Be Responsible! MITnet Rules of Use

MITnet is a shared resource. The MITnet Rules of Use are intended to help you use MIT's computing and network facilities responsibly and safely. Complying with these rules assures that all use of the facilities is respon-sibile, legal, and respectful of privacy.

All network users are expected to follow these rules. ***Violations of the rules can subject offenders to Institute disciplinary proceedings and, in some cases, to state or federal prosecution.***

The following is a summary of the MITnet Rules of Use. You can find the full text in TechInfo in Computing—> Ethics/Policy—>Be Responsible! MITnet Rules of Use. If you have questions or want more information about any of these policies, send e-mail to <net-policy@mit.edu>.

Other MIT computer facilities with access to MITnet may have additional rules (check with your local system manager for details). External networks to which MITnet provides access have their own rules of use — also available on TechInfo.

1. Don't violate the intended use of MITnet.

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose.

Do not try to interfere with or alter the integrity of the system at large, restrict or deny legitimate users access to the system, or use MITnet for private financial gain.

2. Don't let anyone know your password(s).

Although your MITnet username identifies you to the whole Internet user community, your password must be known only by you. Anyone who knows both your username and password can use your account. If he or she does anything that affects the system, it will be traced back to your username. If your username or your account is used in an abusive or otherwise inappropriate manner, you can be held responsible.

3. Don't violate the privacy of other users.

The Electronic Communications Privacy Act (18 USC 2510 *et seq.*, as amended) and other federal laws protect the privacy of users of wire and electronic communications. As Section 3.17 of MIT's *Policies and Procedures* notes, "invasions of privacy can take many forms, often inadvertent or well-intended." Make sure that your use of MITnet does not violate the privacy of others, even unintentionally. Specifically:

- Don't try to access the files or directories of another user without clear authorization from that user. If you are in doubt, ask.
- Don't try to intercept or otherwise monitor any network communications not explicitly intended for you.
- Unless you know how to protect private data on a computer system, don't use the system to store personal information about individuals that they wouldn't normally disseminate freely themselves.
- Don't create any shared programs that secretly collect information about their users.
- Don't log into (or otherwise use) any remote workstation or computer not designated explicitly for public logins over the network — even if the configuration of the computer permits remote access — unless you have explicit permission from the owner and the user of that computer to log into that machine.

4. Don't copy or misuse copyrighted software or related material.

Many programs, and related materials such as documentation, are owned by individual users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. You must abide by these restrictions, because to do otherwise may subject you to civil or criminal prosecution.

Such restrictions may include prohibitions against copying programs or data, the resale of programs or data, or the use of them for non-educational purposes or for financial gain, and public disclosure of information about programs (e.g., source code) without the owner's authorization.

5. Don't use MITnet to harass anyone in any way.

"Harassment," according to MIT's *Policies and Procedures* (Section 3.16), is defined as: "any conduct, verbal or physical, on or off campus, which has the intent or effect of unreasonably interfering with an individual's or group's educational or work performance at MIT or which creates an intimidating, hostile or offensive educational, work or living environment...." Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group.

The Institute's harassment policy extends to the networked world. For example, sending e-mail or other electronic messages which unreasonably interfere with anyone's education or work at MIT may constitute harassment and is in violation of the intended use of the system.

If you feel harassed, seek assistance and resolution of the complaint. To report incidents of on-line harassment, send email to <stopit@mit.edu>. In emergency situations call Campus Police at x3-1212.

6. Don't overload the communication servers; in particular, don't abuse your e-mail or Zephyr privileges.

Guidelines on the use of e-mail are not based on etiquette alone: the e-mail system simply does not have the capacity to process a very large number of e-mail messages at once. If you send out an announcement to a huge list of recipients, the mail servers get overloaded, disks fill up, and staff intervention is required. The overall result is a negative impact on the quality of service provided for all users.

The proliferation of electronic chain letters is especially abusive to the mail system and the network. Chain letters waste valuable computing resources, and may be considered harassing.

A case in point:

I've been disturbed recently by sexually explicit pictures displayed on other's workstations. Is there anything that I or others can do to correct this? I'd like to know if it is contrary to Athena Rules of Use. Don't they forbid the use of MITnet f or transmitting "threatening or harassing materials?" And if this is so, why is such graphically offensive material so readily available at MIT. Can something be done about this?

Mail that actually came to Stephit.

Sam says that he has personal problems w/ people who don't want to look @ these images.

Alpha Sigma

The Vice President's note to the Director of Academic Computing got right to the point:

Last night I learned that Alpha Sigma is running an AppleShare server with a disk mostly full of third party software. I just verified that it is available to the entire campus.

Unless they have campus wide licenses, which I doubt, either deliberately or through not knowing, they represent a serious set of license violations. Several issues:

1. Are we doing anything to tell students in the fraternities and the dormitories about software licenses and the issue of piracy?

2. Should someone write a note to Alpha Sigma?

3. Does the University have any liability in the matter? Are we protected in that Alpha Sigma has a house corporation that would be liable if vendors decided to get nasty?

The University had recently extended its campus network to dormitories and fraternities. Dormitory residents each got a network drop at no cost, but had to supply their own computers and Ethernet boards. Fraternities each got a network connection from the house to the campus at not cost, but had to do their own internal wiring and supply their own computers, tranceivers, and Ethernet boards.

The University purchased site licenses for basic network software, and provided it directly to students. The University developed software for University–specific applications, and distributed it directly as well. Students obtained some additional software by buying it commercially, in some cases through the campus computer store. Students obtained other software by downloading freeware and shareware from network files servers at the University and elsewhere across the campus, the country, and the world.

Greg Jackson, gjackson@mit.edu

Malekh Salimi

What on earth have we done?, Kim wondered. The note prompting Kim's wonderment came from Malekh Salimi, a sophomore:

I deeply resent your invasion of my privacy. How I set up my computer is none of your business. As I understand it, the University respects individual rights. When you directed your staff to examine my computer without my permission, you violated this policy. This is arrogant and tyrannical. I want an apology, and your assurance that Information Systems staff will immediately stop invading my privacy and that of other students.

A quick phone call brought some facts. As the University had turned on subnets in student dormitories, students had connected their computers to the network and left them on. Some students hadn't read their networking manuals. They had unwittingly made their software and personal files accessible to anyone on the global Internet.

As Director of Academic Computing, Kim had worried about this. In response, albeit without a formal policy discussion, network staff had begun scanning the network looking for accessible machines. When staff found accessible machines, they sent the student owners mail saying so, mentioning license restrictions and other problems with accessible machines, and suggesting greater caution. Most students receiving these notices had been very appreciative, and had learned how to secure their machines appropriately.

But some, Kim now knew, had reacted otherwise.

Greg Jackson, gjackson@mit.edu

FROM TECHINFO

Be Responsible! MITnet Rules of Use

Computing Support Services - Training

BE RESPONSIBLE! MITnet RULES of USE

MITnet connects Athena workstations and thousands of other computers at MIT. It also provides access to national and international computer networks. As you explore MITnet and the Internet beyond it, you will discover the many advantages of network connectivity. But connectivity also requires that you understand the responsibilities of being a network user in order to protect the integrity of the system and the integrity of other users.

The following Rules of Use are intended to help you use MIT's computing and network facilities responsibly and safely. Complying with them will help assure that all use of the system is responsible, legal, and respectful of privacy.

If you need help with someone who is willfully violating these rules, send e-mail to <stopit@mit.edu>. For more information, contact Joanne Costello, Manager, Network Support Services, x3-6322 or send email to <joanne@mit.edu>.

1. DON'T VIOLATE THE INTENDED USE OF MITNET.

   The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose. In particular, MITnet may not be used to transmit threatening, obscene, or harassing materials.

2. DON'T LET ANYONE KNOW YOUR PASSWORD(S).

   Your MITnet username identifies you to the whole Internet user community. Anyone who knows your password can use your account. If he or she does anything that affects the system, it will be traced back to your username. If your username or your Athena account is used in an abusive manner, you can be held responsible.

3. DON'T COPY COPYRIGHTED SOFTWARE OR RELATED MATERIAL.
   Many programs, and related materials such as documentation, are owned by individual users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. You must abide by these restrictions, because to do otherwise is a crime.

   Such restrictions may include prohibitions against copying programs or data, the resale of data or programs or the use of them for non-

educational purposes or for financial gain, and public disclosure of information about programs (e.g., source code) without the owner's authorization.

4. DON'T VIOLATE THE PRIVACY OF OTHER USERS.

Federal laws protect the privacy of users of wire and electronic communications. As Section 3.17 of MIT's Policies and Procedures notes, "invasions of privacy can take many forms, often inadvertent or well-intended." You should make sure that your use of MITnet does not violate the privacy of other users, if even unintentionally.

Specifically:

* Don't try to access the files or directories of another user without clear authorization from that user. Typically, this authorization is signaled by the other user's setting file access permissions to allow public or group reading of the files. If you are in doubt, ask.

* Don't try to intercept or otherwise monitor any network communications not explicitly meant for you. These include e-mail and user-to-user dialog, as well as a user's password input.

* Don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves.

* Don't create shared programs that secretly collect information about its users. Software on MITnet is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. This means, for example, that you may not collect information about individual users without their consent.

5. DON'T ABUSE YOUR ELECTRONIC MAIL (E-MAIL) PRIVILEGES; IN PARTICULAR, DO NOT OVERLOAD THE SYSTEM.

Guidelines on the use of e-mail are not based on etiquette alone: the mail system simply does not have the capacity to process a very large number of e-mail messages at once. If you send out an announcement to a huge list of recipients, the mail servers get overloaded, disks fill up, and staff intervention is required. The overall result is a negative impact on the quality of service provided for all users.

The proliferation of electronic chain letters is especially abusive to the mail system and the network. Chain letters waste valuable computing resources, and may be considered harassing. You may lose your MITnet privileges by creating or forwarding chain letters.

6. DON'T USE MITNET TO HARASS ANYONE IN ANY WAY.

"Harassment," according to the Policies and Procedures, "is any verbal or physical conduct, on or off campus, which has the intent or effect of unreasonably interfering with an individual's or group's educational or work performance at MIT or which creates an

intimidating, hostile, or offensive educational or work environment.

"Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation, or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group." With reference to sexual harassment, the definition also includes unwelcome sexual advances and requests for sexual favors which might be perceived as explicitly or implicitly affecting educational or employment decisions concerning an individual.

Sending offensive mail or messages may constitute harassment and is in violation of the intended use of the system. To report incidents of on-line harassment, send e-mail to <stopit@mit.edu>.

FROM MIT WELCOME TO ATHENA

MITnet Rules of Use

MITnet and other computing resources at MIT are shared among community members. The MITnet Rules of Use are intended to help members of the MIT community use MIT's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to community members. Complying with them will help maximize access to these facilities, and assure that all use of them is responsibile, legal, and respectful of privacy.

All network users are expected to follow these rules. ***Violations of the rules can subject the offender to Institute disciplinary proceedings and, in some cases, to state or federal prosecution.***

Additional rules may be in effect for users of other computer facilities that have access to MITnet (check with your local system manager for details). Furthermore, several external networks to which MITnet provides access -- e.g., NEARnet, NSFnet, and CREN (including BITNET and CSNET) -- have their own rules of use to which MITnet users may be subject.

If you have questions or wish further information about any of these network policies, send e-mail to net-policy@mit.edu.

Complying with the Intended Use of the System

It is important that you understand the purpose of MITnet so that your use of the system is in compliance with that purpose.

1. Don't violate the intended use of MITnet.

The purpose of MITnet is to support research, education, and MIT administrative activities, by providing access to computing resources and the opportunity for collaborative work. All use of the MIT network must be consistent with this purpose. For example:

- Don't try to interfere with or alter the integrity of the system at large, by doing any of the following:

* permitting another individual to use your account

* impersonating other individuals in communication (particularly via forged email or Zephyrgrams)

* attempting to capture or crack passwords or encryption

* destroying or altering data or programs belonging to other users

- Don't try to restrict or deny access to the system by legitimate users.
- Don't use MITnet for private financial gain.
- Don't transmit threatening or harassing materials.

Assuring Ethical Use of the System

Along with the many opportunities that Athena provides for members of the MIT community to share information comes the responsibility to use the system in accordance with MIT standards of honesty and personal conduct. Those standards, outlined in Section 4.23 of MIT's **Policies and Procedures**, call for all members of the community to act in a responsible, professional way.

Appropriate use of MITnet resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, particularly copyright and harassment laws.

2. Don't let anyone know your password(s).

While you should feel free to let others know your username (this is the name by which you are known to the whole Internet user community), you should never ever let anyone know your account passwords. This includes even trusted friends, and computer system administrators (e.g., Information Systems staff).

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the system will be traced back to your username -- if your username or account is used in an abusive or otherwise inappropriate manner, you can be held responsible.

In fact, there is never any reason to tell anyone your password: every MIT student, faculty member, or on-campus staff person who wants an account of his or her own can have one (see **Athena Account Policies**). And if your goal is permitting other users to read or write some of your files, there are always ways of doing this without giving away your password.

For information about how to manage the security of your account, including advice on how to choose a good password, how to change passwords, and how to share information on Athena without giving away your password, see the document **Managing Your Athena Account**.

3. Don't violate the privacy of other users.

The Electronic Communications Privacy Act (18 USC 2510 *et seq.* , as amended) and other federal laws protect the privacy of users of wire and electronic communications.

The facilities of MITnet, and the operating systems used by Athena and other MITnet systems, encourage sharing of information. Security mechanisms for protecting information from unintended access, from within the system or from the outside, are minimal. These mechanisms, by themselves, are not sufficient for a large community in which protection of individual privacy is as important as sharing (see, for example, sections 3.18/9 and 4.24 of MIT's **Policies and Procedures**). Users must therefore supplement the system's security mechanisms by using the system in a manner that preserves the privacy of themselves and others.

As Section 3.17 of MIT's **Policies and Procedures** notes, "invasions of privacy can take many forms, often inadvertent or well-intended." All users of MITnet should make sure that their actions don't violate the privacy of other users, if even unintentionally.

Some specific areas to watch for include the following:

- Don't try to access the files or directories of another user without clear authorization from that user. Typically, this authorization is signaled by the other user's setting file access permissions to allow public or group reading of the files. If you are in doubt, ask the user.

- Don't try to intercept or otherwise monitor any network communications not explicitly intended for you. These include logins, e-mail, user-to-user dialog, and any other network traffic not explicitly intended for you.

- Unless you understand how to protect private information on a computer system, don't use the system to store personal information about individuals which they would not normally disseminate freely about themselves.

- Don't create any shared programs that secretly collect information about their users. Software on MITnet is subject to the same guidelines for protecting privacy as any other information-gathering project at the Institute. (This means, for example, that you may not collect information about individual users without their consent.)

- Don't remotely log into (or otherwise use) any workstation or computer not designated explicitly for public logins over the network -- even if the configuration of the computer permits remote access -- unless you have explicit permission from the owner and the current user of that computer to log into that machine.

4. Don't copy or misuse copyrighted software or related material.

Many programs, and related materials such as documentation, are owned by individual users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements.

Such restrictions may include (but are not necessarily limited to) prohibitions against:

- copying programs or data
- reselling programs or data
- using programs or data for non-educational purposes
- using programs or data for financial gain
- using programs or data without being among the individuals or groups licensed to do so
- publicly disclosing information about programs (e.g., source code) without the owner's authorization

You must abide by these legal and contractual restrictions, because to do otherwise may subject you to civil or criminal prosecution.

For more information about the legal issues surrounding duplication of software, see the pamphlet "Is it okay to copy my colleague's software?" To request a copy, send e-mail to sendpubs@mit.edu or call x3-5150.

(For guidelines on how to determine what licensing restrictions apply to specific software on Athena, see the document **Summary of Available Athena Software**. For other licensing questions, send email to swa@mit.edu, or call x3-3700.)

5. Don't use MITnet to harass anyone in any way.

"Harassment," according to MIT's **Policies and Procedures** (Section 3.16), is defined as:

any conduct, verbal or physical, on or off campus, which has the intent or effect of unreasonably interfering with an individual's or group's educational or work performance at MIT or which creates an intimidating, hostile or offensive educational, work or living environment.... Harassment on the basis of race, color, gender, disability, religion, national origin, sexual orientation or age includes harassment of an individual in terms of a stereotyped group characteristic, or because of that person's identification with a particular group.

The Institute's harassment policy extends to the networked world. For example, sending email or other electronic messages which unreasonably interfere with anyone's education or work at MIT may constitute harassment and is in violation of the intended use of the system.

Any member of the MIT community who feels harassed is encouraged to seek assistance and resolution of the complaint. To report incidents of on- line harassment, send email to stopit@mit.edu. (If you believe you are in danger, call the Campus Police *immediately* at x3-1212.)

Assuring Proper Use of the System

MITnet's resources, as well as the resources MITnet gives you access to (e.g., Athena, postal servers, bulletin boards, etc.), are powerful tools that can be easily misused. Your use of the system should be consistent with the intended uses of these resources. In particular, you should not overload the system or otherwise abuse the network.

6. Don't overload the communication servers; in particular, don't abuse your electronic mail (email) or Zephyr privileges.

Electronic mail is a fast, convenient form of communication. It is easy to send electronic mail to multiple recipients, and you can even send a message to many recipients simply by specifying a single list name (i.e., by using a mailing list). However, this ability to send messages to many people makes it easy to misuse the system. The general rule is: *use email to communicate with other specific users, not to broadcast announcements to the user community at large*.

For example, while it is appropriate to use email to have an interactive discussion with a set of people (even 20 or more users) or to use email to send a single copy of an announcement to some "bulletin board" facility with a wide readership (e.g., Network News, or a Discuss meeting), it is *not* appropriate to use email as a way to broadcast information directly to a very large number of people (e.g., an entire MIT class). This is true whether you include the recipient usernames individually or by using a mailing list: under no circumstance should you use the email system to get a general announcement out to some large subset of the MIT community.

These guidelines are not based on etiquette alone: the mail system simply does not have the capacity to process a very large number of email messages at once. When a user sends out an announcement to a huge list of recipients, the mail servers get overloaded, disks fill up, and staff intervention is required. The overall result is a negative impact on the quality of service provided for all users.

These considerations apply to the Zephyr service as well. Zephyr is a central service involving thousands of transactions daily. Using Zephyr to transmit messages to a very large group of people degrades the system performance and is inappropriate.

Finally, the proliferation of electronic chain letters is especially abusive of the mail system and the network. Chain letters waste valuable computing resources, and may be considered harassing. Creating or forwarding chain letters may subject you to Institute disciplinary proceedings.

Steph: we never wanted to arbitrate ourselves.

2 basic tenants - 1. Thought that what students didn't think that what they were doing would be considered harassment.
2. Wanted one place of authority.

So they:

1. Created an awareness poster, w/ 3-line description of what is harassment.
2. created a "stop it" mailing list. Goes to sysadmin of academic computing and to Joanne.

She created a ~~[redacted]~~ FAQ - w/ 4 letters - using your account.

The mail begins with the phrase "Someone using your athena account..."

Then we say that our accounts are for our use only, and that they can have the password changed.

Sam says that they are assuming that if someone was offended, then we must be legit. reason for offense.

We get a lot of mail of people using multiple workstations, tying up a workstation for 8-10 hours, &c.

Instead

Most of the time students change their password, I get apologetic mail that somebody was using my account, + the behavior stopps. (Students have a chance to save face.) We don't have repeat offenders. Never.

Amy: Have you ever had somebody ask you, "why gave you wasting space in ~~[redacted]~~ this class?"
I had a group of horney ~~flat~~ frat boys follow me home from a reg-day movie, trying to get me to re-create some of the sexually explicit scenes. That is one of the reasons that ~~[redacted]~~ pornographic movies are no longer shown for registration days.