2500
ACCEPTABLE COMPUTER USE

1. General

As an institution of higher learning, Northern New Mexico College encourages, supports, and protects freedom of expression as well as an open environment to pursue scholarly inquiry and to share information. Access to information technology, in general, and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. The computing and network resources, services, and facilities of the College are limited and should be used wisely and carefully with consideration for the needs of others. As with any resource, there is a possibility of misuse. In an attempt to prevent or mitigate such misuse, this policy outlines proper and improper behaviors, defines misuse and incidental use, explains rights and responsibilities, and briefly reviews the repercussions of violating these codes of conduct.

Northern New Mexico College provides computing services to College faculty, staff, and students. These services are intended primarily for furthering the education, research, and public service mission of the College and may not be used for commercial purposes or profit-making. This Policy is applicable to all individuals using College-owned or -controlled computer equipment, communications equipment, data -network (wired and wireless), storage devices, and computer-related facilities, whether such persons are students, staff, or faculty. All College policies including, but not limited to, intellectual property protection, privacy, misuse of College equipment, sexual harassment, hostile work environment, data security, and confidentiality shall apply to the use of computing services.

1.1. Departmental Computer Use Policies and Procedures

Individual departments within the College may define “conditions of use” for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines, and/or restrictions. Such policies may not relax, or subtract from, this policy. Where such “conditions of use” exist, the enforcement mechanisms defined within these departmental statements shall apply. Individual departments are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the department administrator shall provide the cognizant vice president and the College Director of IT with a copy of such supplementary policies prior to their implementation. Where the use of external networks is involved, policies governing such use also are applicable and must be adhered to.

1.2. Computing Services

For the purposes of this policy computing services include the following:

- All College data, information, and information systems (including computer applications used by the College that are hosted elsewhere),
- All College computer hardware, software, multi-media, and communication services including all computer resources, communications equipment, and data networks—wired and wireless,
- All College telephones, mobile phones, smart phones, storage devices, and personal digital assistants, and
- All digital assets owned, managed or leased by the College and any that may be entrusted to the College by other organizations (e.g. cloud computing services as well as any other future computing device, service, system, or application.)

2. Rights and Responsibilities

The use of College computing services is a privilege. Users who have been granted this privilege must use the services in an appropriate, ethical, and lawful manner. Unauthorized access is prohibited and may be monitored and reported to the proper authorities. The College does not provide a warranty, either expressly or implied, for the computing services provided. The College reserves the right to limit a computer user's session if there are insufficient resources, and to cancel, restart, log, record, review or hold a job, process, network connection or program to protect or improve system or network performance if necessary.
The College network is large and complex and supports mission critical functions such as patient care, payroll, academic classes, Internet access, and electronic mail.

2.1. User Responsibilities

Users are responsible for all their activities using computing services and shall respect the intended use of such services. Whenever a computing facility has specific rules and regulations that govern the use of equipment at that site and users shall comply with those rules and regulations governing the use of such computing facilities and equipment in addition to any over-arching College policies such as this one. Users must understand and keep up-to-date with this policy and other applicable College computer policies and procedures.

Users shall respect all copyrights including software copyrights. Users shall not reproduce copyrighted work without the owner's permission. In accordance with copyright laws, including the Digital Millennium Copyright Act, college's legal counsel, upon receipt of official notice from a copyright owner, may authorize blocking access to information alleged to be in violation of another's copyright. If after an investigation information is determined by college's legal counsel to be in violation of another's copyright, such information will be deleted from College computing systems.

2.1.1. Copyrights and Software Licenses

Users of College computing resources must comply with copyright law and the terms of licensing agreements, including software licenses, before accessing or using copyrighted material on the Internet. Users are responsible for determining what licenses or permissions are necessary and for obtaining such permissions or licenses before using College computing resources. Purchased music, movies, software, and other multi-media files usually include a license that gives you permission to make copies, change formats or to share the file with others.

Generally, software which the College is not permitted or not licensed to use shall not be installed on College computing services; however, software which has been personally-acquired is permitted to be installed on College computing services so long as the user who has installed the software is able to prove s/he is legally permitted to do so (this is usually done by retaining and providing the license upon request.)

File-sharing applications often involve the unlawful copying or distribution of copyrighted material without permission or license from the copyright owner. Anyone who sends or receives files using file-sharing software may be engaging in an unlawful act unless (a) the user is the copyright owner or has permission from the copyright owner, (b) the material is in the public domain, or (c) fair use or another exception to copyright law applies.

Upon receipt of information alleging that a user may be engaged in unauthorized file sharing of copyrighted material or is in violation of licensing obligations or other copyright law, the College may, without notice, immediately suspend, block or restrict access to an account. The College may take such action when it appears necessary in order to protect the security or integrity of computing resources, or to protect the College from liability.

Users who violate copyright law or license terms may be denied access to College computing resources, and may be subject to other sanctions and disciplinary actions, including but not limited to expulsion or discharge from the College.
In accordance with its legal obligations, the College will continue to develop plans to combat the unauthorized use and distribution of copyrighted materials, including the possible use of technological deterrents. The College will also continue to provide information on alternatives to illegal file-sharing.

2.1.3. Software Developed Internally

College personnel may develop computer programs using College computing resources. Such software may be subject to the College's Intellectual Property Policy.

2.1.4. Computer Security

Individuals using computing services are responsible for keeping accounts and passwords confidential and for safeguarding all College data and information, especially those covered by state and federal regulations such as FERPA, regardless if it is being stored on College computing resources, stored on non-college resources, or being transmitted over communication networks.

2.1.5. Computer Accounts and Passwords

The College, through IT and departments, provides computer accounts to authorized users for access to various College systems. These accounts are a means of operator identification and passwords are used as a security measure. An individual's computer account shall not be shared. Account use is a privilege, not a right.

2.1.5.1. Account Authentication

Passwords, PINs, and other identifiers authenticate the user's identity and match the user to the privileges granted on College computers, computer networks, systems and computing resources. A password is a security measure designed to prevent unauthorized persons from logging on with another person's computer account and reading or changing data accessible to that user. Users should create passwords carefully and handle them with care and attention. For this security feature to be effective, the user must protect the secrecy of his/her password. Each user should:

- choose a password that is s minimum of eight characters to include a number, capital letter, and special character
- change his/her password at a minimum of every ninety (90
  0) days and at any time the user believes the password may have been compromised,
- avoid writing the password down, and
- not disclose or share the password with anyone.

Similar measures apply to all authentication methods such as PINs.

2.1.5.2 Account Termination and Locking

When an individual leaves the College, his or her account(s) must be locked as soon as reasonably possible and, subsequently, deleted within a reasonable time. If misuse or theft is detected or suspected, account(s) will be locked according to the College's procedures.

2.1.6. Computer and Data Security

Everyone at the College shares responsibility for the security of computer equipment, data, information and computing resources.

2.1.6.1. Physical Security

Everyone is responsible for the proper use and protection of College computer resources. Examples of protection measures include:

- locking areas after business hours or at other times when not in use;
- taking special precautions for high-value, portable equipment;
- locking up documents and computing resources when not in use; and

2.1.6.2. Information Security

Security of data and information is an essential responsibility of computer system managers and users alike. For example, users are responsible for:

- ensuring the routine backup of their files;
- using data only for approved College purposes; and
- ensuring the security and validity of information transferred from College systems.

2.1.7. Computer Viruses and Anti-virus Software

All College departments, though department heads or designees, shall ensure anti-virus software is installed on College computing resources when technically possible and that the software is active and kept up to date. This requirement applies to all computer servers as well as all desktop and laptop computers. This will help ensure that College computing services and digital assets are not compromised, misused, deleted or destroyed.

3. Unacceptable Computer Use

The College reserves the right to block access to any external electronic resources that are deemed in violation of this Policy. If it is determined, after an investigation by the appropriate office, that the user violated federal or state law, rules or regulations or College policy by misusing College computing services. The College will disclose illegal or unauthorized activities to appropriate College personnel and/or law enforcement agencies.

3.1. Security Violations

Users shall not

- attempt to defeat or circumvent any security measures, controls, accounts, or record-keeping systems;
- use computing services to gain unauthorized access to Northern's or anyone else's computing services;
- intentionally alter, misappropriate, dismantle, disfigure, disable or destroy any computing information and/or services;
- knowingly distribute malware (i.e. computer viruses, worms, Trojans, or other rogue programs).

3.2. Legal Violations

Users shall not use computing services:

- for unlawful purposes, including fraudulent, threatening, defamatory, harassing, or obscene communications;
- to invade the privacy rights of anyone;
- to disclose student records in violation of FERPA;
- to access other computing services (i.e. other Northern computers or computer systems for unauthorized purposes;
- to access or disclose financial information in violation of the Gramm-Leach-Bliley Act or the College's Information Security Program;
- to access or disclose any non-public or personally identifiable information about a patient, employee, or student without having a legitimate College purpose
- to violate College policy, state law, or federal law, including but not limited to copyright laws.

3.3. Other Misuse

Users shall not use computing services:

- in violation of any College contractual obligation, including limitations defined in software and other licensing agreements;
- in a way that suggests College endorsement of any commercial product (unless a legal agreement exists and any communication or computing activity has been pre-approved by an appropriate vice president);
- to conceal one's identity when using computing services, except when the option of anonymous access is explicitly authorized,
- to possess or distribute obscene or pornographic material unrelated to College instruction, research, or business needs (students are excluded from this provision);
- to masquerade or impersonate another,
- by physically or electrically attaching any device to a College computer, communications devices, or network connection that negatively impacts the performance of any other College computing service;
- to send chain letters, pyramid schemes or unauthorized mass mailings;
- to send non-work or non-class related information to an individual who requests the information not be sent, or
- to send commercial or personal advertisements, solicitations, or promotions.

Users should understand that, due to their nature, electronic communications can be intentionally or unintentionally viewed by others or forwarded to others, and are therefore inherently not private. In addition, addressing errors, system malfunctions, and system management may result in communications being viewed and/or read by other individuals and/or system administrators.

In electronic communications, users must state whether they are speaking for themselves or in an official capacity for the College. Electronic communications that represent the College sent to non-Northern addresses must be done in a professional manner.

4. Incidental Personal Use
The College allows incidental personal use of computing services. Such use must not interfere with an employee fulfilling his or her job responsibilities, consume significant time or resources, interfere with other users' access to resources, be excessive as determined by management, or otherwise violated any federal or state laws, any individual college or departmental policies or codes of conduct, or College policies. Each department should document and communicate what use is acceptable.

5. Privacy Limitations
Users of College computing services, including managers, supervisors, and systems administrators shall respect and protect the privacy of others, in accordance with all applicable state and federal laws, regulations and College policies. Although the College is committed to protect individual and information privacy, the College cannot guarantee the security or privacy of correspondence and information stored and transmitted through College computer networks and systems. Since confidential information is often stored on desktop machines, displayed on screens, or printed on paper that could be in public view, users need to control access by:

- using passwords;
- turning screens away from public view;
- logging out of systems when leaving the work area;
- shredding reports containing private information prior to disposal; and
- clearing confidential information off desks in public areas.

While the College does not routinely monitor individual usage of its computing services, the normal operation and maintenance of the College's computing services require the backup and storage of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendering of services. Similarly, the College does not, in the regular course of business, monitor the content of computing services on its various networks. However, suspicious aggregate behavior, official requests from authorities, forensic evaluation or discovery for purposes of civil litigation, or indications of a security incident, for example, can cause network activities or computing services to be reviewed. It is the right of the College to monitor and review any activities on its resources. It is best, therefore, to assume that any and all actions taken or activities performed using College computing services are not private.

The College may also access and examine the account (e.g. any and all computer accounts on any College computing resource, e-mail boxes, file shares, local or networked storage) of an individual user under the following circumstances and conditions:

- if necessary to comply with federal or state law, or
- if there is reasonable suspicion that a law or College policy has been violated and the examination of the account is needed to investigate the apparent violation, or
- as part of an investigation involving an administrative claim or charge, arbitration or litigation, or if required to preserve public health and safety.

Requests for access based on reasonable suspicion must be approved in writing, in advance, by the cognizant vice president. If access to a faculty member's account is being requested, the President of the Faculty Senate must be notified in conjunction with the request for approval. Each request must specify the purpose of access and such access will be limited to information related to the purpose for which access was granted. If such access is being requested by a vice president, access must be approved by the President. If such access is being requested by the President, access must be approved by the Northern Board of Regents. The Regents' Internal Auditing Policy authorizes the College Audit Department full and unrestricted access to all College records, including but not limited to those contained in computer files, discs, and hard drives.

Accessing an employee's computer files for work-related, non-investigatory purposes (i.e., to retrieve a file or document needed while the employee who maintains the file or document is away from the office) is permitted and does not require authorization by a vice president as long as access is limited to the work-related need. When an employee separates from the College, work-related files, including but not limited to research data, as well as all records made or kept in any College electronic medium, remain the property of the College.

Communications and other documents made or kept by means of College computing services are generally subject to New Mexico's Inspection of Public Records Act to the same extent as they would be if made on paper. Therefore, all employees are urged to use the same discretion and good judgment in creating electronic documents as they would use in creating written paper documents.

6. Reporting Procedures.

Suspected violations of this policy (e.g. any incidents involving the unauthorized access to, destruction of, or misuse of computing services by employees, faculty or students) must be brought to the attention of the dean, director, or department head, and the College IT Security Office. In the case of a criminal violation, the IT Office will notify Campus Security. Violations by non-employees will be referred to the appropriate authorities.

7. Sanctions

The misuse, unauthorized access to, or destruction of College computing services in violation of applicable laws or College policy may result in sanctions, including but not limited to withdrawal of use privilege; disciplinary action up to and including, expulsion from the College or discharge from a position; and legal prosecution.