



**COMPUTER
USE
GUIDELINES
FOR STAFF**



COMPUTER USE GUIDELINES FOR STAFF

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

TABLE OF CONTENTS

INTRODUCTION	1
Misuse	2
Examples of Misuse	2
COMPUTER ACCOUNTS	3
Accessing Your Student Account	3
Student Roaming and Folder Redirection	3
Harassing and/or Obscene Material	4
Wasteful Use of Resources	4
Student Email	4
Help With Computer Resources	4
Violation Procedures	5
COMPUTER GUIDELINES	7
Hardware	7
Software	7
Operating System	7
Word Processing	7
Spreadsheet	7
Database	7
Desktop Publishing	7
Presentation Graphics	7
Unauthorized Software	8
Wireless Internet Access	8
Computer Services for Users With Disabilities	9
EXHIBIT 1* (Guidelines Acknowledgement)	11
APPENDIX A - EMPLOYEE GUIDELINES	13

*(This acknowledgment needs to be signed and submitted to the Institutional Computing office prior to receiving computer access.)

INTRODUCTION

Institutional Computing (IC) provides computing, networking, and information resources to Mesalands Community College students for work related to their courses.

NOTE: Mesalands Community College 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 electronic mail and messages, will not necessarily remain confidential since those networks are configured to permit fairly 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. Appendix A contains guidelines specific to employees and will be distributed accordingly.

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.

MISUSE

Misuse of computing, networking, or information resources will result in the loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable College or campus 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 campus network to gain unauthorized access to any computer systems.

Knowingly performing an act which will interfere 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. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms.

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 by an instructor during a scheduled class.

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. Also, the electronic communications facilities are not to be used for transmission of commercial or personal advertisements, solicitations, promotions, destructive programs, or any other unauthorized use.

COMPUTER ACCOUNTS

All current Mesalands Community College students may obtain computer accounts and therefore Internet access. Computer accounts are automatically created for all registered students. At registration, or at the cashier's office when paying registration fees, students will be given a copy of these guidelines and after reading them will be required to sign the acknowledgment form (Exhibit 1). Upon receipt of this form and notification that required fees have been paid, Institutional Computing will create the account. Returning students need to read the latest version of this set of Guidelines, checking for changes, and then sign another acknowledgement.

ACCESSING YOUR STUDENT ACCOUNT

Students' 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 or 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-Jones

Students, passwords will be initially set to their Social Security Number (with no dashes). However, students may request that Institutional Computing change it at a later date if they so desire. This assignment of user name and password is consistent with that used in WebCT, the College Distance Learning delivery program. It is hoped that this will help reduce the initial confusion about using the campus computing resources and WebCT.

STUDENT ROAMING PROFILE AND FOLDER REDIRECTION

Students are allotted storage on a network server to store personal files. When a student logs into a campus computer their profile will be transferred to the computer they log into. The *My Documents* folder and *Desktop* are all redirected to their shared folder on the network 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 student's 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 student's responsibility to retain backups of data they feel is critical. USB flash drives or "burning" to a CD or CD-R may be used to store this data.

HARASSING AND/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 does not provide on-campus email accounts for students. Students are able to use the already established commercial email providers on the Internet by using computers in the computer laboratories or the Library during regular scheduled open hours. Examples are services obtained through Yahoo or Hotmail.

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 computers. Any student requiring assistance with computer-related homework should contact their Instructor, Educational Services Center, or Success Center for tutoring and/or instruction.

VIOLATION PROCEDURES

Individuals may report incidents of harassment or obscene material or abuse involving student use of the computer labs 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 other sanctions available within the judicial processes as outlined in the Student Handbook.

COMPUTER GUIDELINES

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 is to allow for maximum compatibility among all users.

HARDWARE

The College purchases new equipment regularly to keep the staff and student units from becoming obsolete. As this is done over time, there is no campus-wide standard for a particular computer or printer. Each new 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

Currently our software standards that are in place are as follows:

Operating System: The current proven version of Windows should be the operating system in use on all computers today.

Word Processing: Microsoft Word is the College standard for word processing.

Spreadsheet: Microsoft Excel is the College standard for spreadsheet.

Database: Microsoft Access is the College standard for database software.

Desktop Publishing: The software of choice depends on the particular use for the document so Word, Publisher, PageMaker, etc., may be installed based upon demonstrated need.

Presentation Graphics: Microsoft PowerPoint is the College standard for presentation software.

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. In computer labs, users will find computers with large monitors and keyboards with large embossed keys to aid in readability.

All special accommodations, beyond that already provided in the computer labs, for students with disabilities must be requested through Student Services and follow established procedures.

EXHIBIT 1*

COMPUTER USE GUIDELINES ACKNOWLEDGMENT

I have received and reviewed in its entirety a copy of the Computer Use Guidelines and have had an opportunity to ask questions about it.

I understand that the Computer Use Guidelines is intended to provide guidelines that must be followed while using Mesalands Community College computing resources.

I further understand those actions which may be taken as a consequence of my failure to follow these guidelines.

Signature

Date

Name (**Print Neatly**)

Social Security Number

*Return this completed form to the Library or Student Services.
Accounts will become effective from the first day to the last day of the semester, inclusive.*

*(This acknowledgment needs to be signed and submitted to the Institutional Computing office prior to receiving computer access.)

APPENDIX A

EMPLOYEE GUIDELINES

APPENDIX A

EMPLOYEE GUIDELINES

COMPUTER AND INTERNET ACCOUNTS

College computer and network resources are for College business. Personal use is allowed if that use is not excessive and is within these guidelines. Such usage is also open to monitoring by the Institutional Computing personnel to insure compliance with these rules and to ensure use of email and Internet is not excessive.

Computer and Internet accounts are automatically created for all employees upon hiring and remain active as long as employed by Mesalands Community College. Institutional Computing will establish these accounts upon notification by Personnel.

Note: An acknowledgment form regarding these rules will be kept on file for all employees.

Game playing by employees is not allowed on Mesalands Community College's systems and games are not allowed to exist on campus computers. If an employee finds a game on a campus computer then Institutional Computing is to be notified so it can be removed.

INTERNET GUIDELINES

College employees have a high speed connection to the Internet on their computers available at times. The system has network tools installed to monitor for and protect employee computers against various viruses, worms and other threats, but employees can also avoid possible computer problems by not connecting to known web pages of hacker or other Internet underground type organizations as this is often where computers become infected. As previously stated, usage of this resource is monitored for abuse to insure both minimum personal usage and connection only to proper pages that are business related. This monitoring includes pages visited or attempted to visit, time on a particular page, and whether the page is one blocked by our Internet filter program. Abuse of these resources will be reported to an employee's supervisor.

EMAIL GUIDELINES

Staff Email

Authorized Mesalands Community College Staff are able to use their Internet connection for external email or the internal local area network for internal email. The employee email accounts are established by using first name and first letter of their last name@mesalands.edu such as:

use johns for John Smith and @mesalands.edu for the remainder, which becomes **johns@mesalands.edu** for the email address.

Because there is a finite amount of storage space for the messages, each user must minimize messages kept on the servers. This is done by frequently reading them and either deleting or transferring them to a personal folder on the computer hard drive for retention. At the end of the month messages that are necessary for some archival purpose should be saved to a "personal" folder on the local hard drive and deleted from the mail system. Institutional Computing can provide guidance on how to do this. The email system has established limits on email storage and will issue a warning prior to reaching this limit and shutting down a person's email.

Institutional Computing, under the direction of the Dean of Instructional Services, is currently monitoring email message traffic to insure it meets guidelines. This monitoring can and may include monitoring who is sending email, where email is being sent, how many messages are being sent, where email is coming from, and how many messages are being stored on the server. If deemed necessary, message content may be monitored. Employees shall follow the rules for email system usage found in the Institutional Style and Formatting Handbook. Appendix E of that document has a list of Do's and Don'ts and Appendix F has the email policy.

The following simple rules will help prevent your computer and possibly the network from being infected with email carried viruses, worms or other threats:

1. Do not open an email unless you know the sender/company that sent the email. Delete them immediately.
2. Do not open an attachment from a person or business unless you were expecting to receive it. Delete any email with attachments from unknown senders. Surprise attachments may not be from the sender it says it is from and may contain an infectious file that renders your system and perhaps the network inoperable. Telephone known senders of attachments that are a surprise to verify source.
3. Following these rules means you should only open email from senders you recognize and only open attachments you were already expecting.

Handling Sensitive Information

The increased occurrences of identity theft and new laws controlling an individual's private information require that the employees safeguard this information to avoid such losses so as to protect the employees and students.

Safeguarding this information requires that all employees taking such information off campus, stored in some electronic devices such as a flash/pen drive, zip drive, external hard drive, or a laptop computer must store that information in an encrypted state. This means that there is either a folder on the device or the entire device is encrypted and that is where the sensitive information is stored. That encryption is to be done using a program called TrueCrypt. This is a free program using open source standards. It has been certified for protection of information with up to a Top Secret classification by the government. Institutional Computing offers frequent training on this program and demonstrates its usage and safeguards as well as how to download and install the program. **Use of this safeguard is mandatory and must be implemented when such information is taken off campus for any reason.**

The basic guidelines that must be followed by the College are:

1. Privacy Act

The Privacy Act of 1974, Public Law No. 93-579, 88 Stat. 1897 (Dec. 31, 1974), codified in part at 5 U.S.C. § 552a, states in part,

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

There are specific exceptions for the record allowing the use of personal records:

For statistical purposes by the Census Bureau and the Bureau of Labor Statistics

For routine uses within a U.S. government agency

For archival purposes "as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government"

For law enforcement purposes

For Congressional investigations

Other administrative purposes

The Privacy Act mandates that each United States Government agency have in place an administrative and physical security system to prevent the unauthorized release of personal records.

The Computer Matching and Privacy Protection Act of 1988, P.L. 100–503, amended the Privacy Act of 1974 by adding certain protections for the subjects of Privacy Act records whose records are used in automated matching programs. These protections have been mandated to ensure:

Procedural uniformity in carrying out matching programs
Due process for subjects in order to protect their rights
Oversight of matching programs through the establishment of Data Integrity Boards at each agency engaging in matching to monitor the agency's matching activity.

2. Family Educational Rights and Privacy Act (FERPA)

FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

3. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA mandates the first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health care providers effective April 14, 2003. Developed by the Department of Health and Human Services (HHS), these new standards provide patients with

access to their medical records and more control over how their personal health information is used and disclosed.

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Privacy Rule standards address the use and disclosure of individuals' health information (called "covered entities" as well as standards for individuals' privacy rights to understand and control how their health information is used) referred to as "protected health information" by organizations subject to the Privacy Rule. Within HHS, the Office for Civil Rights (OCR) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

Procedures for Dealing with Employee Violations

Complaints of excessive personal use or of harassment or obscenity involving Mesalands Community College employees on campus computers will be made to Institutional Computing. Institutional Computing may also become aware of possible computer or policy abuse by referral to output from one of the system monitoring programs. In either case, Institutional Computing will investigate the computer, network, and Internet activity of that person and if findings are of concern they will be forwarded to the employee's supervisor. Possible sanctions include deletion of material or direct links to other locations on the Internet that are found to be obscene, loss or restriction of computer resource privileges, and other sanctions available within the *Personnel Handbook* or the *Faculty Handbook* as appropriate, up to and including termination.

