not disclose confidential College information, non-public strategies, student records, or personal information concerning (past or present) members of the TOCC community without proper authorization.
- Do not make false claims or representations about TOCC programs or services, and do not speculate or guess if the information is not verifiable.
- Do not spread gossip, rumors, or other unverified information. Do not assume that everything posted on a social media site is true.
- Do not spend excessive time using social media for personal purposes during working hours or use any TOCC social media sites, networks, equipment, or peripherals for unauthorized commercial purposes.
- Do not transmit chain letters, junk email, or bulk communications.
- Never be rude or argumentative or use inappropriate language. [Correct factual

inaccuracies but avoid negative exchanges whenever possible.]

- Do not represent personal opinions as institutionally endorsed by TOCC. If not authorized to post specific content on behalf of the College, then the following disclaimer must appear in a post: "These are my personal opinions and do not reflect the views of Tohono O'odham Community College."
- Do not expect that posted content will remain private or that dissemination will necessarily be limited to the intended audience, even if accessing their own private account over the TOCC network or using TOCC equipment or peripherals
- Do not insult, disparage, disrespect, or defame the College or members of the TOCC community.
- Do not discuss legal issues or risks, or draw legal conclusions on pending legal or regulatory matters involving the College
- Do not post any information or conduct any online activity that may violate the Tohono O'odham Nation's or applicable federal laws or regulations. Any conduct that is impermissible under the law if expressed in any other form or forum is also impermissible if expressed through social media

2. Monitoring of Social Media by TOCC

TOCC is not responsible for monitoring or pre-screening content posted on its social media sites. Notwithstanding, TOCC reserves the right to monitor its sites and to remove, without notice, any content that TOCC determines to be harmful, offensive, commercial in nature, or otherwise in violation of law or this Policy. If employees and students become aware of objectionable content posted on a TOCC social media or of objectionable comments concerning the College that are posted on an unaffiliated site, they should notify the TOCC IT Department promptly, and not reply on behalf of the College. TOCC's IT Department will work with the appropriate department(s) as necessary to address the objectionable content.

3. TOCC Social Media Site Approval, Administration, and Requirements

a. **Authorization and Administration.**

TOCC social media sites may be administered on behalf of (a) TOCC as an institution; (b) individual programs or departments; (c) members of the faculty, in connection with a specific course; or (d) student organizations. The following policies must be followed:

- Any person or organization who seeks authorization for a new site will be expected to articulate an appropriate purpose of the site and a reasonable plan for managing its content. All new sites require approval from the IT Department.
- Institutional sites that represent TOCC must be authorized in advance by the President of TOCC.
- Sites administered by members of the faculty in connection with specific courses must be authorized by the Academic Dean or Dean for Sustainability.
- Sites sponsored by recognized student organizations in connection with specific activities must be authorized by the Academic Dean or Dean for Student Services.
- When naming pages or accounts, selecting profile pictures or icons, and selecting content to post, authorized TOCC sites that represent only a segment of the TOCC community (for example, an individual College program, department or course) should take care to avoid the appearance of representing the entire institution.

Names, profile images, and posts should all be clearly linked to the particular program, department, or course.

- Unauthorized use of the Tohono O'odham Community College name, logo, or trademarks without the express permission of an authorized official of the College is strictly prohibited.

b. Site Administration

Social media site administration is provided by the IT Manager, the Dean for Student Services and two staff members designated by the IT Manager

4. Posting to Social Media Sites Not Administered by Tohono O'odham Community College

a. TOCC is aware that members of the TOCC community may wish to express their personal ideas and opinions through private social media that are not administered by the College.

b. Employees must ensure that social media activity does not interfere with their work but may use them to express their thoughts or promote their ideas if they do not conflict with TOCC policies. Employees should refrain from sharing confidential or proprietary information about co-workers and students. All personal positions or opinions should be posted specifically as personal views and not those of the College.

5. Confidentiality

Certain College departments in possession of unique information such as personal data, student applications or employee's medical records or criminal histories, require specific guidelines for their release of information due to legal requirements. Employees should consider any information in these categories as confidential and covered by the College Confidentiality Agreement that the employee signs at the commencement of employment. Confidential information subject to the College's Confidentiality Agreement should be released only with the prior approval of the President and then only to the requesting individual, whose own records are involved or in response to a Court or administrative subpoena or authorized request.

If there is a question as to whether a person's right to know conflicts with maintaining confidentiality, the President will make the decision as to whether the information should be released.

Financial data regarding the College must be secured and released only as authorized by the designated supervisor in charge thereof. Employees of the College are expected to maintain confidentiality and are prohibited from using confidential financial information available for the benefit of themselves or others.

G. BRING YOUR OWN DEVICE

Bring your own device (BYOD) is the practice of allowing students to use their own computers and mobile devices to connect to TOCC related systems while on a TOCC campus and in class.

The policies do not apply to students using their own devices working remotely in online courses. The following policies apply:

- Devices must be a laptop or a convertible laptop/tablet. The best example of a convertible tablet is a two-in-one device.
- The student is solely responsible for the repair, maintenance, and updating of the device. The TOCC technology department will assist students in connecting the device to the wireless network, using the wireless printing system, and connecting to TOCC related websites.
- TOCC IT Department Staff will be available to verify minimum requirements.
- If a personal device is broken or sent off for repairs a TOCC computer, Chromebook, and iPad with a keyboard may be available as a loan.
- The following software capabilities must be available for coursework:
    - Ability to run Google Chrome Version 78+
    - Updated virus protection, if using PC or Mac. (TOCC recommends the free Windows Defender for Windows machines)
    - Security: Must have a password/passcode (login) to access the device. This is responsible computing. Students will be bound by the TOCC IT Policy related to passwords, security, and appropriate usage.
- TOCC recommends installing the Google Chrome browser as it works well with G Suite. Students collaborate with Google Docs and Microsoft 365 on a regular basis.
- Alternative browsers including Firefox, Internet Explorer, Opera, and other unlisted browsers are not supported by the TOCC internet system.
- The Operating System on the student's personal device is a matter of personal preference, but the device needs to be able to run the Google Chrome, Microsoft Edge, or Apple Safari Browser. Devices can run Windows, Mac OS, or Chrome OS if the minimum requirements listed here are met.
- Operating System:
    - Windows 8.1, 10
    - MacOS 10.11 or Higher
    - Chrome Version 78 or Higher
    - Battery life: 5 hours
    - Startup time: No longer than 120 seconds
    - Wireless: Integrated
    - Keyboard: Integrated, but can be wireless
    - Audio: Headphone jack with headphones/earbuds
    - Microphone: Integrated
    - Camera: Integrated
    - Processor: 1.6 GHZ or faster 64-bit processor
    - Memory: 4 GB RAM or higher
    - Disk Space: 16gb GB or higher
    - Screen Size: 10 inches or larger
    - Monitor Resolution: 1024 x 768
- Iphones, Android Phones, iPads, Kindles, Galaxy Tablets, and other tablet/eReaders are not supported as part of the BYOD program. Students are permitted to bring and use these as secondary devices at the discretion of the faculty but cannot be used as the primary personal device for classroom use.

H. VIDEO AND STREAMING

TOCC recognizes that movies and video content directly related to the instructional program may be of benefit for student viewing. Any movies or video content shown must be directly related to courses being taught and be in compliance with applicable copyright law and licensing agreements. When using movies and video content, the Instructor shall:

- Use approved movies and video content. Video content of this nature is typically not rated in the manner described in this regulation and can be used if the instructor determines, in their reasonable discretion, that all of the content is clearly appropriate for the students to whom it will be shown. If the instructor has any question about the appropriateness of any portion of the video content, the instructor should follow the procedure described below and seek prior administrative approval.
- Not use a personal video streaming account such as Netflix, Amazon Prime, Hulu, Disney, or others to display movies or video content.
- Not use personally obtained movies and video content licensed for home-use only.
- Display only reasonable and limited portions of a copyrighted work in compliance with the fair use exception described in further detail below unless licensing fees have been paid. (The larger the portion being used, the more likely the copyright violation.)
- Not use movies and video content for entertainment or rewards.

I. WEB PUBLISHING

TOCC recognizes the value and potential of publishing on the Internet. Faculty and staff are encouraged to create electronic home pages or other pages that seek to carry out official business and communication of TOCC's mission. All such pages must be accessible to the staff and students from an official website within TOCC. All staff publishers must adhere to the policies of the College and must comply with all relevant federal and state laws. Web pages shall not display personally identifiable student information unless explicit and verifiable written permission has been granted by the students.

Staff publishers will be responsible for maintaining their educational resource sites. Web pages must reflect positively upon TOCC. Web pages must include an e-mail address of the staff maintaining the page. E-mail addresses/links on web pages must be a tocc.edu address. The TOCC website is maintained under the supervision of the IT Department. Instructor web pages maintained by TOCC must be approved by the Academic Dean and the IT Department.

TOCC provides computer services and networking to enhance TOCC's educational and administrative processes, and to improve communication with the world community. Material that fails to meet established educational objectives or that is in violation of a provision of policy and administrative regulations will be removed.

J. COPYRIGHTED MATERIALS

The following summary of copyright law is provided to guide employees and students.

1. Copyright Protections

United States copyright law grants certain rights and protections to the creators and publishers of creative works. Creative works that can be protected by copyright law are numerous and varied, and include, but are not limited to, books, magazines, pictures, artwork, sculptures, music, movies, television shows, computer software, and video content. Generally, unless permission is received from the copyright owner, copying, creating derivative works from, and publicly displaying or performing copyrighted materials is prohibited.

Many copyright owners will issue licenses outlining acceptable terms of use of their copyrighted works. If such a license is properly obtained, the copyrighted work may be used according to the terms of the license. For example, colleges can legally show copyrighted entertainment movies for events or activities before or after the instructional day by obtaining a public performance site license.

2. Allowable Unlicensed Uses of Copyrighted Materials

There are exceptions to the general requirement that one must obtain a license to use some or all of a copyrighted work. Subject to various limitations, these exceptions allow instructors and students to use, without first obtaining a license, some portions and/or some types of copyrighted works during face-to-face teaching activities.

3. The Fair Use Exception

The "fair use" exception allows limited use of copyrighted works without the need to obtain permission from the copyright holder. Fair use must be evaluated on a case by case basis. The following criteria must be considered in determining application of the fair use exception:

- The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- The nature of the copyrighted work;
- The amount and substantiality of the portion used in relation to the copyrighted work as a whole. (The larger the portion used, the more likely the copyright violation); and
- The effect of the use upon the potential market for or value of the copyrighted work. (It is not typically fair use to make educational copies of works intended for educational use.)

K. VIOLATIONS OF IT POLICIES

Upon receiving notice of a violation, TOCC may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings. A person accused of a violation will be notified of the charge, at the appropriate time, and will have an opportunity to respond before any TOCC imposes a sanction. In addition to sanctions available under applicable law and TOCC policies, TOCC may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, TOCC administered computing rooms, and other services or facilities.

TOCC reserves the right, under circumstances it deems appropriate and subject to applicable laws and regulations, to impose disciplinary measures, up to and including dismissal from the College or termination of employment, upon students, faculty, or staff who use private social media sites or communications resources in violation of the Usage Guidelines in this policy or are deemed to interfere with the conduct of College business. Violations of this policy are subject to sanctions prescribed in, but not limited to, the following policies: TOCC Student Handbook, TOCC Personnel Handbook, and the TOCC Faculty Handbook.

Users who misuse TOCC's computing and network resources or who fail to comply with the college's written usage policies, regulations, and guidelines are subject to one or more of the following consequences:

- Temporary deactivation of computer/network access;
- Permanent deactivation of computer/network access;
- Disciplinary actions taken by the appropriate Dean or President and including suspension or expulsion from school or termination of employment;
- Subpoena of data files;
- Legal prosecution under applicable federal, tribal and/or state laws;
- Possible penalties under the law, including fines and imprisonment.