Acceptable Use Policy

Table of Contents

Purpose ........................................................................................................................................... 1
Scope ............................................................................................................................................... 1
Policy ............................................................................................................................................ 1
Violations ....................................................................................................................................... 2
Exceptions ..................................................................................................................................... 2
Definitions ..................................................................................................................................... 2
Related Documents ....................................................................................................................... 3
Approval and Ownership ................................................................................................................ 3

PURPOSE

The components that make up Texas Wesleyan University’s (TW) computing and information network are critical to the operation of the institution. Inappropriate use of the network can adversely impact the ability of TW to accomplish its mission. Every individual who utilizes the network has a responsibility to use these resources in an appropriate manner. The Acceptable Use Policy addresses that responsibility.

SCOPE

This policy applies to all who use the TW computing and information network including but not limited to Texas Wesleyan employees, students and partners.

POLICY

Authorized Access to Network Information and Resources

Network users are expected to respect restrictions on authorized access to network information and resources. 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.
Care for Network Hardware and Resources

Network users are expected to treat all network hardware with care and are expected to utilize all network 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.

Authorized System Use

Network users are expected to use systems for authorized 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.

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 or partners that result from violation of this policy.

Any employee 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, any other supervisor or the Human Resources Department as soon as possible.

EXCEPTIONS

Exceptions to this policy must be made in writing, using the appropriate Exceptions form, by the designated Owner of the system or information that will be out of compliance with this policy and approved by all identified on the Exceptions form including the executive (top senior manager/VP) over the reporting line and Chief Information Officer.

DEFINITIONS

Computing and Information Network – The collection of hardware components and computers interconnected by communication channels owned and/or operated by TW or one of its contracted service providers that allow sharing of resources and information.

Partner – Any non-employee of Texas Wesleyan who is contractually bound to provide some form of service to Texas Wesleyan.

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.
User - Any Texas Wesleyan employee or partner who has been authorized to access any Texas Wesleyan electronic information resource.

**RELATED DOCUMENTS**

Information Security Policy  
Network Protection Policy

**APPROVAL AND OWNERSHIP**

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Title</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorizing Person</td>
<td>Title</td>
<td>MM/DD/YYYY</td>
<td></td>
</tr>
</tbody>
</table>