



COMPUTER USE GUIDELINES

Original: August 1999
Revised: January 2000
Revised: July 2001
Revised: January 2002
Revised: July 2002
Revised: July 2004
Revised: June 2005
Revised: July 2006
Revised: August 2008
Revised August 2010

TABLE OF CONTENTS

INTRODUCTION	1
MISUSE	3
Examples of Misuse.....	3
COMPUTER ACCOUNTS	4
Initial Password.....	5
Student Data Storage	5
Wasteful Use of Resources.....	5
Student Email.....	6
Violation Procedures.....	7
Unauthorized Software	8
Wireless Internet Access.....	9
SOCIAL MEDIA	10
All Social Media Sites, Including Personal Sites	10
Best Practices	11
Institutional Social Media	11

INTRODUCTION

College owned or operated computing resources are provided for use by faculty, students and staff of Mesalands Community College. All faculty, students and staff are responsible for the use of Mesalands computing resources in an effective, efficient, ethical and lawful manner. The following guidelines relate to the use of these computing resources. Additional requirements and procedures may be required for the authorized use of specific College computing laboratories. (Any additional requirements or procedures will be posted in the respective areas.)

The College will make reasonable efforts to maintain the integrity and effective operation of its computer systems including email, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature of technology, the College can assure neither the privacy of an individual user's use of the College computer system resources nor the confidentiality of particular messages that may be created, transmitted, received or stored thereby. In addition, communications of College personnel that are sent by email constitute "correspondence" and, therefore, will be considered public record subject to public inspection. Additionally, files in user accounts are subject to the discovery process or subpoena. Email is stored as files and is, therefore, subject to the same rules and restrictions as any other files. Additionally, email is very easy to forward and any email sent can easily become a matter of general dissemination. Forwarding email from an account at the College to a private account with an internet service provider may make the private account subject to the same potential for discovery and subpoena during legal actions as is the account at the College. The College reserves the right to inspect and disclose the contents of email.

Mesalands Community College also reserves the right to view or scan any file or software stored on College computers or passing through the network, and will do so periodically as deemed necessary to protect the liability of the College and to audit use of College resources. Violations of policy that come to the attention of College officials during these and other activities will be acted upon. The College cannot and does not guarantee confidentiality of stored data. Users should be aware that use of one of the data networks, such as the Internet, and email and messages, will not necessarily remain confidential since those networks are configured to permit easy access to transmissions.

Computers and networks 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 systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Users are responsible to the College community as a whole to understand what information technology resources are available, to recognize that the members of the College community share them, and to refrain from acts that waste resources, prevent others from using them, harm resources or information, or abuse others.

Students may have the right to access information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. All existing laws (federal and state) and College 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.

Only College owned or Institutional Computing approved equipment may be attached to the local network.

All users are required to observe the proprietary rights of software owners and comply with all copyright laws, treaties and compacts of the United States and all laws of the state of New Mexico, including the New Mexico Computer Crimes Act, NMSA 1978, § 30-45-1 to 30-45-7.

MISUSE

Misuse of computing, networking, or information resources can result in the loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users will be held accountable for their conduct under any applicable College policy or procedure. Complaints alleging misuse of resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works including, but not limited to, images, text, or software, without permission of the owner, is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

EXAMPLES OF MISUSE

- Failure to obey the rules for the computer labs, such as no eating or drinking.
- Using a computer account other than your own or sharing the account of someone else.
- Giving your password to another user for the purpose of sharing your personal account.
- Using the College network to gain unauthorized access to any computer systems.
- Knowingly performing an act which interferes with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place an excessive load on a computer system or network.
- Manipulation, retrieval or dissemination of any material that is threatening, abusive, libelous, obscene or pornographic, whether in text, audio, or graphic form, regardless of intent.
- Willful destruction of data or software.
- Game playing by anyone is not allowed on Mesalands Community College's systems unless it is sanctioned during a scheduled class or student organization event.
- Using the electronic communications facilities (such as email or telephone, or systems with similar functions) to send fraudulent, harassing, obscene, indecent, profane, intimidating, or other unlawful messages are prohibited by federal law.
- Intentional use of any College resource for transmission of commercial or personal advertisements, solicitations, promotions, or destructive programs.

COMPUTER ACCOUNTS

Computing resources and accounts are owned by the College and are to be used only for College-related activities that support the mission, goals and purposes of the College.

All current Mesalands Community College students are provided computer accounts and, therefore, Internet access. Computer accounts are automatically created for all registered students. These guidelines are available for review online: <http://www.mesalands.edu/computeruse/>. Please contact Institutional Computing if you have any questions.

Courtesy accounts may only be authorized when they are related to official College business and activities. The College will not provide computer access to persons or entities not affiliated with the College, as that would violate New Mexico Constitution article 9, §14, which prohibits donations by the state to private individuals or entities.

Nonpayment of fees or withdrawal from classes will result in forfeiture of a student-user account.

NOTE: All student information and files are purged from the College computers after every semester.

ACCESSING YOUR STUDENT ACCOUNT

Student's user names will be their first and last name with first letters capitalized and no space between. Student accounts will be created using the name given at registration. In the event of a duplicate first and last name, Institutional Computing may use a middle initial, a shortened version of the first name, or any other combination of the user's name. Nicknames and aliases will not be allowed. For example:

Name	User Name
Joe Smith	JoeSmith
Joe Bob Brown	JoeBrown
Mary Beth Smith-Jones	MarySmith

INITIAL PASSWORD

Student default passwords will be set to their Mesalands Student ID Number. It is recommended that this default password be changed as soon as possible.

STUDENT DATA STORAGE

As a convenience, students are allotted storage on a network server to store personal class-related files. When a student logs into a campus computer a connection is made mapping the local M: drive to their shared area on the server.

The amount of storage space allotted by Institutional Computing will depend on current resources and enrollment. Should a student require more space in their shared folder, they may request a quota increase from Institutional Computing.

Upon receiving a request for quota increase Institutional Computing will evaluate the student's current usage to determine if the student is utilizing his/her space for academic purposes. Access to the students' shared network folder will be limited to the student and Institutional Computing. Institutional Computing makes no guarantee that student data on the network will be available or stored reliably. It remains the students' responsibility to retain backups of data they feel is critical. USB flash drives or "burning" to optical media may be used to store this data.

Mesalands Community College Institutional Computing is not responsible for lost or damaged data, storage device or portable devices. It is the responsibility of the user to ensure they have taken appropriate measures to safeguard their data by storing it on the M: drive or a USB flash drive. Users are advised that some computers are configured to delete all user data after a reboot.

HARRASING OR OBSCENE MATERIAL

Internet users are to refrain from displaying or distributing material (text, audio, or video) which is obscene, pornographic, threatening or harassing. This includes knowingly sending or receiving such materials via email through the Internet.

WASTEFUL USE OF RESOURCES

Users are to refrain from deliberately performing any act which will impair the operation of the computing resources of the College. Such acts include injecting computer viruses and sending excessively large mailings, large print jobs, batch programs, "junk mail" (including chain letters), etc. Those who use computing resources for recreation, entertainment, personal and extracurricular work are to yield to those who have course-related need for facilities.

STUDENT EMAIL

Mesalands Community College, through a partnership with Google, provides students with an email account. Student email accounts end with the Mesalands.net domain. Students are encouraged to check this email account frequently as College employees are required to utilize the Mesalands.net email addresses when contacting current students.

HELP WITH COMPUTER RESOURCES

To assist students in becoming familiar with the campus computers, a Computer Lab Assistant may be made available in one of the computer labs at posted times throughout the semester. The purpose of this Lab Assistant is to assist beginners with specific problems related to accessing computer resources. Institutional Computing will not do a person's homework nor teach computer related curriculum.

Students requiring assistance with computer-related homework should contact their Instructor or the Educational Services Center for tutoring and/or instruction.

Students experiencing difficulties with College computers or technology resources may contact Institutional Computing by email via support@mesalands.net.

PEER TO PEER FILE SHARING

H.R 4137, the Higher Education Opportunity Act (HEOA), is a reauthorization of the Higher Education Act. It includes provisions that are designed to reduce the illegal uploading and downloading of copyrighted works through peer-to-peer (P2P) file sharing. These provisions include requirements that:

- Institutions make an annual disclosure that informs students that the illegal distribution of copyrighted materials may subject them to criminal and civil penalties and describes the steps that institutions will take to detect and punish illegal distribution of copyrighted materials.
- Institutions certify to the Secretary of Education that they have developed plans to “effectively combat” the unauthorized distribution of copyrighted material.
- Institutions, “to the extent practicable,” offer alternatives to illegal file sharing.
- Institutions identify procedures for periodically reviewing the effectiveness of the plans to combat the unauthorized distribution of copyrighted materials.

In response to the requirements set forth by the HEOA Institutional Computing maintains a section of the [mesalands.edu](http://www.mesalands.edu) website dedicated to fulfilling the requirements of the HEOA, available at <http://www.mesalands.edu/p2p/>

VIOLATION PROCEEDURES

Individuals may report incidents of harassment or obscene material or abuse involving student use of the computer labs, email, or the Internet to Student Services. Referrals are made to the Dean of Student Services for possible disciplinary action when deemed necessary. Possible sanctions include the deletion from Mesalands Community College servers of materials or direct links to other locations on the Internet which are found to be obscene, loss of computer resources use, and/or other sanctions available within the judicial processes as outlined in the Student Handbook.

COMPUTER SPECIFICATIONS

With the wide variety of software and hardware available in the information world, it is essential that a set of institutional standards be implemented. Standards are necessary to allow for maximum compatibility among all users.

HARDWARE

Each new technology purchase brings a new level of capability and therefore complexity in the computers, printers, and support equipment purchased. In order to reduce the costs of support and supplies for a wider variety of computers the Institutional Computing department attempts to use the same vendor for computer and printer hardware. To assist in keeping this consistency, it is required that all computers and computer related equipment must be ordered through the Institutional Computing department. Hardware vendors are continually screened as to service, reliability, and quality of their products prior to purchase.

SOFTWARE

Institutional Computing maintains a defined set of software standards to ensure compatibility and usability of College computers. Any additions to this list of supported software must demonstrate a business or academic need and be approved and installed by Institutional Computing. Any software not listed here will be supported by Institutional Computing on a best effort basis.

Currently supported desktop software standards are as follows:

Operating System: Microsoft Windows XP or Microsoft Windows 7

Word Processing: Microsoft Office Word

Spreadsheet: Microsoft Office Excel

Database: Microsoft Office Access

Desktop Publishing: Microsoft Office Publisher

Presentation: Microsoft PowerPoint

Cloud Based Applications: Google Apps provided by Mesalands.net.

UNAUTHORIZED SOFTWARE

Software installed on the College computers is approved for use by Institutional Computing. **NO** additional software may be installed or executed. If there is a particular educational requirement for additional software, a request will be made through your instructor or supervisor as appropriate. This restriction applies to all software and upgrades.

WIRELESS INTERNET ACCESS

Institutional Computing will make a wireless network connections or Wi-Fi available for student usage. This allows students to connect to the Internet using their own laptop, notebook or other portable devices.

Because the wireless network is publicly available it is not secured by any means. Students must ensure they are not sharing any resources on their personal computers prior to connecting to the wireless network. Institutional Computing will not be liable for damages incurred as a result of using the wireless network.

User guidelines apply to usage of the wireless Internet. In the event user abuse is detected the violating user may have their access to the wireless network and institutional computers revoked.

COMPUTER SERVICES FOR USERS WITH DISABILITIES

In accordance with our mission and in compliance with the American Disabilities Act, Institutional Computing has computers in the computer labs available for users with disabilities.

In an effort to ensure access to computer resources and services to users with disabilities, Institutional Computing will provide any number of services upon request. The type and nature of the special assistance is usually determined by the request.

All special accommodations, beyond those already provided in the computer labs, must be requested through Student Services and follow established procedures.

SOCIAL MEDIA

Social media are powerful communications tools that have a significant impact on organizational and professional reputations. Because they blur the lines between personal voice and institutional voice, Mesalands Community College has crafted the following policy to help clarify how best to enhance and protect personal and professional reputations when participating in social media.

Social media is defined as media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Examples include, but are not limited to, LinkedIn, Twitter, Facebook, YouTube, and MySpace.

Both in professional and institutional roles, employees need to follow the same behavioral standards online as they would in real life. The same laws, professional expectations, and guidelines for interacting with students, parents, alumni, donors, media, and other College constituents apply online as in the real world. Employees are liable for anything they post to social media sites.

ALL SOCIAL MEDIA SITES, INCLUDING PERSONAL SITES

Protect confidential and proprietary information: Do not post confidential or proprietary information about Mesalands Community College, students, employees, or alumni. Employees must still follow the applicable federal requirements such as Family Education Rights and Privacy Act (FERPA). Adhere to all applicable College privacy and confidentiality policies. Employees who share confidential information do so at the risk of disciplinary action or termination.

Respect copyright and fair use: When posting, be mindful of the copyright and intellectual property rights of others and of the College. Questions related to fair use or copyrighted material can be directed to the Library.

Do not use College logos for endorsements: Do not use the Mesalands Community College logo or any other College images or iconography on personal social media sites. Do not use Mesalands Community College's name to promote a product, cause, or political party or candidate.

Respect College time and property: College computers and time on the job are reserved for College-related business as approved by supervisors and in accordance with the Computers Users Guidelines.

Terms of service: Obey the Terms of Service of any social media platform employed.

BEST PRACTICES

This section applies to those posting on behalf of an official College department, though the guidelines may be helpful for anyone posting on social media in any capacity.

Think twice before posting: Privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect both on the poster and the College. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. If you would not say it at a conference or to a member of the media, consider whether you should post it online. If you are unsure about posting something or responding to a comment, ask your supervisor for input or contact the College Director of Public Relations.

Strive for accuracy: Get the facts straight before posting them on social media. Review content for grammatical and spelling errors. This is especially important if posting on behalf of the College in any capacity. (See “Institutional Social Media” below.)

Be respectful: Understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the poster and/or the College and its institutional voice.

Remember your audience: Be aware that a presence in the social media world is or easily can be made available to the public at large. This includes prospective students, current students, prospective and/or current employers and colleagues, and peers. Consider this before publishing to ensure the post will not alienate, harm, or provoke any of these groups.

On personal sites, identify your views as your own. If you identify yourself as a College faculty or staff member online, it should be clear that the views expressed are not necessarily those of the institution.

Photography: Photographs posted on social media sites easily can be appropriated by visitors. Consider adding a watermark and/or posting images at 72 dpi and approximately 800x600 in resolution to protect your intellectual property. Images at that size are sufficient for viewing on the Web, but not suitable for printing. Remember that images produced by the College are not public property to be posted without the consent of the Public Relations Director.

INSTITUTIONAL SOCIAL MEDIA

If you post on behalf of an official College department, the following policies must be adhered to in addition to all policies and best practices listed above:

Notify the College: Departments or units that have a social media page or would like to start one should contact their supervisor for permission and guidance. All institutional pages must have a full-time appointed employee who is identified as being responsible for content. Ideally, this should be the head of the department.

Acknowledge who you are: If you are representing the College when posting on a social media platform, acknowledge this.

Have a plan: Departments should consider their messages, audiences, and goals, as well as a strategy for keeping information on social media sites up to date. The Public Relations Director can assist and advise you with your social media planning.

Link back to the College: Whenever possible, link back to the College website. Ideally, posts should be very brief, redirecting a visitor to content that resides within the College web environment. When linking to a news article check first to see whether you can link to a release on the College web page instead of to a publication or other media outlet.

Protect the institutional voice: Posts on social media sites should protect the College's institutional voice by remaining professional in tone and in good taste. No individual Mesalands Community College department should construe its social media site as representing the College as a whole. Consider this when naming pages or accounts, selecting a profile picture or icon, and selecting content to post names, profile images, and posts should all be clearly linked to the particular department rather than to the institution as a whole.