

Trinity International University

Terms and Conditions for University Technology and Telecommunications Systems

Acceptable Use Policy

Table of Contents

0.0 Highlights	1
1.0 General Information	1
2.0 Computer login and Phone PIN Accounts	1
3.0 The University Network.....	2
4.0 Intended Uses of University Systems and Network.....	2
5.0 Intended Uses of the University Internet Connection	2
6.0 E-mail.....	3
7.0 Confidentiality of User Data	3
8.0 Internet Blocking and Proxy Services.....	4
9.0 On-line Conduct.....	4
10.0 Laws concerning computer usage.....	5
11.0 Suspension or Termination of Accounts.....	6

0.0 Highlights

The following summarizes major points contained in this document. Please read the entire document. This policy supercedes all other policies with respect to Acceptable Use of University networks, phone systems, computer systems, and technology.

0.1 Account Holder responsibilities

Computer login and phone PIN (Personal Identification Number) account holders are responsible for any activity originating from their accounts. Your computer and account may be used:

- for authorized network access to university systems and resources that are used for curricular, academic, and administrative activities
- for e-mail and access to Worldwide Web pages

You may not use University computers, networks, system resources, and phones:

- for commercial or business purposes not related to the University
- for accessing or distributing defamatory, abusive, obscene, sexually oriented / pornographic, threatening, racially offensive or illegal material
- for any activity which interferes or inhibits the use of the network or University systems by others
- to connect non-authorized private networks. University networks may not be modified or extended in any manner that violates a federal, state, or local law or a University policy

Additionally, you may not use University computers, networks, and system resources:

- for unauthorized browsing or exploring, or making other unauthorized attempts to view data, files or directories belonging to TIU or to other users.
- to transmit, use or serve unauthorized software
- to violate copyrights of documents or media
- for misuse of message boards or any web based community
- for computer tampering or unauthorized alteration of data, identification, or credentials
- for introducing deviant software (viruses, worms, etc..) into the University network and systems

Your computer login and phone PIN should NOT be used by family members, friends, classmates or colleagues. Your computer login or phone PIN may be suspended or terminated, and other

disciplinary action taken, for: violating policies in these *Terms and Conditions*

0.2 Students, employees, or other persons granted permission to connect a personal computer to the University network or phones to the University system are subject to all of the terms and conditions in this document.

1.0 General Information

Trinity International University provides computing and telecommunications services to employees and currently registered students, on networks owned and operated by the University. The University reserves the right to circumscribe operation of its computing and telecommunications facilities, using policies consistent with its mission and the role technology is intended to play within that mission. Specifically, each person's conduct in the use of such services is expected to be consistent with and conform to the policies set forth herein and with the University's Mission: *Forming Students to Transform the World Through Christ.*

In any given academic term, computer logins are granted only to students who are officially registered for that term. We trust that all who use the University's technology and systems will behave in ways that demonstrate convincingly to the world that we are *a community seeking to honor Christ and His Kingdom in all we do.*

2.0 Computer login and Phone PIN Accounts

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, or a PIN. Only the person to whom the account is assigned is authorized to use it; the password is intended to ensure this. To allow friends, classmates, parents, spouse, children, colleagues, or anyone else to use one's account is to be in violation of the Acceptable Use Policy. Attempts to use another person's account will result in termination of the violator's account, and other disciplinary actions may be taken as well.

2.1 Employees will automatically receive user accounts when they arrive for their first day of work. During orientation, it shall be verified that the employee has read these *Terms and*

Conditions and pledges to abide by the policies contained therein.

2.2 Students are given accounts when they matriculate, and upon arrival at the University must agree that they have read these *Terms and Conditions* and pledge to abide by the policies contained therein.

3.0 The University Network

The University network connects many University computers, those owned and operated by the University as well as personal computers connected to the University network, and provides the University's gateway to the Internet. In this way the University network mediates access to many other networks and computer systems not owned or operated by the University. Users of the University network are required to adhere to all policies and procedures established by the University, for the University network and for the other networks and systems accessed through this gateway.

3.1 Employees connect to the University network using University-owned computers, located in offices, classrooms or labs. Special permission must be obtained to connect personally owned computers to the University network, and those who connect personal computers to the network must sign a form agreeing to abide by all of the policies in these *Terms and Conditions*.

3.2 Students using University computers in the computer labs, or who use computers set aside by academic or administrative departments for student use, will in general be able to connect to the University network.

3.3 Students in University housing may use personal computers to connect to the University network, and are expected to abide by all of the policies contained in these *Terms and Conditions*.

3.4 Employees or students with notebook computers will be able to connect to the University network from locations set aside for this purpose, in the Library or in other University facilities.

3.5 Individuals may not connect wireless access points to the University network, in any University-owned facility.

4.0 Intended Uses of University Systems and Network

The University network and systems are to be used primarily for activities related to the educational mission of the University. Personal use of the network is limited to communicating by e-mail and accessing Intranet or Internet Web pages, providing such use complies with these Terms and Conditions and does not, at the University's discretion, utilize excessive capacity of resources, or in the case of employees, interfere with the employee's work.

Individuals are not allowed to operate servers of any kind on the University network.

In order to receive a computer account, you agree to abide by the policies set forth in these *Terms and Conditions*, including:

- agreement not to publish, on any system connected to the University network, and not to include in any e-mail communication, information which violates or infringes upon the rights of any other person, is abusive, profane or sexually offensive, or contains advertising or solicitation for goods or services;
- agreement not to transmit via the University network copyrighted documents or media for which you do not have written authorization from the copyright owner;
- agreement not to conduct commercial or business activities, or to perform or solicit others to perform any activity prohibited by law.

5.0 Intended Uses of the University Internet Connection

The University recognizes the value of Internet access to its mission, as well as to employees and students for personal communication. However, the University's Internet resource is limited, expensive, and shared by many users.

Personal use, other than for e-mail and access to Web pages, is not permitted. The University reserves the right to block traffic which creates congestion and contributes no value to the University's mission.

6.0 E-mail

E-mail services are extended for the sole use of University faculty, staff, students and other appropriately authorized users to accomplish tasks related to and consistent with the University's mission. Any e-mail address or account assigned by the University to individuals, sub-units, or functions of the University, is the property of the University.

The University e-mail system is for use by faculty, staff, and students. All messages sent or received are normally retained until deleted by the recipient. Once an account has been terminated, however, no e-mail will be retained. E-mail users are assigned storage quotas and must manage their e-mail accounts in such a way as to stay within quotas.

6.1 E-mail content. All users of the University's e-mail system are expected to abide by the acceptable use policy contained in these *Terms and Conditions*. University policy prohibits sending e-mail containing defamatory, abusive, obscene, sexually oriented, threatening, racially offensive or illegal material. Since the University may be held responsible for inappropriate employee and student use of its e-mail system, it may utilize e-mail monitoring software to screen e-mail sent or received through the University e-mail system. University employees will not normally inspect the contents of e-mail sent to an identified addressee, or disclose such contents to anyone other than the sender or intended recipient, without consent, unless required to do so by law or by the policies of the University, or to investigate complaints regarding e-mail alleged to contain defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

The University reserves the right to cooperate fully with local, state, and federal officials in investigations relating to e-mail transmitted or received using University computing systems, the University network, or the University Internet connection.

6.2 Official communication. Official notifications made by University offices are increasingly made using e-mail, rather than by paper memos sent through the University mail services. E-mail used for such notifications will be delivered to the recipient's University e-mail account.

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.

6.3 Restraint in using e-mail. University e-mail should not be used: (a) to create or forward "chain letters" or "pyramid schemes"; (b) to send or forward "junk mail" or "spam" to individuals not specifically requesting it; (c) to send e-mail using forged addresses or headers; or (d) to broadcast a message to a large number of recipients.

The rule of thumb for (d) is that a message should not be sent to more than forty recipients. This allows broadcasts to be sent to classes, clubs or committees, and other small groups. It does not allow a list of hundreds or thousands of recipients to be broken up into many small lists, to circumvent the "rule of forty."

6.4 Normal account termination. Students or employees who leave the University will have their e-mail accounts terminated. Employee e-mail accounts will normally be terminated on the last day of employment. Students may continue to use University e-mail for up to 30 days after withdrawal or graduation, to permit time for making other arrangements and notifying friends and family of the new e-mail address.

7.0 Confidentiality of User Data

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. University personnel can and will access files when necessary for maintaining the University network and computer systems. Every effort will be made to respect the 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. 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.

8.0 Internet Blocking and Proxy Services

Those who use the University network as a gateway to the Internet have access to networks and computer systems which contain information over which the University has no control. The University reserves the right to block access to subject matter on the Internet which is in conflict with the University's *Mission*.

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.

8.1 The University Proxy Server. A proxy server mediates access to Internet web pages. Its use enables access to certain materials to be restricted. The proxy server (**bess-proxy.tiu.edu, port 8860**) must be used for all Internet access. Use of other proxy servers, or of the above proxy server on any port other than port 80 is prohibited, and is considered to be a violation of the Acceptable Use Policy of these *Terms and Conditions*.

9.0 On-line Conduct

Users may not, under any circumstances submit, publish, or display, on any network or computing system accessed through their University account, any material which is defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal. Transmission of any material, information or software in violation of any local, state or federal law is prohibited. Users agree by virtue of access to the University's computing and e-mail systems, to indemnify, defend and hold harmless the University for any suits, claims, losses, expenses or damages, including but not limited to litigation costs and attorney's fees, arising from or related to the user's access to or use of University e-mail and computing systems, services and facilities.

9.1 Commercial or Business Activity. Users of University computer systems or the University network may not use these to engage in commercial or business activity.

9.2 Authorized Software. Only software for which the owner or copyright holder has given

written consent for online distribution may be transferred to or stored on University systems, or operated on computers connected to the University network. Software designed to interfere with others' use of computing systems or networks is prohibited.

The University reserves the right to terminate accounts and/or University networking privileges of users who violate this policy.

9.3 Copyrighted Material. Copyrighted material must not be placed on University computing systems. Furthermore no one may transfer copyrighted material using the University network, without written permission.

Only the author(s) or individuals that they specifically authorize may transfer copyrighted material from other media to University computing systems. Material in this category includes not only human readable documents, but also software and data files used with software designed to play musical, video, or multimedia productions. In particular, providing access to copyrighted MP3 files from media is prohibited.

9.4 Public Domain Material. Users may upload public domain programs or non-copyrighted information using the University's computing systems. Users assume all risks regarding the determination of whether such programs or other materials are in the public domain.

9.5 Inappropriate Material. Off-University systems which University users may access can contain material which is abusive, defamatory, inaccurate, obscene, profane, sexually oriented, threatening, racially offensive, or illegal. The University reserves the right to monitor its computer systems and University network to ensure that such materials are not present. Students or employees who knowingly bring such materials into the University computing environment will be subject to the same disciplinary policies which apply in other University situations. Electronic forums do not constitute a separate universe of discourse, governed by a separate ethic, but must be governed by the same moral and ethical guidelines which govern other means of discourse at the University.

9.6 Message Boards. The University has no control over the content of messages on external message boards, but all content posted by University users to any message board must adhere to these *Terms and Conditions*. The

University reserves the right to terminate accounts of users who misuse message boards.

9.7 Real-time / Interactive Communication.

The use of real-time, interactive messaging systems is recognized to be of value in certain situations. The University reserves the right, however, to limit or circumscribe the use of such systems, and to terminate user accounts and/or University networking privileges for those who misuse such services.

9.8 Modem Usage. A modem pool is maintained to allow users working at off-University locations to access the University e-mail system. The modem pool is limited, and users are asked to keep modem sessions brief.

9.9 Security. Security on computer systems receives a high level of priority at the University. Users who identify situations that pose threats to information security are asked to notify the Information Technology Help Desk.

Passwords should be so chosen that they are unlikely to be guessed by others. Strong passwords usually contain mixed-case letters as well as numerals or punctuation marks. Please assist University security efforts by choosing passwords wisely, changing them periodically, and not revealing them to others. Users should notify Computing Services if their passwords are forgotten or if there is reason to believe someone has obtained unauthorized access to their accounts.

9.10 Privacy of Information. All information on University computer systems should be considered private, unless it has been explicitly classified otherwise. Any attempt to circumvent computer or network security in order to gain access to private information is illegal, as outlined below.

Under the Illinois Freedom of Information Act (FOIA), electronic files are considered the same as paper files. Any official university documents (as defined by law) in the files of employees of the State of Illinois are considered public documents, and may be subject to inspection through FOIA. Any inspection of electronic files and any action based upon such inspection will be governed by all applicable U. S. and Illinois laws and by university policies.

10.0 Laws concerning computer usage

10.1 Computer Tampering. The following excerpt is from the Illinois Criminal code. § 16D-3. Computer Tampering.

(a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him:

- (1) Accesses or causes to be accessed a computer or any part thereof, or a program or data;
- (2) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains data or services;
- (3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and damages or destroys the computer or alters, deletes or removes a computer program or data;
- (4) Inserts or attempts to insert a "program" into a computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete, or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such program".

* * *

(b) Sentence: A person who commits the offense of computer tampering as set forth in subsection (a).(1) of this Section shall be guilty of a Class B misdemeanor.

(2) A person who commits the offense of computer tampering as set forth in subsection (a)(2) of this Section shall be guilty of a Class A misdemeanor and a Class 4 felony for the second or subsequent offense.

(3) A person who commits the offense of computer tampering as set forth in subsection (a)(3) of this Section shall be guilty of a Class 4 felony and a Class 3 felony for the second or subsequent offense.

* * *

(c) Whoever suffers loss by reason of a violation of subsection (a)(4) of this Section may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses. Source P.A. 91-233 effective 1-1-00.

10.2 Unlawful use of recordings. The following excerpt is from § 720 ILCS 5 / 16-8 of the Illinois Criminal Code. Sec. 16-8. Unlawful use of unidentified sound or audio visual recordings.

(a) A person commits unlawful use of unidentified sound or audio visual recordings when he intentionally, knowingly, recklessly or negligently for profit manufactures, sells, distributes, vends, circulates, performs, leases or otherwise deals in and with unidentified sound or audio visual recordings or causes the manufacture, sale, distribution, vending, circulation, performance, lease or other dealing in and with unidentified sound or audio visual recordings.

(b) Unlawful use of unidentified sound or audio visual recordings is a Class 4 felony; . . .

11.0 Suspension or Termination of Accounts

User accounts on University computers are terminated on the last day of work for employees and upon withdrawal or graduation for students. E-mail accounts remain active for up to 30 additional days for students. The University reserves the right to suspend or terminate a user's account on the University computing systems, or to suspend or terminate University network privileges, for breaches of policy as set forth in these *Terms and Conditions*.

12.0 Acceptable Use Policy for University Network/Telecommunication System Users

The following policies extend or interpret the above Terms and Conditions with respect to University network and telecommunication system usage:

12.1 University network services and wiring may not be modified or extended. This applies to network wiring, hardware, and in-room jacks. Use of non-University Ethernet switches, network hubs, or wireless networking technology on the University network is expressly prohibited.

12.2 University network users may not allow their University network connection to be used by anyone outside the University community, and under no circumstances may users provide access to University systems or networks for other individuals

12.3 University network users may not operate network services from their computers (BBS, Chat, DHCP, DNS, anonymous FTP, IRC, NNTP, POP2/POP3, SMTP, INS, etc.). Users who have a *bona fide* academic need to operate such services must obtain written authorization from University network administration prior to activating any such service.

12.4 Commercial network resources and software which are licensed by the University for internal usage only may not be used outside the University network.

12.5 Network usage that inhibits or interferes with the use of the network by others is not permitted. Applications which make heavy use of network bandwidth for extended periods of time, and applications designed to send repeated e-mail messages or mass e-mail messages ("e-mail bombs" or "bulk e-mailers") are not permitted.

12.6 University network may only be used for legal purposes and to access only systems, software and data to which the user has authorized access. Providing access to copyrighted software or other material (including MP3 or similar files from copyrighted media) on the network is prohibited.

12.7 Respecting the rights of other users, including their rights as set forth in other University policies for students, faculty, and staff, is required at all times.

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

12.9 University network is provided for use within the context of the academic mission of the University. It may not be used for commercial purposes or for advertising. Users may not provide open access from their computers to anything protected by copyright (including MP3 files from copyrighted media), or of a sexually explicit or pornographic nature, or which violates University policy or Residence Life community standards.

12.10 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.

12.11 The University may refuse network access to anyone who violates its policies or abuses the rights of others. If it is suspected that a University network connection has been used to violate policy, that connection may be suspended without prior notice, pending investigation and resolution of the issue. The University reserves the right to scan any part of its network, including the University network, for security problems, and to monitor traffic and usage patterns on its network.

12.12 The University retains the right to block or to disable network applications which use excessive network bandwidth or which facilitate illegal activity.

13.0 Other Provisions

The *Terms and Conditions* shall be interpreted, construed and enforced in all respects in accordance with the laws of the State of Illinois. Each user irrevocably consents to the jurisdiction of the courts of the State of Illinois and the federal courts situated in the State of Illinois, in connection with any action to enforce the provisions of the *Terms and Conditions*, to recover damages or other relief for breach or default under the *Terms and Conditions*, or otherwise arising under or by reason of the *Terms and Conditions*.

CHI\4045452.2