

Manhattan College

RESPONSIBLE USE OF COMPUTING AND INFORMATION SERVICES

Policy and Procedures

October, 1997

Version 1.07

Approved by Computer Governance Committee: March 18, 1997

Reviewed by Educational Affairs Commission and Referred to College Senate: April 30, 1997

Reviewed by College attorney: October 9, 1997

Approved by Board of Trustees: October 23, 1997

CONTENTS

	PAGE
INTRODUCTION	3
POLICY STATEMENT	3
REASON FOR POLICY	4
PERSONS AND ACTIONS AFFECTED	4
WHO SHOULD READ THIS POLICY	4
RELATED DOCUMENTS	5
CONTACTS	5
DEFINITIONS	6
KEY POLICY AREAS	7
PRIVACY	7
User IDs and Passwords	7
User Programs/Files	7
Administrative Databases	8
Network Tracking	8
Invasion of Privacy	8
COPYRIGHT AND COMMERCE	8
Fair Use and Public Domain Exceptions	9
HARASSMENT	10
POLICY ENFORCEMENT	11
Actions	11
Violations	11
REPORTING VIOLATIONS	12
Potential Consequences	12
Procedures for Systems or Network Administrators	13
APPENDIX A: General Areas of Violations	14
APPENDIX B: Specific Violations and Reporting Procedures	15

INTRODUCTION

Colleges and universities play an important role in the rapidly expanding field of computing technology. They provide an institutional base for enhancing competencies in computer usage, stimulating research and development of hardware and software, and enriching the capability of all academic programs to achieve excellence in teaching. Since higher education has an overarching goal of preparing students to assume responsibility for civic life and the further development of society, colleges and universities are duty bound to promote those virtues which build the character of the students and thus the common good of society. Thus, responsible use of computing technology must be carefully articulated due to the rapid developments in the field, developments which do not lend themselves easily to traditional categories of responsible use. Such responsibility is necessary to protect the rights of the community with regard to use of computer technology and is one facet of broader policies concerning academic integrity in higher education. But more is at stake than self interest in a smooth running institution. Responsible computer and information services use prepares the students for the above-mentioned goal of higher education - responsible citizenry - and enables faculty, administrators and staff to serve as role models for such responsible citizenry.

The mission of Manhattan College is to provide a contemporary, person-centered educational experience characterized by high academic standards, reflection on values and principles, and preparation for a life-long career. This policy is supportive of that mission.

This responsible use policy deals with three key areas: privacy, copyright and commerce, and harassment. It states who is covered by the policy, provides definitions of terminology used and detailed procedures to be followed for reporting violations.

POLICY STATEMENT

Manhattan College expects all members of its community to use computing and information services in a lawful, ethical and responsible manner. The College may restrict the use of its computers and network systems for electronic communications or other activities, in response to properly considered or otherwise adjudicated complaints presenting evidence of violations of College policies or codes, or of federal, state or local laws and regulations. Specifically, the College, through usual channels and established procedures, reserves the right to limit access to its computing and information services networks through College-owned or other computers and to remove or limit access to material posted on College-owned computers.

REASON FOR POLICY

The College adopts and promulgates this policy:

- *to enforce its policies regarding harassment, discrimination and the safety of individuals;*
- *to safeguard the integrity of computers, networks, and data either at Manhattan College or elsewhere;*
- *to ensure that use of electronic communications complies with all other College policies and procedures for maintaining public order and/or the educational environment;*
- *to prevent the posting of proprietary software or the posting of electronic copies of literary works or other intellectual property in disregard of copyright restrictions or contractual obligations;*
- *to protect the College against seriously damaging or legal consequences;*
- *to be in compliance with all governmental regulations regarding electronic communications.*

PERSONS AND ACTIONS AFFECTED

This policy applies to all members of the Manhattan College community including: faculty (full-time and part-time); administrators and staff both full-time and part-time; students (undergraduate and graduate; matriculated or non-matriculated) and to anyone else to whom computing/information services privileges utilizing resources of Manhattan College have been extended. The policies outlined herein shall apply when any member of the class as defined above: uses, accesses, or otherwise interacts with any of the computing facilities, hardware or software owned or licensed by Manhattan College, or any component of the College's network infrastructure or College systems whether such use, access, or interaction occurs on College property (including the College's residence halls) or from a remote off-campus site; or when anyone covered by this policy makes it appear to other individuals or entities that such use, access or interaction is associated in any way with Manhattan College. Any members of the Manhattan College community who do not accept the provisions of these policies may not use, access or otherwise interact with any of the College computing facilities.

WHO SHOULD READ THIS POLICY

All members of the Manhattan College community affected by this policy should read and understand it.

RELATED DOCUMENTS

<i>Manhattan College Documents</i>	<i>Other Related Material</i>
<i>Faculty Handbook</i>	<i>Electronic Communications Privacy Act of 1986 (P.L. 99-508; 18 U.S.C. 2510 et seq.)</i>
<i>Student Handbook, 1996-1998 (and as revised thereafter)</i>	<i>Family Educational Rights and Privacy Act of 1974 ("FERPA")</i>
<i>Procedure on Sexual Harassment (Presidential Memo of 3/1/89)</i>	<i>Telecommunications Act of 1996 (P.L. 104-104; 110 Stat. 56)</i>
<i>Policy and Procedures on Sexual Harassment and Discrimination (1987; revised 1997)</i>	<i>The Communications Decency Act of 1996 (Title V of the Telecommunications Act of 1996)</i>

(Drafting committee recommendation: It is strongly suggested that all other College policies and procedures be assembled in an organized fashion and referenced as appropriate herein including links to source documents.)

CONTACTS

Direct any general questions about this policy to your department's administrative office. If you have questions about specific issues or application of specific provisions, call the following offices:

Faculty Issues

Departmental Chairperson/Director; Dean; Provost - (718) 862-7303

Student Issues

Dean of Students - (718) 862-7932

Harassment

Affirmative Action Officer - (718) 862-7398

Electronic Communications or Network Issues

Director, Computer Center - (718) 862-7489; Asst. Provost - (718) 862-7268,

Copyright

Public Services Librarian - (718) 862-7167

DEFINITIONS

These definitions apply to these terms as they are used in this policy:

College Computers and Network Systems (College Systems): *Computers, terminals, networks, servers, switches, routers, hubs, PBXs and other similar devices that are owned or administered by the College and/or for which the College is responsible. Throughout this policy, the shortened term "College systems" is used to mean College computers and network systems.*

Departmental Policy Officer: *A person with responsibility for issues having policy implications for students and/or faculty and/or staff in a department, school, unit or other area of the College.*

Education Records: *Records specifically related to a student and maintained by an educational institution or a party acting on its behalf. These records are protected by and subject to the provisions of the Family Educational Rights and Privacy Act of 1974 ("FERPA").*

Electronic Communications: *The use of computers and network communications systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, or other such electronic tools. These communications are protected by and subject to the provisions of the Electronics Communications and Privacy Act of 1986."*

Harassment: *Repeated and unwanted actions that have the purpose or effect of creating an offensive, intimidating, demeaning or hostile educational or employment environment.*

Network Systems: *Includes voice, video and data networks, switches, routers, storage devices and other related systems and devices.*

Obscene: *The definition of obscenity follows the three-pronged test outlined by the US Supreme Court in Miller v. California, 413 U.S. 15 (1973). To be defined as obscene the material must (1) when considered as a whole by an average person, applying contemporary community standards, be judged to appeal to prurient interest, (2) depict or describe in a patently offensive way, sexual conduct specifically defined by applicable state law, and (3) lack serious literary, artistic, political or scientific value when the work is taken as a whole.*

Sexual Harassment: *Unwelcome sexual advances, requests for sexual favors, and other physical and/or expressive behavior of a sexual nature where: submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment or education; submission to or rejection of such conduct by an individual is used as the basis for academic or employment decisions affecting the individual; or such conduct has the purpose or effect of substantially interfering with an individual's academic or professional performance or creating an intimidating, hostile or demeaning employment or educational environment (see *Policy and Procedures on Sexual Harassment and Discrimination*).*

System or Network Administrator: *A College employee responsible for the operation or operating system environments of College systems.*

KEY POLICY AREAS

The key areas addressed below are recognized as important and necessary components of any organizational responsible computing use policy. These areas, however, are not exhaustive of all possible issues that are addressable within the framework and spirit of this policy statement. They may also not specifically address new and emerging technologies and possible abuses thereof. Manhattan College reserves the right to utilize procedures detailed herein to address other rights and violations that reasonably fall within the general areas outlined in Appendix B.

PRIVACY

Users Right to Privacy

Manhattan College shall respect the privacy of electronic communications and subscriber information of all users of College systems in accordance with the rules and procedures of the Electronic Communications and Privacy Act of 1986. However, in the event that an electronic communication contains information regarding or threats of bodily harm, Manhattan College reserves the right to divulge the identities of the parties involved in such communication to the proper authorities.

User IDs and Passwords

Manhattan College has an obligation to respect the privacy of all users of College systems. Each user number, log in name, account name, or any other user ID and associated password is the property of an individual student, staff, faculty, administrator, department, or administrative unit. No one shall use another's or authorize anyone else to use your user number, login name, user ID, or account name and password. No one shall use aliases, nicknames, pointers, or other electronic means to attempt to impersonate, redirect, or confuse others. No one shall use any means to capture information intended for others without permission of the intended recipient. Toward this end, owners accept the burden for stewardship and responsible use and dissemination of their user numbers, log in names, user IDs, and account names and passwords.

User Programs/Files

Programs and files belong to the owner of the user account or directory containing the programs and files. The files and their intellectual content are presumed to be private and confidential unless the owner has explicitly made them available to the public. If the owner allows access to files via file sharing, then it is presumed that the owner has waived his or her privacy rights but retains whatever copyright rights, if any, may exist. When necessary for the maintenance of a system or network, Computer Center personnel may gain access to files belonging to others. In such circumstances, Computer Center personnel are charged with holding individual-level data confidential except when that information is needed to resolve an accusation of a violation of the College's Responsible Use of Computing and Information Services policy. Programs and files that belong to the owner of a personal computer shall be subject to the same rights to privacy afforded to programs and files resident on any computer connected to the College systems.

Administrative Databases

The privacy and confidentiality of computer files also applies to information from the College's administrative databases. Improper access and/or dissemination of information from administrative databases is a violation of the College's Responsible Use of Computing and Information Services policies. To obtain information from or access to administrative databases requires written permission of an appropriate administrator. Access to such information through a duly assigned administrative account by the authorized account user shall constitute permitted use and proper access. Education records are protected by and subject to the provisions of the Family Educational Rights and Privacy Act of 1974 ("FERPA").

Network Tracking

Some programs gather information about users. If such information could directly or indirectly identify a person using the program, then, to the extent practicable, each user shall be warned and given a chance to leave the program before data collection begins. To avoid issuing excessive warning messages, an exception is made for host or network operating systems (which may keep logs of user account numbers, log in/disconnect times, amount of computer resources consumed, etc.) and for electronic mail software which keeps a log of users of the mail servers and summary information (but not the text of) messages sent and received.

Invasion of Privacy

College systems shall not be used to invade someone's privacy including: intrusion upon the solitude or seclusion of another or their private affairs or concerns; public disclosure of private facts; misappropriation of one's name or likeness (including College system user names); or knowingly or recklessly placing someone before the public in a false light. Any of these actions which would be highly offensive to a reasonable person may also subject the offending party to civil liability.

COPYRIGHT AND COMMERCE

Manhattan College respects an owner's interest in proprietary software or other assets pertaining to computers or network systems, even when such software or assets are not securely protected. Legitimate use of a computer or network system does not extend to whatever an individual is capable of doing with it.

Manhattan College adheres to US copyright laws, including the Copyright Act of 1974 and as amended, and thus does not condone any unfair (i.e. outside "fair use" exception) or otherwise unauthorized use of copyrighted information (including computer software) or the posting of electronic copies of literary works in disregard of copyright restrictions or contractual obligations. Anything less than adherence to the letter and the spirit of copyright law is unethical. The unauthorized use of any software or data which is protected by copyright is both unethical and illegal unless you are the owner of a license to use such data or program. The placement of misappropriated copyrighted material on College systems violates the College's policy on Responsible Use of Computing and Information Services.

Any use of College systems for commercial activity is generally incompatible with the College's legal status as a not-for-profit corporation chartered by the Regents of the University of the State of New

York and exempt from taxation under IRC 501(c)(3). Trafficking, for-profit or otherwise, in goods and/or services using College systems, when not compatible with the interests of Manhattan College, is generally inconsistent with Manhattan College's tax-exempt status and unrelated to its educational mission (Eg. sale of software via the Internet from the residence halls). Such activity violates this policy.

Fair Use and Public Domain Exceptions

One of the rights accorded to the owner of copyright is the right to reproduce or to authorize others to reproduce the work. This right is subject to certain limitations found in the Copyright Act (Title 17, U.S. Code). One of the more important limitations is the doctrine of "fair use." The statute contains a list of the various purposes for which the reproduction of a particular work may be considered "fair," such as criticism, comment, news reporting, teaching, scholarship, and research. It also sets out four factors to be considered in determining whether or not a particular use is fair:

- (1) the purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work.

The distinction between "fair use" and infringement may be unclear and not easily defined. There is no specific number of words, lines, or notes that may safely be taken without permission.

Acknowledging the source of the copyrighted material does not substitute for obtaining permission. The safest course is always to get permission from the copyright owner before using copyrighted material. When it is impracticable to obtain permission, use of copyrighted material shall be avoided unless the doctrine of "fair use" would clearly apply to the situation. One in a relative position of authority shall not knowingly or recklessly direct others to reproduce copyrighted material without properly secured permission from the copyright owner.

Material in the "public domain" (as generally defined by relevant laws or regulations) or software labeled generally as "freeware" is there for all to use and may be used freely. Material labeled as "shareware" may be subject to use restrictions and shall be used in accordance with the author's directions.

HARASSMENT

College systems are not to be used for harassment of any individual or groups or classes of individuals. Harassment is the sending, posting, forwarding, copying, relaying or otherwise transmitting or conveying intimidating, abusive, or other repeated and unwelcome messages after a request to stop.

College systems are not to be used for sexual harassment, a form of harassment that warrants its own policy and procedures (*Policy and Procedures on Sexual Harassment and Discrimination*) which are hereby incorporated by reference.

College systems are not to be used for viewing, downloading or transmitting obscene material. Such use may constitute sexual harassment.

College systems are not to be used for any purposes which are inconsistent with policies set forth in the Faculty and/or Student Handbooks.

POLICY ENFORCEMENT

Actions

1. The College reserves the right to limit access to its computers and network systems when applicable College policies or codes, contractual obligations, or state, federal or local laws are violated, but does not monitor or generally restrict the content of material transported to or from and/or across its system.
2. The College reserves the right to remove or limit access to material posted on College systems when applicable College policies or codes, contractual obligations, or state, federal or local laws are violated, but does not monitor the content of material posted on College systems.
3. The College does not monitor or generally restrict material residing on computers housed within a private domain or on non-College computers, whether or not such computers are attached to campus networks.

Violations

Violations of this policy may involve the use of College computer and network systems including electronic communication to:

- harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect action;
- impede, interfere with, impair, or otherwise cause harm to the activities of others;
- download, post to, or transport across College systems, material that is illegal, obscene, proprietary, in violation of College contractual agreements, or otherwise is damaging to the institution;
- harass or threaten or cause harm to classes of individuals, whether by direct or indirect action.

Note: As a matter of policy, the College protects expression by members of its community and does not wish to become an arbiter of what may be regarded as "offensive" by some members of the community. The College cannot protect individuals against the existence or receipt of material that may be offensive to them. However, in exceptional cases, the College, through usual channels and established procedures, may decide that such material directed to individuals or classes of individuals presents such a hostile environment that certain restrictive actions are warranted.

REPORTING VIOLATIONS

College community members shall report any violation of this policy to the Dean of Students Office (Jasper Hall- Room 222) or the appropriate person listed in Appendix B. Written statements can be submitted on the College's incident report forms (available in Dean of Students Office), in another written format of the reporter's choice or using one of the formats described in Appendix B. Any evidence to prove the allegations shall also be included with the report. Reports shall include as much detail as possible and shall include only factual information and be void of opinions and/or personal beliefs or suspicions. The general area of violation shall also be listed (see Appendix A). The Dean of Students can assist complainants in completing an incident report if necessary.

- A) When the alleged policy violator is a student, the report will be processed in accordance with the College Student Judicial Procedures as outlined in the Manhattan College Student Handbook.
- B) When the alleged policy violator is other than a student, the matter will be referred by the Dean of Students to the Vice President of Human Resources and/or the Provost for review and/or adjudication.
- C) The Dean of Students can act upon a complaint only if the violator is a member of the Manhattan College community. If the violator and/or sender of electronic messages is not a member of the Manhattan College community, the Dean of Students may assist the complainant by referring him/her to appropriate sources of help outside the College community.

Potential Consequences

Student violators may be subject to revocation of privileges and restitution for any damages resulting from their violations. Violations which were initiated from the residence halls may result in residence hall probation or expulsion from the residence halls. Other sanctions based on the severity of the violation(s) include disciplinary probation and/or expulsion from the College. Disciplinary sanctions for students are explained in detail in the Manhattan College Student Handbook.

Based on the severity of the violation, non-student College community members may be subject to reprimand, suspension or termination of employment. Restitution may be required for any damages resulting from their violation.

Procedures for Systems or Network Administrators

In certain cases, the priorities of protecting the College against seriously damaging consequences and/or safeguarding the integrity of computers, networks, and data either at the College or elsewhere, may make it imperative that temporary restrictive action be taken on an immediate basis. In such instances, systems or network administrators may take temporary restrictive action, preferably with the prior approval of the departmental policy officer, pending final adjudication by the College. All restrictive actions taken must be documented and justified in accordance with this policy. If there is no designated policy officer, or if the policy officer is not immediately available, the Dean of Students or Provost may be contacted for guidance or assistance.

The incident and any action taken shall be documented and this information protected as would any confidential material. This information may be subject to review by appropriate College authorities, so it is important that the information be current, complete and correct, maintained in an electronic database as appropriate, and easily retrievable.

Note: In some instances, such incident reports may, of necessity, include education records and as such will be protected from disclosure under the Family Educational Rights and Privacy Act of 1974 ("FERPA").

APPENDIX A

General Areas of Violations

A	Refusal to comply with any lawful directive of a clearly identifiable College official acting in the performance of his or her duties in the enforcement of this College policy
B	To forge, fraudulently alter, or willfully falsify or otherwise misuse College or non-College records ,documents, or communications including electronic communications or to possess such altered documents without proper authority
C	To harass, abuse or threaten another using College systems as the means for such harassment, abuse, or threats
D	To sexually harass another person
E	To violate copyright law ("fair use" is not a violation) using College systems
F	To traffic, for profit or otherwise, in goods and/or services, using College systems when incompatible with the interests of Manhattan College
G	To recklessly or maliciously interfere with or damage College systems, data, files, or other information
H	To invade someone's privacy and/or violate provisions of FERPA

APPENDIX B

Violations Targeting Individuals

VIOLATION	WHO FILES COMPLAINT	WHO RECEIVES COMPLAINT¹
The sending to an individual using College systems repeated and unwanted (harassing) communications including but not limited to communications that are sexual in nature or communications motivated by race, ethnicity, religion, gender or sexual orientation.	Targeted individual	-Dean of Students OR -Dept. Chair/Director; Dean of School; Provost -Affirmative Action Officer
The posting or other dissemination using College systems of personal, confidential or sensitive information about an individual(s) (Eg academic records; medical information; other information that if disseminated could have legal or damaging implications for the targeted person or individual). Personal expression is not meant to be limited or restricted by this policy, however a targeted person may nonetheless have other remedies against the violator.	Targeted individual OR System or network administrator	Dean of Students OR Dept. Chair/Director; Dean of School; Provost Affirmative Action Officer

¹For students: Dean of Students; for faculty: Dept. Chair/Director, Dean of School or Provost; for Staff/Administrators: Affirmative Action Officer
Complaint recipient shall also notify Director of Security

Violations Causing Harm to Activities of Others

VIOLATION	WHO FILES COMPLAINT	WHO RECEIVES COMPLAINT¹
Propagating chain E-mail; “jamming” or “bombing” electronic or voice mailboxes	System or network administrator OR Individual(s) affected	-Dean of Students OR -Dept. Chair/Director; Dean of School; Provost -Affirmative Action Officer
Forging, altering, or willfully falsifying electronic mail headers, directory information, or other electronic information	System or network administrator OR Individual(s) affected	-Dean of Students OR -Dept. Chair/Director; Dean of School; Provost -Affirmative Action Officer
Forging academic documents using electronic communications; hoarding, damaging or otherwise interfering with access to academic resources using College systems; misrepresentation one’s work using electronic communications; collusion on examinations, papers, or other academic work using College systems; fabrication of research data using College systems	Faculty member OR Individual whose work is stolen, misrepresented or otherwise compromised or damaged	-Dean of Students OR -Dept. Chair/Director; Dean of School; Provost -Affirmative Action Officer

¹For students: Dean of Students; for faculty: Dept. Chair/Director, Dean of School or Provost; for Staff/Administrators: Affirmative Action Officer
Complaint recipient shall also notify Director of Security

Violations Involving Illegal, Proprietary or Damaging Material

VIOLATION	WHO FILES COMPLAINT	WHO RECEIVES COMPLAINT¹
Electronically distributing or posting copyrighted material in violation of license restrictions or other contractual agreements; launching a computer “worm”, virus or other rogue program; knowingly or recklessly downloading illegal, proprietary or damaging material to College systems; transporting illegal, proprietary or damaging material across College systems	System or network administrator OR Anyone with evidence of a violation	-Dean of Students OR -Dept. Chair/Director; Dean of School; Provost -Affirmative Action Officer

¹For students: Dean of Students; for faculty: Dept. Chair/Director, Dean of School or Provost; for Staff/Administrators: Affirmative Action Officer
Complaint recipient shall also notify Director of Security

Violations Targeted at Classes of Individuals

VIOLATION	WHO FILES COMPLAINT	WHO RECEIVES COMPLAINT¹
Posting hate speech regarding a group’s race, ethnicity, religion, gender, or sexual orientation when such expression presents a hostile environment, constitutes harassment or otherwise warrants restrictive actions	System or network administrator OR Member or the targeted group	-Dean of Students OR -Dept. Chair/Director; Dean of School; Provost -Affirmative Action Officer

¹For students: Dean of Students; for faculty: Dept. Chair/Director, Dean of School or Provost; for Staff/Administrators: Affirmative Action Officer
Complaint recipient shall also notify Director of Security

