

The University of Texas At Tyler
STUDENT INFORMATION TECHNOLOGY RESOURCES
ACCEPTABLE USE POLICY

The University of Texas at Tyler relies heavily on networked computers and the data contained within those systems to achieve its missions. This Acceptable Use Policy is to protect these resources in accordance with state law and Regents Rules. Information Technology resources include all computer and telecommunications hardware, software, and networks owned, leased, or operated by The University of Texas System and the information stored therein. All individuals granted access to U. T. Tyler Information Technology resources must follow the acceptable use rules below:

General	<ul style="list-style-type: none"> U. T. Tyler Information Technology resources are provided for the express purpose of achieving the University's mission to provide a setting for free inquiry; encourage excellence in teaching and learning; stimulate productive scholarship and research and promote community and public service by its faculty, staff and students. Exercise of First Amendment rights is encouraged and incidental use of Information Technology resources is permitted unless it violates state and federal laws or university rules. (BPM 53-02-96) U. T. Tyler Information Technology resources must not be used to: engage in acts against the mission and purposes of U. T. Tyler, intimidate or harass, degrade performance, deprive access to a U. T. Tyler resource, obtain extra resources beyond those allocated, or to circumvent U. T. Tyler computer security measures. Information Technology resources must not be used to conduct a personal business or used for the exclusive benefit of individuals or organizations that are not part of the University of Texas System. Any exceptions must be in support of System missions and require the prior written approval of an executive officer. Pornographic materials must not be intentionally accessed, created, stored or transmitted on U. T. Tyler Information Technology resources other than in the course of academic research where this aspect of the research has the explicit written approval of an executive officer. Students must not copy or reproduce any copyrighted or licensed software or files, except as expressly permitted by the software license, must not use unauthorized copies on University-owned computers or must not use software known to cause problems on UT Tyler computers. (COPYRIGHT LAW)
Data Protection	<ul style="list-style-type: none"> Data will be accessed on a need to know basis. Users of Information Technology resources must not attempt to access data or programs contained on systems for which they do not have authorization or explicit consent.
Virus Protection & Security Patches	<ul style="list-style-type: none"> All computers, both University owned and privately owned, connecting to the U. T. Tyler network must run current virus prevention software. This software must not be disabled or bypassed with the exception of installation of software, or other special circumstance or procedure that requires the temporary disabling of virus prevention software. Computers found to be infected with a virus or other malicious code will be disconnected from the U. T. Tyler network until deemed safe by the Office of Information Technology and Communications (OISC). (UT Tyler Network Policy) All computers, both University owned and privately owned, connecting to the U. T. Tyler network must be current on operating system and application critical updates and security patches. Computers found to be deficient in security patches will be disconnected from the U. T. Tyler network until deemed safe by the Office of Information Systems and Communications (OISC). (UT Tyler Network Policy)
Student Email	<ul style="list-style-type: none"> The following email activities are prohibited by policy: <ul style="list-style-type: none"> Using email for purposes of political lobbying or campaigning except as permitted by the Regents' Rules and Regulations. Posing as anyone other than oneself when sending email, except when authorized to do so by the owner of the email account. Reading another User's email unless authorized to do so by the owner of the email account, or as authorized by policy for investigation, or as necessary to maintain services- Sending or forwarding chain letters. (UT Tyler Email Policy) Sending unsolicited messages (SPAM) to large groups Sending excessively large messages or attachments unless in performance of official U. T. Tyler business. Sending threatening or harassing email. Sending or forwarding email that is likely to contain computer viruses.
Internet Use	<ul style="list-style-type: none"> Due to network maintenance and performance monitoring and to ensure compliance with applicable laws and policies, all user activity may be subject to logging and review. Personal commercial advertising must not be posted on U. T. Tyler web sites.
Network Device Connection	<ul style="list-style-type: none"> All devices which are connected to the U. T. Tyler local area network (LAN), either via a hard-wire cable connection or a wireless connection, must be reported to the Office of Information Systems and Communications (OISC) for approval. (UT Tyler Network Policy) Routers, switches, wireless access points, and other network devices in student housing must be reported to the Office of Information Systems and Communications (OISC) for approval. (UT Tyler Network Policy) Exception: Computers and printers connected in student housing DO NOT need to be reported, but must have current virus protection and be up to date on operating system patches. For more information on devices connecting to the U. T. Tyler network, please view the U. T. Tyler Network Connection Policy at http://www.uttyler.edu/inforesources/uttnetworkpolicy.pdf (UT Tyler Network Policy)
Portable and Remote Computing	<ul style="list-style-type: none"> It is recommended that all computers and portable-computing devices using U. T. Tyler Information Technology be password protected using "strong" password standards and be changed at least annually or if there is suspicion that the password has been compromised. It is recommended that unattended portable computing devices be physically secure. If it is determined that required security related software is not installed on a remote computer or that a remote computer has a virus, is party to a cyber attack or in some way endangers the security of the U. T. Tyler network, the network connection will be disabled. Access will be re-established once the computer or device is determined to be safe by OISC.
Security	<ul style="list-style-type: none"> Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems should not be downloaded and/or used, except as authorized by the OISC. For example, password cracking programs, packet sniffers, or port scanners on U. T. Tyler Information Technology shall not be used (Section 33.02 Texas Penal Code)