

Acceptable Use Policy

1. Purpose	1
2. Audience	2
3. Privacy Expectations	2
4. Responsibilities	3
5. Requirements.....	4
6. Disciplinary Actions	7
7. Authoritative Source	9
8. Revision History	9
9. Approvals	12

1. Purpose

The UT Austin Acceptable Use Policy serves as a supplement to the UT Austin [Information Resources Use and Security Policy](#). University [information resources](#) consist of the computer devices, data, applications, and the supporting networking infrastructure. These technologies are critical to the multifaceted mission of the university, a mission that includes teaching, research, and public service. Information technology offers increased opportunities for communication and collaboration and has changed the way we conduct business as a university:

- All students, faculty, and staff use e-mail services
- All members of the university can obtain wireless connectivity
- Every campus dormitory room has a connection to the Internet
- Students submit assignments via the Internet

These are but a few of the many examples of how information resources are connected to many activities at the university. While these resources help the university function, they also require responsible use from every user. Your actions on the UT Austin campus can affect people all around the world. You must use these technologies responsibly and with respect.

This policy establishes guidelines for acceptable use of information resources. It includes examples of what you can do and cannot do, and what rights you have. All of these guidelines are based on the following underlying principles:

- Information resources are provided to support the essential mission of UT Austin.

Acceptable Use Policy

Document Version: Approved

- UT Austin policies, UT System regulations, state and federal law govern your use of information resources.
- You are expected to use information resources with courtesy, respect, and integrity.
- The information resources infrastructure is provided for the entire campus. This infrastructure is finite and requires millions of dollars to maintain, and all users are expected to use it responsibly.
- Simply because an action is easy to do technically does not mean it is legal or even appropriate.

All guidelines in this document are based on these important principles. In many cases, they are similar to guidelines governing other forms of communication at the university.

Technical terms referred to in this document are defined in the [ISO Technical and Security Glossary](#).

Last Reviewed: September 9, 2007

Last Edited: September 9, 2007

See the [change log](#) for a list of significant changes made to this document.

2. Audience

The UT Austin Acceptable Use Policy provides guidance for all individuals that have, or may require, access to the UT Austin information resources, including but not limited to all faculty, staff, students, contractors, visitors, and vendors using university information resources.

3. Privacy Expectations

As a user of information resources at the university, there are certain things you can expect.

3.1. Are my e-mails private?

In general, electronic communications transmitted across a network should never be considered private or confidential. When you are considering the safety and security of a communication, it is best to think of e-mail and instant messages like postcards—viewable by anyone with access.

3.2. Are my files private?

The university respects the contents of your files and monitors the university network in accordance with the UT Austin [Network Monitoring Standards](#). Additionally, Information Technology (IT) administrators may become aware of file content while dealing with specific operational problems. Usage logs are frequently kept to diagnose such problems. Furthermore, the university will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance has included providing, when required, copies of system files, e-mail content, or other information ordered by the court.

The university does not monitor personal Web pages for the purpose of determining content. However, when credible evidence of illegal or otherwise impermissible activity is reported, appropriate action will be taken.

The university does not review electronic communication for the purpose of determining whether impermissible activity is occurring. However, in the course of assuring the viability of the university's network, IT administrators may become aware of activity that poses a risk to the network's proper operation. In such cases, IT administrators may need to disable or block access to the services or systems involved if they are deemed to pose a risk to the network's optimal performance. Also, during the process of diagnosing potential problems involving the proper function of the network, any information obtained that indicates possible unauthorized distribution of copyrighted materials may be referred to the UT [Information Security Office](#) for further investigation.

3.3. What are my First Amendment rights?

As an academic institution, we place great value on freedom of thought and expression. With a population of over 71,000, the university community encompasses a wide array of opinions, views, approaches, and temperaments. Ideally, we would like all those associated with the university to exercise their freedoms in a mature, responsible, and respectful manner, and we encourage them to do so. We do not punish or prevent expression that may be offensive but that violates no specific law or university regulation.

4. Responsibilities

Just as everyone in the university community is expected to use physical resources at UT Austin responsibly, we are all expected to help protect information resources at UT Austin. Protecting information resources is not the sole responsibility of IT administrators, any more than taking care of books is singularly the responsibility of librarians.

4.1. Protecting IT Resources from Physical Access

You are responsible for the use of the university information resources you have been provided.

You must control unauthorized use of your university information resources by preventing others from obtaining access to your computer, or to the access port assigned for your exclusive use.

4.2. Protecting IT Resources from Electronic Access

Likewise, you are responsible for protecting your information resources from unauthorized electronic access by using effective passwords (or other access controls) and by safeguarding those passwords.

Although you may believe that the data you store on a UT Austin computer system need no protection from access, remember that an insecure account may provide an access point for the entire computer system. Persons attempting to gain unauthorized access to a system do so through user accounts, and your password may be the only safeguard against such access.

4.3. Using Electronic Communications Responsibly

All members of the university community are encouraged to use electronic communications for university-related activities and to facilitate the efficient exchange of useful information. However, access to the university's electronic communications services is a privilege, and certain

Acceptable Use Policy

Document Version: Approved

responsibilities accompany that privilege. People who use university communication services (such as e-mail) are expected to use them in an ethical and responsible manner, following general guidelines based on common sense, common decency, and civility applied to the networked computing environment.

Electronic communications should meet the same standards for distribution or display as if they were tangible documents or instruments. Identify yourself clearly and accurately in all electronic communications. Concealing or misrepresenting your name or affiliation to dissociate yourself from responsibility for your actions is never excusable.

All stored electronic correspondence belongs to somebody. It should be assumed to be private and confidential unless the owner has explicitly made it available to others.

Civil discourse is at the heart of a university community free of intimidation and harassment. It is based upon a respect for individuals as well as a desire to learn from others. While debate on controversial issues is inevitable and essential, bear in mind that it is your responsibility to do so in a way that advances the cause of learning and mutual understanding.

4.4. Using Limited Resources Responsibly, Efficiently, and Fairly

You are expected to promote efficient use of network resources, consistent with the instructional, research, public service, and administrative goals of the university. Show consideration for others and refrain from engaging in any use that would interfere with their work or disrupt the intended use of network resources.

It is not responsible to use disproportionate amounts of information resources. Examples of disproportionate uses generally include activities such as the misuse of peer-to-peer (P2P) applications, streaming media at high bit rates, or serving a multi-user game.

4.5. Complying with the Terms of the User Agreement

As a member of the university, you are expected to read, understand, and comply with the terms of the agreement you acknowledge annually online. If you have questions, ask for clarification from your local IT support contact or from the Information Security Office.

4.6. Complying with University Rules and Federal Laws

As a member of the university, you are expected to comply with all applicable university regulations and federal and state laws. The University of Texas at Austin reserves the right to terminate computing services of users who repeatedly violate university rules or infringe upon the rights of copyright holders. If you have questions about whether you may be infringing on another's copyright, please review [Crash Course in Copyright](#) from UT System.

5. Requirements

1. You are the only person who can use an information resource (such as an electronic identifier or an electronic mail account) that the university has provided for your exclusive use.

2. **NEVER GIVE YOUR PASSWORD TO ANYONE ELSE**, even people you trust, such as your friends or relatives or someone who has offered to help you fix a problem. If you suspect someone may have discovered or guessed your password, [change it immediately](#).
 - i. You are responsible for all charges accrued using the computing account or computing resources assigned to you, even if a friend using your account without your permission runs up the charges.
 - ii. You will also be held responsible for destructive or illegal activity done by someone to whom you gave access—even if the computing resource doesn't require a password, such as access to your dormitory Ethernet port.
3. Do not give others access to university information resources unless they are authorized and authenticated to do so. You may not extend access to university information resources to others without permission (e.g., proxy services, accounts for non-university personnel, etc).
4. You may not be paid, or otherwise profit, from the use of any university-provided information resource or from any output produced using it. You may not promote any commercial activity using university information resources. Examples include, attempting to sell football tickets or used text books via the UT course management service or advertising a "Make Money Fast" scheme via a newsgroup. Such promotions are considered unsolicited commercial spam and may be illegal as well.
5. Never use any university-provided information resource to do something illegal, threatening, or deliberately destructive—not even as a joke. The Information Security Office will investigate all complaints. The Office of the Dean of Students handles complaints about students; the Office of the Executive Vice President and Provost handles complaints about UT Austin faculty and staff. Violations can result in disciplinary action, criminal charges, or both. Law enforcement agencies will investigate violations of state or federal law.
 - i. Ignorance is no excuse. Read the [Computer Crimes Law](#).
 - ii. Never deliberately install any unauthorized or malicious software on any system.
 - iii. You cannot be exempt from the law because you are "just a student," "you were conducting research," or you were "just playing around."
 - iv. If you are a student with a part-time job at the university, you may be disciplined both as an employee and as a student, resulting in both professional and educational consequences.
6. Be civil. Do not send rude or harassing correspondence.
 - i. If someone asks you to stop communicating with him or her, you should. If you fail to do so, the person can file a complaint and you can be disciplined.
 - ii. If you ever feel that you are being harassed, university staff members will assist you in filing a complaint. Please report the problem to Student Judicial Services at 471-2841, or contact the Information Security Office at security@utexas.edu. If you are concerned for your safety or feel that you are in danger, call the UT police department at 471-4441, or call the Austin police if you are off-campus.
7. Use resources appropriately. Do not interfere with the activities of others or use a disproportionate share of information resources. Examples of inappropriate use of resources are shown below. These actions frequently result in complaints and subsequent disciplinary action.

Acceptable Use Policy

Document Version: Approved

- i. Sending an unsolicited message(s) to a large number of recipients (known as "spamming the network").
 - ii. Consuming an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications).
 - iii. Deliberately causing any denial of service, including flooding, ICMP attacks, or the unauthorized automated use of a service intended solely for human interaction.
8. Never falsify your identity or enable others to falsify identity using university information resources. This type of forgery can result in serious criminal penalties and disciplinary action by the Office of the Dean of Students or the Office of the Executive Vice President and Provost.
 - i. All electronic correspondence must correctly identify the sender.
 - ii. All electronic correspondence belongs to someone and should be treated as private communications unless the author has explicitly made them available to others.
9. Never infringe upon someone else's copyright. It is a violation of university policy and federal law to participate in copyright infringement. **The university complies with all legal requests (e.g., subpoenas) for information and will not hesitate to report your use in response to a lawful request.** Copyrighted materials include, but are not limited to, computer software, audio and video recordings, photographs, electronic books, and written material. If you share movies or music that you did not create, you may be infringing on another's copyright. Consequences of copyright infringement can include disciplinary actions by the university. In addition, copyright owners or their representatives may sue persons who infringe on another's copyright in federal courts. Such lawsuits average \$750 per allegedly violated song in penalties or fines, for example. See the [Keep it Legal: Finding Legal Online Music, Movies, and Other Content](#) and the [Fair Use of Copyrighted Materials](#) for more information.
10. Never try to circumvent login procedures on any computer system or otherwise attempt to gain access where you are not allowed. Never deliberately scan or probe any information resource without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences, including disciplinary action by the Office of the Dean of Students or the Office of the Executive Vice President and Provost.
11. Never use or disclose [Category-I](#) data, or data that is otherwise confidential or restricted, without appropriate authorization. Examples of groups that can provide appropriate authorization include, but are not limited to [Office of Admissions](#), [Human Resource Services](#), [Office of the VP for Institutional Relations and Legal Affairs](#), [Information Security Office](#), and the university's [Public Information Officer](#).
 - i. Make sure any individual with whom you share Category-I data is authorized to receive the information.
 - ii. Do not share Category-I data with friends or family members.
 - iii. Do not share university business data that may be classified as Category-I data, such as the status of negotiations, terms of contracts, and new research or products or relationships under development.
 - iv. Comply with the university's agreements to protect vendor information such as software code, proprietary methodologies, and contract pricing.

- v. If your office routinely receives requests for Category-I data, work with an appropriate group within the university to develop formal processes for documenting, reviewing, and responding to these requests.
- vi. If you receive a non-routine request for Category-I data from a third party outside of the university, check with an appropriate group within the university to make sure the release of the data is permitted.
- vii. Report violations of university policies regarding use and/or disclosure of confidential or restricted information to the Information Security Office (security@utexas.edu, 512-475-9242).

6. Disciplinary Actions

6.1. What are the consequences for violating the rules listed in Section V of this document?

Punishment for infractions includes, but is not limited to:

- Verbal warnings
- Revocation of access privileges
- Disciplinary probation
- Suspension from the university
- Criminal prosecution

If your activity breaks the law, you can be prosecuted. Even if you are not charged criminally, you can still be suspended from the university. Such suspensions happen to several people each semester.

The university reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

If you are unsure whether an action you are considering is an acceptable use of electronic resources, write to the Information Security Office at security@utexas.edu, or contact Student Judicial Services before you act. Representatives from either department will be glad to work with you to prevent problems later on.

6.2. What is NOT against law or policy?

Some things you might think violate UT Austin policies may not be. Before you report what you believe is an incident of misuse, please read this section carefully. It is written primarily for those planning to report what they believe to be an infraction of law or policy.

6.2.1. First Amendment Rights

Acceptable Use Policy

Document Version: Approved

In general, expressions of opinion by members of the university community that do not otherwise violate state and federal laws or university rules are protected as “free speech.” This is true even though the opinions expressed may be unpopular or offensive to some. With a population of 71,000, UT Austin encompasses a wide array of opinions and views. We encourage all those associated with the university to exercise their constitutional rights and freedoms responsibly. We do not, however, punish people who express views that may be unpopular or offensive, but who break no laws or university rules while doing so.

6.2.2. "Spam," unsolicited and unwanted e-mail, and other junk mail from a source outside UT Austin

Many people are annoyed by junk mail such as "spam" and other kinds unsolicited or unwanted e-mail. If the offending e-mail is against UT Austin rules, the Information Security Office investigates the report and takes appropriate action.

It is not unusual, though, for junk mail to originate from a source outside the university. In most such cases, the university has little control. You, however, as the recipient have a great deal of control.

You can ignore or delete the junk mail. [Read Don't Get Hooked: Protect Yourself Against Phishing Scams](#) for more tips on dealing with unsolicited mail.

You can write the administrator of the Internet service provider from which the e-mail was sent, as described later in this section. Responsibly administered mailing lists will remove your name from their subscriber list if you ask them to do so. Not all lists, however, will honor your request.

ITS uses robust hardware and software to control spam on all e-mail services provided centrally by ITS. Specific questions about spam can be addressed to the [ITS Help Desk](#).

Repeated incidents involving offensive e-mail may become harassment. If you feel this is occurring, write security@utexas.edu. If you feel threatened, call UT Police, 471-4441.

6.2.3. Breaches of “netiquette”

Disagreements between people, even heated arguments, unless threatening or otherwise unlawful, are not considered violations. UT Austin does, however, strongly encourage all its users to be polite and courteous.

A well-known problem with e-mail, blogs, and social networks is that it's easy to fire off a quick, angry response that you'll later wish you hadn't sent. In doing so, should you cross the line beyond merely being rude or stating an unpopular, offensive view, you may run the risk of violating criminal laws or inviting an action in civil court. “Counting to ten” before saying something you may later regret applies in cyberspace too.

6.2.4. Off-topic postings

Off-topic postings to blogs, social networks, etc., are breaches of network etiquette, but are not against university rules unless the content of the posting itself is a violation. Find out what

is appropriate for each group before you post messages. If someone else posts an off-topic message and you decide to write them about it, be polite. Many such postings are not intentional.

6.3. How do I report an incident?

Note: Before you report an incident involving what you believe to be a misuse of information resources, see Section VI of this document. That section lists activities that do not violate laws or policies.

How you report an incident involving the misuse of IT resources depends upon the nature of the incident:

- If you believe that your personal safety is threatened, call UT Police, 471-4441.
- For others incidents, contact the Information Security Office at security@utexas.edu or the UT Austin compliance hotline (via helpline@compliance.utexas.edu or 1-877-888-0002). You will receive an acknowledgment, and the incident will be handled by staff at the appropriate university office, such as Student Judicial Services or the Office of the Provost.
- For reporting problems with "spam" or unsolicited mail, you may want to notify the Internet service provider (ISP) from which the mail was sent. Send a simple, polite note to the ISP, including a complete, unaltered copy of the spam (including the [e-mail headers](#)) for them to analyze. Don't expect a personal reply, because the ISP will probably be awash in complaints just like yours.

7. Authoritative Source

The authoritative source on this policy and responsibility for its implementation rests with the Office of the Associate Vice President and [Chief Information Officer](#).

8. Revision History

Version	Date	New	Original
	2/24/2011	Created PDF of web version	No change

Acceptable Use Policy

Document Version: Approved

Version	Date	New	Original
	2/23/2009	Updated example in Section V.4 to read, "Examples include, attempting to sell football tickets or used text books via the UT course management service or advertising a "Make Money Fast" scheme via a newsgroup. Such promotions are considered unsolicited commercial spam and may be illegal as well."	For example, you cannot advertise a "Make Money Fast" scheme. Such promotions are called "chain letters" and are explicitly illegal.
	11/10/2007	<p>During the annual review of this document, a number of wording changes were made to align the language with the expectations outlined in the Information Resources Use and Security Policy. In addition, the following changes were made:</p> <ol style="list-style-type: none">1. Policy moved from Information Technology Services site to Vice President for Information Technology site.2. Formatted document to conform to other policy documents. Added section II. Audience.3. From "What can I expect?":<ul style="list-style-type: none">• Changed heading to "III. Privacy Expectations."• Consolidated "What can I do about being harassed?" into section VI. Disciplinary Actions.• Removed "What happens if someone complains about me?"4. Updated Privacy Expectations (Sec III) to make mention of the U. T. Austin Network Monitoring Standards (http://www.utexas.edu/its/policies/opsmanual/monitor.php).5. Updated Requirements (Sec V) to more directly cover copyright violations associated with peer-to-peer misuse (Rule #7, Rule #9)	

Version	Date	New	Original
	4/9/2007	<p>Section II, change requested by Compliance Office and Legal Affairs:</p> <p>"Furthermore, the university will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance has included providing, when required, copies of discussions on university operated mailing list servers, discussion threads on university operated news servers, e-mail content stored on university IT resources, or other information ordered by the court."</p>	<p>"Furthermore, the university will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance has included providing, when required, copies of discussions on university operated mailing list servers, discussion threads on university news servers, or other information ordered by the court."</p>

Acceptable Use Policy

Document Version: Approved

Version	Date	New	Original
	11/17/2006	Removed language about Brightmail and IronPort technologies from section VI, "Spam" #3. Replaced with "ITS uses robust hardware and software to control spam on all e-mail services provided by ITS. Specific questions about spam can be addressed to the ITS Help Desk."	"ITS uses a combination of Ironport appliances and Brightmail software to control spam on all e-mail services provided by ITS. Specific questions about spam can be addressed to the ITS Help Desk."

9. Approvals

Name	Role	Members	Date
Chief Information Security Officer	Approval	Cam Beasley	March 3, 2011