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.

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 employees and staff. 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 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.

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 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.

Computing and information network. The collection of hardware components and computers interconnected by communication channels owned and/or operated by Texas Wesleyan or one of its contracted service providers that allow sharing of resources and information.

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.

Password: An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

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: An individual who employs computers to support Texas Wesleyan business/academic activities, who is acting as the source or destination of information flowing through a computer system.

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 student and employee 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 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 to be used for Texas Wesleyan education, research, academic development, administrative functions, and public service purposes only. Violations include, but are not limited to, activities such as:

- advertising for a for-profit organization;
- running a business or money-making enterprise; and/or
- activities that violate city, state or federal law.

User Accounts
User accounts are designed to ensure that authorized persons have access to appropriate network information and resources and to properly protect those assets. Users are expected to respect these restrictions. Violations of this policy include, but are not limited to, activities such as:

- use of another's password (with or without their knowledge);
- sharing of one's own password with another;
- employing either directly or by implication a false identity when using an account or other network resources;
- attempts to gain access to information or resources for which a user does not have explicit authorization;
- giving another individual the means to access data or resources they are not authorized to access;
- obtaining, possessing, using, or attempting to use information related to someone else's account;
- successfully or unsuccessfully attempting to inspect, modify, distribute, or copy data, mail, messages, or software without proper authorization;
- tapping voice, video, or data lines;
- accessing files by circumventing privacy or security restrictions; and/or
- violations of copyright.

The individual to whom an account is assigned is responsible for all activities and communications that originate from his/her account.

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 faculty, staff, 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
User should have no expectation of privacy. Unless contractual agreements dictate otherwise, messages sent over Texas Wesleyan computer and communications systems are the property of Texas Wesleyan. Administration reserves the right to examine all data stored in or transmitted by these systems. Because Texas Wesleyan computer and communication systems are to be used for University purposes, users are to have no expectation of privacy associated with the information they store in or send through these systems.

When providing computer-networking services, Texas Wesleyan does not provide default message protection services such as encryption. No responsibility is assumed for the disclosure of information sent over Texas Wesleyan networks, and no assurances are made about the privacy of information handled by Texas Wesleyan internal networks. In those instances where session encryption or other special controls are required, it is the user's responsibility to ensure that adequate security precautions have been taken. Nothing in this paragraph must be construed to imply that Texas Wesleyan policy does not support the controls dictated by agreements with third parties, such as organizations that have entrusted Texas Wesleyan with confidential information.

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 designee. The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee.

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 Technology Department personnel should be contacted. Every reasonable attempt will be made to recover the lost or corrupted data. However, Texas Wesleyan University cannot guarantee full restoration in every instance. Further, other users can hold neither Texas Wesleyan University nor any Office of Information Technology personnel accountable for unauthorized access, nor can they guarantee data protection in the event of media failure, fire, criminal acts, or natural disaster.

Copyright Laws-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.

Unless placed in public domain by its owners, software programs are protected from unauthorized use and duplication by law. 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 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.

Care for Network Hardware and Resources
Texas Wesleyan University network users are expected to treat all network and computing hardware with care and are expected to utilize all network and computing resources in ways that respects all others who use the network. The following activities are considered violations of this policy:

- damaging University hardware or software;
- introducing viruses or malware;
- deliberately slowing a system or service; and/or
- attempting to make a system or service inoperable.

Specific Issues of Responsible Use
In addition to the issues of responsible user behavior already described in this policy, the following 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
Any violation of this policy may result in disciplinary action, up to and including termination of employment or expulsion from the University. Texas Wesleyan reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Texas Wesleyan does not consider conduct in violation of this policy to be within an employee's, student's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Texas Wesleyan reserves the right not to defend or pay any damages awarded against employees, students or partners that result from violation of this policy.

Any employee, student, or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her supervisor (employees), the Dean of Students (students) or the Human Resources Department as soon as possible.

The Office of Information Technology 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)