MENU

Acceptable Use Policy for University Students

Table of Contents

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.

While these resources help the university function, they also require responsible use from every user. Your actions can affect people all around the world. You must use these technologies responsibly and with respect.

This policy establishes guidelines and best practices 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.
- UT Austin policies, UT System rules, state and federal law govern your use of information resources.
- 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.

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.

Definitions:

- University: The University of Texas at Austin.
- System: The University of Texas System.
- University Information Resources: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf.
- University Data: All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records.
- Confidential Data or Confidential Information: All University Data that is required to be maintained as private or confidential by applicable law.
- User: Any individual granted access to University Information Resources.

2. Audience

All university students granted access to or use of university Information Resources must be aware of and agree to abide by the following acceptable use requirements:

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.

E-mails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements.

Users who are University employees are to use University provided e-mail accounts, rather than personal e-mail accounts, for conducting University business.

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.

University Information Resources are provided to users for the purpose of conducting the business of University and/or System. However, users are permitted to use University Information Resources for use that is incidental to the their official duties to the University as permitted by this policy. Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University have no expectation of privacy regarding any University Data they create, send, receive, or store on University owned computers, servers, or other information resources owned by, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission without notice. Users who are faculty and staff have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device.

3.3. What rules govern speech made using University information resources?

The University's policy on Speech, Expression, and Assembly is set forth in Chapter 13 of the University's Institutional Rules, including the University's regulations on prohibited expression. Chapter 13 applies to all

speech on campus, including speech made using University information resources. Although this IT policy describes additional best practices concerning certain speech and expressive activities, such practices are aspirational. Chapter 13 determines what will constitute a violation of University standards for speech, expression, and assembly and when such violations will subject a student to discipline.

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 & Electronic 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.

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.

4.2. 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 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 ethics and responsibility 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.

4.3. 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.

4.4. Complying with the Terms of the Acceptable Use Policy

As a member of the University, you are expected to read, understand, and comply with the terms of the Acceptable Use Policy. If you have questions, ask for clarification from your local IT support contact or from the Information Security Office.

4.5. 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

5.1 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.

5.2 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.

1. University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Identification Cards, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.

2. Users must not give others access to University Information Resources unless they are authorized and authenticated for such access. Users may not extend access to University information resources to others without permission (e.g., proxy services, accounts for non-university personnel, etc).

3. Each User will be held responsible for all activities conducted using the User's password or other credentials.

5.3 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).

5.4 Incidental Use of University Information Resources is permitted, but must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy.

1. Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University e-mail accounts.

2. A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located.

3. Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited.

4. Users may not be paid, or otherwise profit, from the use of any university-provided information resource or from any output produced using it. Users 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. Incidental Use for purposes of political lobbying or campaigning is prohibited.

6. Storage of any e-mail messages, voice messages, files, or documents created as Incidental Use by a User must be nominal.

5.5 Never use any university-provided information resource to do something illegal 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.

1. Ignorance is no excuse. Read the Computer Crimes Law.
2. Never deliberately install any unauthorized or malicious software on any system.
3. You cannot be exempt from the law because you are "just a student," "you were conducting research," or you were "just playing around."
4. 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.

5.6 Chapter 13 of the University's *Institutional Rules* applies to communication using university-provided IT resources..

1. If someone asks you to stop communicating with them, you should. If you fail to do so, the person can file a complaint and you can be disciplined.
2. If you believe that communication you receive violates the University's *Institutional Rules*, and you wish to make a complaint, you may request a University staff member 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.

5.7 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.

1. Sending an unsolicited message(s) to a large number of recipients (known as "spamming the network").
2. Consuming an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications).

3. Deliberately causing any denial of service, including flooding, ICMP attacks, or the unauthorized automated use of a service intended solely for human interaction.

5.8 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.

1. All electronic correspondence must correctly identify the sender.
2. All electronic correspondence belongs to someone and should be treated as private communications unless the author has explicitly made them available to others.
3. The following email activities are prohibited when using a University provided email account:
    A. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work related purpose.
    B. Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of University.
    C. Sending or forwarding any email that is suspected by the User to contain computer viruses.
    D. Any Incidental Use prohibited by this policy.
    E. Any use prohibited by applicable University or System policy.

5.9 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 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.

5.10 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.

5.11 Additional Requirements for Portable and Remote Computing.

1. All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including e-mail, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.
2. University Data created or stored on a User's personal computers, smart phones or other devices, or in databases that are not part of University's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources.
3. University issued mobile computing devices must be encrypted.
4. Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted.
5. University Data created and/or stored on personal computers, other devices and/or non-University databases should be transferred to University Information Resources as soon as feasible.
6. Unattended portable computers, smart phones and other computing devices must be physically secured.
7. All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.

5.12 Never use or disclose Confidential 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.

1. Make sure any individual with whom you share Confidential data is authorized to receive the information.
2. Do not share Confidential data with friends or family members.
3. Do not share University business data that may be classified as Confidential data, such as the status of negotiations, terms of contracts, and new research or products or relationships under development.
4. Comply with the University's agreements to protect vendor information such as software code, proprietary methodologies, and contract pricing.
5. If your office routinely receives requests for Confidential data, work with an appropriate group within the University to develop formal processes for documenting, reviewing, and responding to these requests.
6. If you receive a non-routine request for Confidential 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.
7. Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on centrally managed services, rather than local hard drives or portable devices.
8. Confidential or essential University Data stored on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, must be encrypted in accordance with University, System's, and any other applicable requirements.

9. All Confidential University Data must be encrypted during transmission over a network.
10. Users who store University Data using commercial cloud services must use services provided or sanctioned by the University, rather than personally obtained cloud services.
11. Users must not try to circumvent login procedures on any University Information Resource or otherwise attempt to gain access where they are not allowed. Users may not deliberately scan or probe any University Information Resource without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences.
12. All computers connecting to a University's network must run security software prescribed by the Information Security Officer as necessary to properly secure University Information Resources.
13. Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.
14. 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?

Consequences for infractions include, but are not limited to:

Verbal warnings
Disciplinary action under Chapter 11 of the Institutional Rules, as set out in Section 13—1202 of those rules
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. "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 of 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.

6.3. How do I report an incident?

Note: Before you report an incident involving what you believe to be a misuse of information resources, review Section VII of this document. This section lists commonly complained-of activities that do not violate laws or rules.

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 1-877-507-7321). 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. Alternatively, you may also use the following form to report matters to University Compliance Services (https://www.reportlineweb.com/utaustin).
- 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
	8/28/2019	Aligned with Insitutional Rules on Student Services and Activities	
	8/24/2015	Aligned with AUP changes to IRUSP	
	06/24/2013	Reviewed and fixed broken links.	
	5/28/2013	Converted back to HTML	No change
	2/24/2011	Created PDF of web version	No change
	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	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: 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?": • Changed heading to "III. Privacy Expectations." • Consolidated "What can I do about being harassed?" into section VI. Disciplinary Actions.	

Version	Date	New	Original
		• 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://security.utexas.edu/policies/monitoring.html). 5. Updated Requirements (**Sec V**) to more directly cover copyright violations associated with peer-to-peer misuse (**Rule #7, Rule #9**)	
	4/9/2007	Section II, change requested by Compliance Office and Legal Affairs: "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."	"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."
	4/9/2007	Removed language about Brightmail and IronPort technologies from section VI, "Spam" #3. Replaced with "ITS uses robust hardware and software to control spam	"ITS uses a combination of Ironport

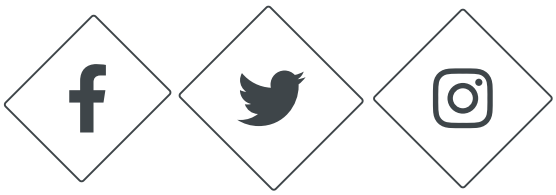
Version	Date	New	Original
		on all e-mail services provided by ITS. Specific questions about spam can be addressed to the ITS Help Desk."	appliances and Brightmail software to control spam on all e-mail services provided by ITS. Specific questions about spam can be addressed to the ITS Help Desk."

Revision History

10. Approvals

Name	Role	Members	Date
Chief Information Security Officer	Approval	Cam Beasley	September 24, 2015

Approvals



Information Security Office

Privacy Policy | Accessibility Policy

TEXAS