UNIVERSITY POLICIES

Acceptable Use Policy for Technology and Telecommunication Systems

Students are responsible for abiding by the complete text contained within the policy. This policy applies to all individuals with respect to the acceptable use of university networks, phone systems, computer systems, and technology.

Trinity International University provides technology services to employees and currently registered/matriculated students, on networks owned and operated by the university. TIU 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.

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 applications which utilize the networks. University students, faculty, and staff may be subject to additional guidelines outlined in their respective handbooks.

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

Permitted Use

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

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.

- 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.
- 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.
- 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.

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:

- Using the resources for any purpose that violates federal or state laws.
- 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.
- Using the resources and misrepresenting your identity or affiliation.
- Using the resources for computer tampering or unauthorized alteration of data, identification, or credentials.
- Using the resources to transmit, use or serve unauthorized and/or illegally acquired software, media (audio files/video files).
- 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.
- Violating copyrights of documents or media.
- Using the resources and introducing deviant software (viruses, worms, etc.) into the University network and systems.
- Using the resources to access or distribute defamatory, abusive, obscene, sexually oriented, pornographic, threatening, racially offensive or illegal material.
- Using the resources for misuse of social media, message boards, or any web based community.

- Using the resources in a manner that requires the University network security to be compromised.
- Attempting to evade, disable, or obtain passwords or other security provisions of systems on the network.
- Using the resources for any activity that interferes or inhibits the use of the network or University systems by others.
- Intercepting or tampering with network packets.
- 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.
- Tampering with sound systems, lighting systems, or video cameras. Access is limited to trained and authorized personnel.
- 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.
- Using the resources for commercial, sales, and/or advertising purposes.
- 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.

Copyright Policy

The Copyright Permissions Act of 1976 as it may have been or will be amended from time to time requires that permission to reproduce copyrighted materials be obtained from the copyright owner except under very limited circumstances. Faculty, staff, and students of Trinity are expected to comply with the provisions of the state and federal intellectual property laws, such as the Copyright Act. Procedures for obtaining copyright permissions for course materials have been established and should be followed. Copies of this procedure and other information explaining the Copyright Permissions Act as it pertains to copying both course materials and material for personal use are available through the Dean's Office.

Family Educational Rights and Privacy Act of 1974

The purpose of the Family Educational Rights and Privacy Act of 1974 (Public Law 93-380) as amended (FERPA) is to ensure access to educational records for students and parents while protecting privacy of such records and to control the careless release of educational information.

In accordance with requirements established by FERPA also commonly known as the "Buckley Amendment," Trinity International University hereby provides notice of intention to comply fully with FERPA and also provides notice to students of their rights under FERPA.

In general, the purpose of FERPA is to give presently or formerly enrolled students access to their individual educational records maintained at Trinity and to protect such students' right to privacy by limiting the transfer of their records without their consent. "Educational records" are defined as those records, files, documents, and other materials directly related to a student that are maintained by Trinity, or by a person acting for Trinity, in the normal course of business. The Records Office has a full copy of FERPA should you desire to review it in full.

FERPA clarifies that an institution is not required to grant access to students to certain materials, including the following:

- Private notes and other materials created by Trinity's personnel, provided they are not revealed to another individual.
- Medical, psychiatric, or similar records created or maintained by a physician, psychiatrist, or psychologist (or other recognized professional acting in such capacity) that are used solely in connection with treatment purposes and only available to recognized professionals in connection with such treatment (provided, however, that a physician or other appropriate professional of the student's choice may review such records).
- Law enforcement records, which are kept separate from educational records, are maintained for law enforcement purposes only and are available only to law enforcement officials. (In each case, student access to such records is at the sole discretion of the individual who maintains these materials.)

It should also be noted that FERPA specifically indicates that the legislation does not alter the confidentiality of communications otherwise protected by law. To ensure that the school does not compromise the rights of individuals enjoyed prior to the enactment of the legislation, students and alumni will not be permitted access to materials of an evaluative nature that were received or placed in files prior to November 19, 1974.

Additionally, as provided by FERPA, students shall not have the right to see confidential letters and statements of recommendation placed in educational records prior to January 1, 1975, provided that they are used only for the purposes for which they were intended. FERPA further stipulates that students do not have the right to see financial records of their parents.

As provided by the legislation, students may voluntarily waive their rights of access to confidential recommendations on or after January 1, 1975, in three areas: admissions, job placement, and receipt of awards. Under no circumstances, however, can a student be required to waive this right.

FERPA also makes clear that the parent or legal guardian of a dependent student, as defined for federal Income Tax purposes, has a right to information about his or her child without the school's having to seek the student's consent. Thus, upon the written request of a parent or legal guardian of a dependent student, the school will honor this right to the extent that it is required by law.

As provided by FERPA, the school retains the right to release at its discretion the following categories of information with respect to each student presently or previously attending the school: the student's name, address, telephone listing, e-mail address, photograph, date and place of birth, major field of study, grade level, enrollment status (e.g., undergraduate or graduate, full-time or part-time, etc.), dates of attendance, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors, awards received, and the most recent educational agency or institution attended. Students have a right to inform the school within a reasonable period of time that any or all of this information which is designated as "directory information" should not be released without their prior consent. Requests by the student to suppress from public distribution the above mentioned

information are to be made annually. Email records@tiu.edu to initiate such suppression.

As required by FERPA, the school hereby provides public notice of its intention to publish this type of information in the annual directory. In complying with the legislation, the school has adopted the procedures and policies below, in addition to those previously noted. Except for those parties stated below, no one shall have access to education records without the written consent of the student concerned. The exceptions to the consent requirement are as follows:

- University officials, including faculty, who have legitimate educational interests.
- Officials of other schools or school systems in which the student intends to enroll, upon condition that the student is notified of the transfer, receives a copy of the record if desired, and has an opportunity for a hearing to challenge the content of the record.
- Those representatives of the federal government and the state who are identified in FERPA, provided that any data so released are not to include information (including social security numbers) that would permit the personal identification of the students unless otherwise specifically provided by federal law.
- Those who serve in connection with the student's application for, or receipt of, financial aid.
- State and local officials or authorities to which such information is specifically required to be reported or disclosed pursuant to state statute adopted prior to November 19, 1974.
- Organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction if such studies are conducted in such a manner as will not permit the personal identification of students or their parents by persons other than representatives of such organizations, and such information will be destroyed when no longer required for the purpose for which it is conducted.
- Accrediting organizations in order to carry out their accrediting functions, or by the dean of students or the emergency dean, designated to act in an emergency to protect the health or safety of the student or other persons.
- To parents of a dependent student as defined in Section 152 of the Internal Revenue Code.
- To comply with a judicial order or lawfully issued subpoena, subject to the notice provisions of the law.
- In connection with a health or safety emergency.
- Information that has been designated as "directory information."
- To the parent of a student who is not an eligible student or to the student.
- To an alleged victim of any crime of evidence, as that term is defined in Section 16 of Title 18, United States Code, of the results of any disciplinary proceeding conducted by an institution of postsecondary education against the alleged perpetrator of that crime with respect to that crime.
- Records (usually only transcripts) released to any organization, agency, or individual at a student's request shall be transmitted with a notice informing the recipient that such information is released only on the condition that the recipient will not permit any other party to have access to such information without the written consent of the student.
- Each office that maintains education records shall maintain a record for each student that shall list all individuals (except institution officials described above), agencies, or organizations that have requested or obtained access to such student's education record.
- Student may inspect material belonging to their education record solely at the office that is responsible for maintaining such information. Any Trinity employee may require that the student inspect that record only in the presence of the professional or staff person qualified to assist in interpreting the information.

Each Trinity department has the ultimate responsibility for establishing appropriate procedures; however, each Trinity department has been instructed to ask that the student's request be made in writing and, where appropriate, in person. On request, students may be required to identify themselves in filing a request prior to having access to their records. The student is obligated to examine the record during reasonable hours at the place the record is maintained and not to interfere with the operation of the office in which the record is being maintained. Under the Act, the school has forty-five days from the time of request until it must comply with the request.

Copies of records accessible to students shall be transmitted to the student upon payment of the established fee for issuing such copies. The Act does not preclude the school's right to destroy any records if not otherwise precluded by law, unless prior to destruction the student has requested access. In fact, there is general encouragement to reduce the number of records so that destruction of records is consistent with the spirit of the law.

As of January 3, 2012, the U.S. Department of Education's FERPA regulations expand the circumstances under which your education records and personally identifiable information (PII) contained in such records, including your Social Security Number, grades, or other private information, may be accessed without your consent. First, the U.S. Comptroller General, the U.S. Attorney General, the U.S. Secretary of Education, or state and local education authorities ("Federal and State Authorities") may allow access to your records and PII without your consent to any third party designated by a Federal or State Authority to evaluate a federal- or state-supported education program. The evaluation may relate to any program that is "principally engaged in the provision of education," such as early childhood education and job training, as well as any program that is administered by an education agency or institution. Second, Federal and State Authorities may allow access to your education records and PII without your consent to researchers performing certain types of studies, in certain cases even when we object to or do not request such research. Federal and State Authorities must obtain certain use-restriction and data security promises from the entities that they authorize to receive your PII, but the Authorities need not maintain direct control over such entities. In addition, in connection with Statewide Longitudinal Data Systems, State Authorities may collect, compile, permanently retain, and share without your consent PII from your education records, and they may track your participation in education and other programs by linking such PII to other personal information about you that they obtain from other Federal or State data sources, including workforce development, unemployment insurance, child welfare, juvenile justice, military service, and migrant student records systems.

Firearms, Weapons, and Explosives

Possession of firearms, weapons, or explosives on campus is not permitted. Students who are found in possession of any type of firearm, weapon, or explosive are subject to immediate dismissal from the institution. This includes, but is not limited to, BB guns, paint ball guns, air-soft pellet guns, bows and arrows, ammunition, sling blades of more than four inches, toy guns, and any other weapon of any kind or imitation thereof that could be used to cause fear or injury to another person.

Student Loan Program Code of Conduct

Trinity International University (TIU) has adopted a Code of Conduct, in compliance with sec 487(a) (25) of the HEA of 1985.

The goal of the TIU Office of Student Financial Services is to provide the highest quality service in the most efficient and timely manner possible, while upholding the mission of the institution and acting with the integrity of a Christian institution. The TIU Office of Student Financial Services willingly adheres to the following Code of Conduct. Likewise, all officers, employees, and agents of TIU willingly agree to adhere to the Code of Conduct.

> Code of Conduct: TIU will not enter into a revenue-sharing agreement with any lender. A "revenue-sharing arrangement" is defined to mean any arrangement made between an institution and a lender under which the lender makes Title IV loans to students attending the institution (or to the families of those students), the institution recommends the lender or the loan products of the lender and, in exchange, the lender pays a fee or provides other material benefits, including revenue or profit-sharing, to the institution or to its officers, employees or agents.

TIU embraces a ban on the employees of the university receiving gifts from a lender, guaranty agency, or loan servicer. No officer or employee of the TIU Office of Student Financial Services, (or an employee or agent who otherwise has responsibilities with respect to educational loans) will solicit or accept any gift from a lender, guarantor, or servicer of education loans. A "gift" is defined as any gratuity, favor, discount, entertainment, hospitality, loan, or other item having monetary value of more than a *de minimus* amount. However, a gift does not include:

- A brochure, workshop, or training using standard materials relating to a loan, default aversion, or financial literacy, such as a brochure, workshop, or training.
- Food, training, or informational material provided as part of a training session designed to improve the service of a lender, guarantor, or servicer if the training contributes to the professional development of the institution's officer, employee, or agent.
- Favorable terms and benefits on an education loan provided to a student employed by the institution if those terms and benefits are comparable to those provided to all students at the institution.
- Entrance and exit counseling as long as the institution's staff are in control of the counseling and the counseling does not promote the services of a specific lender.
- Philanthropic contributions from a lender, guarantor, or servicer that are unrelated to education loans or any contribution that is not made in exchange or advantage related to education loans.
- State education grants, scholarships, or financial aid funds administered by or on behalf of a State.

TIU embraces a ban on contracting agreements. No officer or employee of the university (or agent who otherwise has responsibilities with respect to education loans) will accept from a lender, or an affiliate of any lender, any fee, payment, or other financial benefit as compensation for any type of consulting arrangement or contract to provide services to or on behalf of a lender relating to education loans.

TIU embraces a prohibition against steering borrowers to particular lenders or the delay of loan certifications. For the first-time borrower, TIU will not assign, through the award packaging or other methods, the borrower's loan to a particular lender. In addition, TIU will not refuse to certify, or delay the certification, of any loan based on the borrower's selection of a particular lender or guaranty agency.

TIU embraces a prohibition on offers of funds for private loans. TIU will not request or accept from any lender any offer of funds for private loans, including funds for an opportunity pool loan, to students in exchange for providing concessions or promises to the lender for a specific number of Title IV loans made, insured, or guaranteed, a specific loan volume, or a preferred lender arrangement. An "opportunity pool loan" is defined as a private education loan made by a lender to a student (or the student's family) that involves a payment by the institution to the lender for extending credit to the student.

TIU bans the use of staffing assistance from lenders. TIU will not request or accept from any lender any assistance with call center staffing or Office of Student Financial Services staffing, except that provided by a lender that involves professional development training, educational counseling materials (as long as the materials identify the lender that assisted in preparing the materials), or staffing services on a short-term, nonrecurring basis during emergencies or disasters.

TIU adopts a ban on advisory board compensation. An employee of TIU who serves on an advisory board, commission, or group established by a lender or guarantor (or a group of lenders or guarantors) is prohibited from receiving anything of value from the lender, guarantor, or group, except for reimbursement for reasonable expenses incurred by the employee for serving on the board.

VA Benefits

In accordance with Title 38 US Code 3679 subsection (e), this school adopts the following additional provisions for any students using U.S. Department of Veterans Affairs (VA) Post 9/11 G.I. Bill® (Ch. 33) or Vocational Rehabilitation & Employment (Ch. 31) benefits, while payment to the institution is pending from the VA. This school will not:

- Prevent the student's enrollment.
- Assess a late penalty fee to the student.
- Require the student to secure alternative or additional funding.
- Deny the student access to any resources (access to classes, libraries, or other institutional facilities) available to other students who have satisfied their tuition and fee bills to the institution.

However, to qualify for this provision, such students may be required to:

- Produce the VA Certificate of Eligibility by the first day of class.
- Provide a written request to be certified.
- Provide additional information needed to properly certify the enrollment as described in other institutional policies.

® GI Bill® is a registered trademark of the U.S. Department of Veterans Affairs (VA).