Texas Wesleyan University
Information & Communication Technology

Policy for the Acceptable Use of Information Technology Resources

As with nearly all other corporations and educational institutions, the rapid emergence of the Internet, the growth of the World Wide Web, the incorporation of electronic mail in various curricula, and the availability of distributed information resources across a common network has caused Texas Wesleyan University to examine the many issues involved in the responsible use of information technology using institutional resources. This policy is the product of that study, and adherence by all Texas Wesleyan University students and staff is necessary. Adherence to this policy will ensure a computing environment that will perpetuate Texas Wesleyan University's academic and service mission. It is imperative that the campus community accepts that technological resources require responsible behavior from all its users. Simply stated, the continued and efficient accessibility of computer resources is the responsibility of the entire campus community.

> This policy in conjunction with the *Policy for the Acceptable Use of Network Resources* will govern the use of information technology resources at Texas Wesleyan University.

Purpose

Information technology, including systems, software, and data, plays an increasingly important role in education and administration at Texas Wesleyan University. This policy is designed to define the appropriate and responsible use of the campus computing and network facilities by students and employees. Further, it is the intent of this policy to allow the greatest access of campus computing resources consistent with generally accepted principles of ethics that govern the Texas Wesleyan University community. In support of its mission of education and public service, Texas Wesleyan University seeks to provide access to its information technology for students and employees within institutional priorities and financial capabilities.

Scope

Access to Texas Wesleyan University-owned computer facilities, equipment, hardware, software, printing services, and Information Technology Services staff-provided user support is a privilege, not a right. This privilege is extended to all students and employees. Accepting access to this technology carries an associated expectation of responsible and acceptable use. Since technology now serves as a major source of information and interaction for research and education, this policy applies to all students and employees at Texas Wesleyan University who utilize any University information resource.

Definitions

The following terms are defined to add clarity to this policy.

Chief Information Officer. The administrator responsible for the administration and support of the University's information technology resources. The chief information officer reports to the senior vice president of Finance and Administration.

Computer. An electronic device that performs logical, arithmetic, and memory functions by manipulating electronic or magnetic impulses, and that includes all input, output, processing, storage, software, and communication facilities that are connected or related to an electronic system or communication network.

Computer hardware. Any and all tangible or physical devices attached to or used in conjunction with a computer system.

Computer network. The interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more interconnected computers.

Computer program. An ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

Computer resources. Any and all computerized institutional data, computer hardware, and computer software owned by or operated at Texas Wesleyan University.

Computer software. A set of computer programs, procedures, or associated documentation used in the operation of a computer system.

Computer supplies. Paper tape, magnetic tape, tape cartridges, diskettes, floppy diskettes, compact discs, and computer output, including paper and magnetic media.

Computer system. A set of related computer equipment, hardware or software.

Data. A representation of information, knowledge, facts, concepts, or instructions that have been prepared or are being prepared in a formalized manner and have been processed, are being processed, or are intended to be processed in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, compact discs, and as stored in the memory of Texas Wesleyan University computers. Data are property.

Information technology. Any and all computer or electronic resources that are utilized in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data.

Property. Anything of value, including but not limited to financial instruments, information, electronically produced data, computer software, and computer programs.

Responsible use. Any action or behavior of an individual that does not cause accidental or unauthorized destruction, disclosure, misuse, or modification of or access to the information technology or computer resources owned or operated by Texas Wesleyan University.

User. Any person authorized to access and utilize the information technology resources at Texas Wesleyan University.

User account. Any physical area of any Texas Wesleyan University computer system that has been specifically established and set aside for any user.

Compliance

All users of Texas Wesleyan University information technology resources are required to comply with and, by using any such resources, agree to comply and be subject to this *Policy for the Acceptable Use of Information Technology Resources* (hereafter referred to as "policy"). Texas Wesleyan University, through an appropriate review and amendment process, reserves the right to amend this policy at any time, and without prior notice, in order to better provide information technology access to students and employees. Texas Wesleyan University reserves the right to limit, restrict, or extend computing privileges and access to its information technology resources.

Limitations

Texas Wesleyan University computing resources and associated user accounts are only to be used for Texas Wesleyan University activities for which they are assigned, intended, or approved by a University official. Texas Wesleyan University computing systems are not to be used for any non-University related purpose. When accessing any remote resources utilizing Texas Wesleyan University information technology, users are required to comply with both the policies set forth in this document and all applicable policies governing the use and access of the remote computer system.

User Accounts

User accounts are designed only 1) to establish a system control mechanism for user identification, and 2) to afford users a physical location where they can store relevant academic and administrative data. At no time should user accounts be used to execute any computer software or computer programs other than those programs specifically granted and offered for user execution by Texas Wesleyan University. Physical storage in user accounts of any information, data, or programs not congruent with the mission of Texas Wesleyan University or specific functioning of the user's position of employment in support of the stated mission is prohibited.

All users are responsible for both the protection of their user account password and the data stored in their user account. Users are prohibited from sharing their user account password with anyone at anytime; thereby granting unauthorized access to Texas Wesleyan University computer systems. It is required that users change their user account password periodically to help prevent compromise and unauthorized access of their user account. Any suspected unauthorized access of a user account should be reported immediately to the Chief Information Officer or other University authority. User accounts are deactivated and removed from further access and use when the user's affiliation (e.g., employment, matriculation, current enrollment, etc.) is terminated. All data, files, or messages are removed from user accounts when account deactivation occurs.

Ownership

Texas Wesleyan University owns and operates the computers, computer networks, software, data files, messages, connections to external computer networks, and subscriptions to external computer services. Users cannot claim ownership of any data stored in Texas Wesleyan University computer systems.

These information technology resources are provided for the use of Texas Wesleyan employees and students in support of its programs and are to be used for education, research, academic development, administrative functions, and public service. Use of these resources is a privilege, not a right. When using these resources, individuals agree to abide by the applicable policies of the University, as well as federal, state, and local laws.

Privacy

<u>User privacy is not guaranteed.</u> When University information systems are functioning properly, a user can expect the files and data he or she generates and stores in his or her user account to be private information, unless the creator of the file or data takes action to reveal it to others. Users should be aware, however, that no information system is completely secure. Persons both within and outside of the University may find ways to access files. Accordingly, the University cannot and does not guarantee user privacy and users should be continuously aware of this fact.

Texas Wesleyan University firmly supports all users' privacy as long as the user adheres to this policy defining the responsible use of information technology resources. Authorized Information &

Communication Technology Department personnel have the right to examine stored information and communications when investigating cases of abuse of this policy, dealing with mis-addressed e-mail, and when troubleshooting technical problems with the system.

The University will not routinely monitor the content of electronic communications or personal WWW home pages, but will investigate properly identified allegations of misuse and will comply with applicable University regulations and state and federal laws.

The University reserves the right to access and disclose the contents of the electronic communications of its employees and other authorized users, but will do so only when it has a legitimate business need and after authorization from the senior vice president and provost or his/her designee. The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee.

Authorized Information & Communication Technology Department personnel may routinely log usage data for system management purposes. The University does not archive contents of shared system disks or e-mail communications. However, disks on system computers are regularly backed up with "snapshot captures" for the purpose of being able to recover from crashes. These backups are only retained for a brief period. Note that this means that the University does not guarantee the integrity or permanence of material stored on system disks.

Data Security

Texas Wesleyan University provides reasonable security against unauthorized intrusion and damage to data, information, files, and messages stored on its computer systems within institutional priorities and financial capabilities. The University maintains facilities for archiving and retrieving data stored in user accounts. If a user needs to recover data after an accidental loss, Information & Communication Technology Department personnel should be contacted. Every reasonable attempt will be made to recover the lost or corrupted data. Due to variables associated with the magnetic storage of data, however, Texas Wesleyan University cannot guarantee full restoration in every instance. Further, other users can hold neither Texas Wesleyan University nor any Information & Communication Technology Department personnel accountable for unauthorized access, nor can they guarantee data protection in the event of media failure, fire, criminal acts, or natural disaster.

Copying Software

Respect for the intellectual work and property of others has traditionally been essential to the mission of academic institutions. As members of the university community, Texas Wesleyan University values the free exchange of ideas. Just as Texas Wesleyan University does not tolerate plagiarism, it does not condone the unauthorized copying of software, including programs, applications, operating systems, and databases. Software should not be copied. This refers to any and all software found on Texas Wesleyan University computer systems, encompassing all network servers, personal computers (to include all campus computer lab systems), and computer networks operating on campus. To copy software without the permission of its owner is illegal and a criminal offense.

Copyright Laws-Software

Unless placed in public domain by its owners, software programs are protected by Section 117 of the 1976 Copyright Act. Educational institutions and their constituencies are not exempt from the law. Software is also protected by the license agreement between the owner and purchaser. It is illegal to duplicate, copy, or distribute software or its documentation without the permission of the copyright owner. Violations of authorial integrity, including plagiarism and copyright violations, may be grounds for sanctions against members of the University community.

Liability for Errors

Texas Wesleyan University makes every effort to maintain an error-free hardware and software environment for its authorized users. Nevertheless, it is impossible to ensure that hardware or system software errors will not occur or that staff will always give the most correct advice. Texas Wesleyan University presents no warranty, either expressly stated or implied, for the services or access provided to its authorized users. Damages resulting directly or indirectly from the use of Texas Wesleyan University information technology resources are the responsibility to the authorized user.

Right to Monitor

Texas Wesleyan University owns the campus computer systems networked together on a common fiber-optic network. Every computer attached to the campus network for any reason (e.g., Internet connectivity, e-mail accessibility, etc.) is subject to monitoring by Information & Communication Technology Department personnel. Due to the exponential growth of the number of data packets transmitted through Texas Wesleyan University network, this monitoring is required in order to detect and correct network problems as they occur, thereby ensuring the continued stability of the campus-wide computing environment. Even with the right to monitor, users should continue to expect that their data, files, and e-mail will remain private. System monitoring is a mechanism for monitoring computer system or user activities, not a method for accessing private information. Texas Wesleyan University reserves the right to monitor any computer action or any system record of any action that a user performs while utilizing the campus network.

Campus Computing Facilities

Computer labs on the Texas Wesleyan University campus are not available for general use during the periods when the rooms have been reserved for teaching purposes unless otherwise specified by the professor. It is the responsibility of every user to utilize these facilities in a responsible manner and in accordance with posted computer lab rules and policies. Accidental damage or damage caused by other parties should be reported as soon as possible so that corrective action can be taken.

Specific Issues of Responsible Use

In addition to the issues of responsible user behavior already described in this policy, the following more specific practices applicable to all Texas Wesleyan University computer systems/network users are prohibited:

- access, use, inspection, or modification of data or functions that are neither allotted nor authorized as a part of the user's account or specified as public domain information
- access, use, inspection, or modification of data that refer to computer utilization, computer access authorization, or security
- abuse or improper use of computer hardware, software, or network resources whether located on the Texas Wesleyan University campus or elsewhere on the Internet
- installing or executing unauthorized software on any computer resource
- any activity that might inject a computer virus on to the computer or network systems
- causing noise, displaying abusive or inappropriate behavior towards other users, or creating other disturbances in any campus computing area
- to cause or purposefully allow a computer malfunction or interruption of operation
- sending, printing, or storing obscene, pornographic, fraudulent, harassing, threatening, abusive, racist, or discriminatory images, files, or messages for non-educational purposes
- displaying or printing sexually explicit, graphically disturbing, discriminating, racist, or sexual harassing images or text for non-educational purposes in any campus computing facility or any campus location that can potentially be in view of other individuals
- access or use of another user's account and the data contained in that account
- theft, destruction, or removal of data or University-owned computer resources

- physical or electronic interference with other computer systems users
- dissemination or distribution of a user account password to any other person
- unauthorized use, access, duplication, disclosure, alteration, damage, or destruction of data contained in any electronic file or program, or on any computer, network, or library resource
- use of University information technology resources and associated user accounts that are not assigned, intended, or approved by a University official
- any other practice or user activity that, in the opinion of the chief information officer or the senior vice president and provost, constitutes irresponsible behavior, promotes illegal activities, results in the misuse of computer resources, or jeopardizes the operation of computer or network systems

Violations

This policy applies to all units of Texas Wesleyan University. It is expected that enforcement will require cooperation between such departments as ICT, Human Resources, and Student Services. Prior to any prolonged denial of access or other disciplinary action, a user shall be provided with such due process as may be recommended by University Legal Counsel.

In accordance with established University practices, policies, and procedures, confirmation of inappropriate use of University technology resources may result in termination of access, disciplinary review, suspension, expulsion, termination of employment, legal action, or other disciplinary action. If disciplinary action is deemed necessary, the case will be handled as follows:

1. Policy violations by a student will be referred to the associate vice president of student life and will be handled as outlined in the *Student Handbook.*

2. Policy violations by an employee will be referred to the appropriate supervisor and/or vice president and will be handled as outlined in the *Staff Policy Manual* (staff) or *Faculty Handbook* (faculty).

3. It is understood that University policy does not preclude enforcement under the laws and regulations of the United States of America, the State of Texas, Tarrant County, or City of Fort Worth.

Information & Communication Technology Department personnel will, when necessary, work with other University offices such as the Judiciary Board (in cases involving students), Campus Security, directors/department heads, Deans of the schools, Faculty Council, the University Legal Counsel, and others in the resolution of problems. Anyone who breaks the law may face criminal and/or civil legal action.

Summary

Computer and network resources are of significant value, and their abuse can have a negative impact on other users and the mission of the University as a whole.

Each authorized user of information technology resources at Texas Wesleyan University must assume responsibility for their own behavior while utilizing these resources. Users of information technology at Texas Wesleyan University should accept that the same morality and ethical behavior that serve as guides in our non-computing environments should also serve as guides in our computing and networking environment as well.

The Information & Communication Technology Department of Texas Wesleyan University gratefully acknowledges the model and selected text from "Policy for the Responsible Use of Information Technology," Nichols College (CAUSE Information Resources Library document number CSD1182).