TRINITY INTERNATIONAL UNIVERSITY

TIU POLICY: **Acceptable Use Technology Policy**

TIU POLICY #: **P-401**

STATUS: **Approved, October 2009**
Updated, August 2016

I. PURPOSE:

Trinity International University (University) provides technology services to employees and currently registered/matriculated students, on networks owned and operated by the University. The University reserves the right to circumscribe operation of its technology services, using policies consistent with its mission and the role technology is intended to play within that mission. The purpose of this policy is to articulate conduct in the use of such services.

II. SCOPE:

This policy applies to all users of the University's network, telecommunications, and technology systems. This includes but it is not limited to e-mail, file transfer, video cameras, or use of applications which utilize the networks. University students, faculty, and staff may be subject to additional guidelines outlined in their respective handbooks.

III. POLICY:

The University network and systems are to be used primarily for activities related to the educational mission of the University.

A. Permitted Use

1. Employees and students are expected to read their University e-mail and are strongly encouraged to use their University e-mail accounts for all communication within the University to ensure reliable and secure delivery.

2. Users are required to know and follow the specific policies and usage procedures for any systems and networks to which they have authorized access.

3. The University recognizes the value of internet access to its mission, as well as to employees and students for personal communication. The University reserves the right to block traffic that creates congestion and contributes no value to the University's mission. Those who use the University network as a gateway to the internet have access to networks and computer systems that contain information over which the

University has no control. The University reserves the right to block access to subject matter on the internet that is in conflict with the University's mission and core values. Any access to sexually explicit or pornographic materials by way of the University internet connection will be blocked, logged, and reported. Students and employees who show evidence of attempted access to such materials are subject to disciplinary action.

4. Electronic records and documents must be managed alongside traditional records to ensure compliance with state and federal regulations and to preserve institutional history. Maintenance and disposal of electronic records, as determined by the content, is the responsibility of the legal custodian and must be in accordance with guidelines established by University approved records retention and disposition schedules (See Document Retention Policy).

B. Privacy

The University will treat data created and/or transmitted by users of its network and computer systems, as allowed in these Terms and Conditions, as confidential. Confidentiality in this context does not imply complete privacy, only that access is limited to authorized individuals in whom the University has placed confidence. Whenever possible, a user's privacy will be respected, but this cannot be viewed as absolute. The University is careful to abide by the requirements of the Family Educational Rights and Privacy Act (FERPA) and the Gramm-Leach-Bliley Act, both of which mandate that institutions implement safeguards for certain information pertaining to students and other consumers.

1. Students and employees can use University owned systems only by obtaining “accounts” for these systems. These accounts are accessed using a username (also called a login name) and a password. Only the person to whom the account is assigned is authorized to use it; the password is intended to ensure this.

2. University personnel can and will access files when necessary for maintaining the University network and computer systems. Every effort will be made to respect privacy of user files, and the contents of user files will be examined only when it is required by law or by the policies of the University.

3. The University reserves the right to cooperate fully with local, state, and federal officials in investigations relating to information accessed or distributed using University computing systems, the University network, the University phone system, or the University internet connection.

C. Unacceptable Use

Any actions that compromise the integrity of the University, data facilities, networks, services, or resources are strictly prohibited. Examples of unacceptable uses include, but are not limited to the following:

1. Using the resources for any purpose that violates federal or state laws;
2. Using someone else’s identity and password for access to University resources, logging others into the network to access University resources, or using the network to make unauthorized access to other networks. Forgery or other misrepresentation of identity

via electronic or other form of communication will be subject to disciplinary action. Prosecution under State and Federal laws may also apply. This includes the use of a network (IP) address not specifically assigned to the individual, or use of a forged or false identity in sending e-mail;

3. Using the resources and misrepresenting your identity or affiliation;
4. Using the resources for computer tampering or unauthorized alteration of data, identification, or credentials;
5. Using the resources to transmit, use or serve unauthorized and/or illegally acquired software, media (audio files/video files);
6. Using the resources for unauthorized browsing or exploring, or making other unauthorized attempts to view data, files or directories belonging to the University or to other users;
7. Violating copyrights of documents or media;
8. Using the resources and introducing deviant software (viruses, worms, etc.) into the University network and systems;
9. Using the resources to access or distribute defamatory, abusive, obscene, sexually oriented, pornographic, threatening, racially offensive or illegal material;
10. Using the resources for misuse of social media, message boards, or any web based community;
11. Using the resources in a manner that requires the University network security to be compromised;
12. Attempting to evade, disable, or obtain passwords or other security provisions of systems on the network;
13. Using the resources for any activity that interferes or inhibits the use of the network or University systems by others;
14. Intercepting or tampering with network packets;
15. Using excessive data storage or network bandwidth in activities such as the "broadcasting" inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages;
16. Tampering with sound systems, lighting systems, or video cameras. Access is limited to trained and authorized personnel;
17. Tampering, modifying, or extending cabling and wiring. This applies to network cabling, hardware, and in-room jacks. Use of non-University network switches, hubs, or wireless networking technology on the University network is prohibited;
18. Using the resources for commercial, sales, and/or advertising purposes;
19. Using the resources for political activities.

The appropriate use of University Technology is a condition of employment and the misuse of University resources may have employment consequences up to, and including, termination.