

# TELECOMMUNICATIONS USE POLICY

---

## 1. Introduction

---

This Telecommunications Use Policy governs the use of computers, networks and other telecommunication systems at Truckee Meadows Community College. As a user of these resources, you are responsible for reading and understanding this document. This document protects the consumers of computing resources, computing hardware and networks and system administrators.

TMCC recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This policy reflects these firmly held principles within the context of the TMCC's legal and other obligations.

## 2. Rights and Responsibilities

---

Computers, networks and telecommunication systems can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the system and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, Users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

## 3. Existing Legal Context

---

All existing laws (federal and state) and Nevada System of Higher Education (NSHE) regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. ([BOR Handbook, Title 4, Chapter 1](#))

Users do not own accounts on TMCC computers, but are granted the privilege of exclusive use. Under the Electronic Communications Privacy Act of 1986 (Title 18 U. S.C. section 2510 et. seq.), users are entitled to privacy regarding information contained on these accounts. This act, however, allows system administrators or other TMCC employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the TMCC or NSHE. For example, system administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information that may be used as evidence in a court of law. In addition, student files on TMCC computer facilities are considered "educational records" under the Family Educational Rights and Privacy Act of 1974 (Title 20 U.S.C. section 1232[g]).

Misuse of computing, networking, telecommunications or information resources may result in the loss of computing, network and/or telecommunication systems access. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable NSHE, TMCC, or campus policies, procedures, or collective bargaining agreements. Illegal production of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment. TMCC supports the policy of EDUCOM on "Software and Intellectual Rights."

## 4. Disclaimer

---

TMCC is not responsible for loss of information from computing misuse, malfunction of computing hardware, malfunction of computing software, or external contamination of data or programs. It cannot be guaranteed that, in all instances, copies of critical data will be retained for all systems. It is ultimately the responsibility of computer users to obtain secure backup copies of their own files for disaster recovery.

Both the nature of electronic communications and the public character of the TMCC's business make electronic communications less private than users may anticipate, and confidentiality of electronic communications should not be expected. Users, therefore, should exercise extreme caution in using electronic communications to communicate confidential or sensitive matters. The TMCC has the right to inspect, monitor, or disclose electronic communications that utilize any TMCC-owned equipment. Without prior notice and without consent, the TMCC may perform routine maintenance or system administration of computers and other electronic communications equipment which may result in observation of the contents of files and communications.

Electronic communications that utilize TMCC equipment, whether or not created or stored on TMCC equipment, may constitute a TMCC record subject to disclosure under state, federal or other laws, or as a result of litigation.

The TMCC cannot guarantee that users will not receive electronic communications they may find offensive, nor can the TMCC guarantee the authenticity of electronic communications received, or that electronic communications received were in fact sent by the purported sender. Users are solely responsible for materials they access and disseminate on the TMCC's telecommunications systems.

## 5. Telephone Systems

---

Telephone systems shall be accessed primarily for business purposes. TMCC personnel shall not make personal long distance telephone calls from TMCC telephones unless it is an emergency. In the case of an emergency, employees will use their personal identification code number provided by the central services department to make personal long distance telephone calls. On a monthly basis, employees will be made aware of their monthly personal long distance telephone charges. Employees are required to submit to the TMCC reimbursement for any personal long distance telephone charges on a monthly basis.

## 6. Security

---

TMCC is embracing the philosophy of security in depth. Although the emphasis of centralized security over decentralized access set reflects a major paradigm shift, every effort has been made to ensure essential services and research initiatives will not be negatively impacted. It is clear that consistency in firewall, wireless access and overall network management and rule establishment coupled with timely administration is essential for the TMCC to maintaining secure communications links and trusts. It is recognized that there will be times when exceptions to security rules may need to be granted on a temporary, semi-permanent or permanent basis; for these special cases, there is an additionally established procedure and policy for considering the implementation of firewall rule exceptions.

## 7. Enforcement

---

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the accounts or network. This may be done through electronic mail or in-person discussion and education.

Repeated minor infractions or misconduct that is more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior. The human resources director and/or the associate dean of

students will be notified of infractions depending on whether the infraction involves a TMCC employee or student. In addition, offenders will be referred to their sponsoring advisor, department, employer, or other appropriate TMCC office for further action. It will be the responsibility of the supervisor to inform the appropriate vice president. If the individual is a student, the matter may be referred to the dean of students for disciplinary action.

Infractions of this policy may give rise to disciplinary action under [NAC 284](#) and the "Prohibitions and Penalties" sections of the [State of Nevada Rules for State Personnel Administration](#), and [BOR Handbook, Title 2, Chapter 6](#). Any offense that violates local, state, or federal laws may result in the immediate loss of all TMCC telecommunication systems access privileges and will be referred to appropriate TMCC offices and/or law enforcement authorities.

With rights comes responsibility. Conduct that violates this policy includes, but is not limited to, the activities in the following list:

- Altering or attempting to alter files or systems without authorization.
- Attempting to alter any TMCC computing or network components without authorization or beyond one's level of authorization, including but not limited to bridges, routers, switches, wiring, and connections.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Connecting unauthorized equipment to the college network or computers.
- Deliberately wasting/overloading computing resources, such as printing excessive copies of a document.
- Displaying obscene, lewd, or sexually harassing images or text in a public computer, facility, or location that can be in view of others.
- Failing to submit reimbursement any personal long distance telephone charges on a monthly basis.
- Failing to use their personal identification code number to make long distance personal telephone calls.
- Failure to comply with authorized requests from designated TMCC officials to discontinue activities that threaten the operation or integrity of computers, systems or networks.
- Forging the identity of a user or machine in an electronic communication.
- Initiating or propagating electronic chain letters or inappropriate mass mailing. This includes, but is not limited to, multiple mailings to the TMCC Campus, newsgroups, mailing lists, or individuals.
- Intentionally or negligently performing an act that places an excessive load on a computer or network to the extent that other users may be denied service or the use of electronic networks or information systems may be disrupted.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms.
- Negligently or intentionally revealing passwords or otherwise permitting the use by others of TMCC-assigned accounts for computer and network access. Individual password security is the responsibility of each user. The user is responsible for all uses of their accounts, independent of authorization.
- Providing services or accounts on TMCC computers or via TMCC networks to other users from a personal computer unless required to meet the normal activities of students working as individuals or in collaborative groups to fulfill current course requirements.
- Registering a TMCC IP address with any other domain name or the TMCC name without authorization.
- Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing laws, NSHE, or TMCC regulations.
- Transmitting sensitive or confidential data over an unsecured wireless network.
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Unauthorized scanning of ports, computers and networks.
- Unauthorized use of a computer account or using college resources to gain unauthorized access to any computer system and/or using someone else's computer without their permission or otherwise utilizing network or system identification numbers, accounts or names that are not assigned for one's specific use.
- Using TMCC resources for commercial activity such as creating products or services for sale.

- Using electronic mail to harass or threaten others. This includes, but is not limited to, sending repeated, unwanted email to another user.
- Violating terms of applicable software licensing agreements, copyright laws, or their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.

## **NSHE computing resources policy, Approved 6/18/99**

### **I. Principles:**

---

Academic freedom in teaching and research and the right of freedom of speech for faculty, staff and students are fundamental principles of the Nevada System of Higher Education. Nothing in these policies limits or removes the right of free speech or the academic freedom of faculty, staff, and students engaged in the learning process, nor relaxes their responsibilities as members of the NSHE community. This computer resources policy seeks to achieve objectives necessary for the legitimate and proper use of the NSHE computing resources. It is intended that these ends should be achieved in ways that maximally respect the legitimate interests and rights of all computer users. The NSHE acknowledges its responsibilities to respect and advance free academic inquiry, free expression, reasonable expectations of privacy, due process, equal protection of the law, and legitimate claims of ownership of intellectual property. Each institution within NSHE may adopt further computing resources policies congruent with these principles.

### **II. Use of Computing Resources:**

---

The computing resources of the Nevada System of Higher Education are the property of the NSHE and are intended for support of the instructional, research, and administrative activities of system institutions. Examples of computing resources are system and campus computing facilities and networks, electronic mail, Internet services, lab facilities, office workstations and NSHE data. Users of NSHE computing services, data and facilities are responsible for appropriate and legal use.

Appropriate use of system computing resources means 1) respecting the rights of other computer users, 2) protecting the integrity of the physical and software facilities, 3) complying with all pertinent license and contractual agreements, and 4) obeying all NSHE regulations and state and federal laws.

Students enrolled in kindergarten through twelfth grades using NSHE computing facilities and networks for K-12 classes and activities must abide by school district and NSHE policies. K-12 students enrolled in NSHE courses will be treated as NSHE students and therefore must abide by NSHE policies.

Inappropriate use of computing or networking resources, as defined in this policy, may result in the loss of computing privileges. If a violation of appropriate use occurs, a warning will first be given, notifying the individual that their action violates policy or law and that their access will be suspended if the action continues. All NSHE Code and campus by-laws shall be followed if the need to suspend computing privileges from faculty, staff, or students occurs. However, if the security and operation of the computing systems or networks are jeopardized, access may be immediately cancelled.

In congruence with NRS 281.481, NSHE employees shall not use the NSHE computer resources to benefit their personal or financial interest. However, in accordance with NRS 281.481(7), limited use for personal purposes is allowable if the use does not interfere with the performance of an employee's duties, the cost and value related to use is nominal, and the use does not create the appearance of impropriety or of NSHE endorsement. Personal use shall not interfere with official institutional use. An employee who intentionally or negligently damages NSHE computing resources shall be held responsible for the resultant expense. These policies also apply to NSHE students.

A NSHE account given to students, faculty, and staff is for the use only of the person to whom it is given. Unauthorized access or privileges are not allowed. In electronic communication such as mail, the user should not misrepresent his or her identity. No user should attempt to disrupt services of the computing and network systems, including the knowing

propagation of computer viruses or the bombardment of individuals, groups, or the system with numerous repeated unwanted messages.

### III. Privacy Issues:

---

The NSHE provides security measures to protect the integrity and privacy of electronic information such as administrative data, individual data, personal files and electronic mail. All FERPA (Family Educational Rights and Privacy Act) requirements are followed. Users must not circumvent security measures. While computing resources are system property and all rights are retained regarding them, these rights will be balanced with a reasonable and legitimate expectation that technical staff and administrators will not casually or routinely monitor traffic content or search files. The content of files shall only be examined when there is a reasonable suspicion of wrongdoing or computer misconduct as determined by the institution president or his or her designee. Examination of files shall be limited to the matter under consideration.

Disciplinary matters involving computer and network systems shall be handled in accordance with Chapter 6 of the NSHE Code. Within the limits of the capability of the computer system, NSHE shall protect the legitimate privacy interests of users and those about whom information is stored.

### IV. Software Management Responsibility:

---

Users of NSHE computing resources are responsible for the legality of their software at all times. Data or software written or created by NSHE staff or students must not be copied or used without the author's permission. All commercial software must be licensed. Users must be aware of the license conditions and should never copy software without consulting the license agreement. Evidence of legal ownership is required. Individual employees and students are responsible for not installing illegal computer software on NSHE equipment. All NSHE institutions will enforce copyright laws and provide appropriate software management controls.

### V. Internet Policy:

---

You should be aware that the NSHE agreement with the provider for Internet access prohibits:

1. attempted unauthorized access or destruction of any customers' information;
2. knowingly engaging in any activities that will cause a denial-of-service to any customers; and
3. using products and services to interfere with the use of the network by other customers or authorized users, or in violation of the law or in aid of any unlawful act.

### VI. Legal Context:

---

All federal and state laws, NSHE Code and regulations, and individual institutional policies are applicable to computer and network usage. Violation of NSHE Code provisions may result in disciplinary action. Violation of applicable laws may result in civil damages and criminal sanctions under state and federal law. Applicable statutes are summarized by System Computing Services and NSHE legal staff and can be found on the NSHE homepage on the World Wide Web. This list is by no means exhaustive, but it provides the individual user an overview of the provisions of these and other statutes as they relate to computer use.