

Policy for the Responsible Use of Information and Technology Resources

Responsible Department: Information Technology

Responsible Administrator: Kay Reeves, Executive Director for Information Technology

Reviewed/Updated Date: November 1, 2016

Date of Scheduled Review: November 1, 2019

Executive Summary

The following policy outlines the protocol and procedures regarding the use of technology and storage of data at Abilene Christian University. The policy applies to all persons who use ACU's computing resources, including but not limited to employees, students, visitors, and contractors. The following basic principles will be covered in this policy:

- ACU owns all data stored on any and all computing devices in the possession of the university, and thus, with cause, and by request of Human Resources and the Legal office have the right to look at or collect any of that data.
- ACU is responsible for all data going across both its wired and wireless network, and thus, with cause, and by request of Human Resources and the Legal office have the right ask questions about, and observe any of this data.
- Use of technology is governed by ACU's employee code of conduct; including ethical, immoral, and/or criminal activity.
- Violations of this policy may result in revocation of access, suspension of accounts, disciplinary action including dismissal, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities.

I. PURPOSE

This policy is designed to perpetuate ACU's academic, research, and service mission by defining the appropriate and responsible use of the information and technology resources at ACU. Each authorized user of these resources must assume responsibility for his/her own behavior while utilizing these assets. Users of these resources should accept that the same morality and ethical behavior that serve as guides in its non-technology environments should also serve as guides in its information and technology environment. It is imperative that the campus community understands that information and technology resources require responsible behavior from all its users.

II. SCOPE

This policy applies to all faculty, staff, students, contractors or any other individual using information and technology at ACU. Access to ACU-owned hardware, software and support provided by technology staff members is a privilege and not a right. Accepting access to this information and technology carries an associated expectation of responsible and acceptable use. When accessing any remote resources using ACU technology resources, users are required to comply with both the policies set forth in this document and all [applicable policies](#) governing the use and access of the remote systems. When these policies conflict with each other, this policy and all other ACU policies will supersede the remote system's policies.

III. DEFINITIONS

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.

Hardware - Any and all tangible or physical devices attached to or used in conjunction with a computer system.

Network - The interconnection of communication lines, including wireless connections, with a computer through remote terminals or a complex, consisting of two or more interconnected computers.

Program - An ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

Resources - Any and all computerized institutional data, computer hardware, and computer software owned by or operated at ACU and any of those of a hosted service.

Software - A set of computer programs, procedures, or associated documentation used in the operation of a computer system.

System - A set of related computer equipment, hardware or software.

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, digital media or those of a hosted service. Data are property.

Data Steward - Individual responsible for the accuracy and institutional responsibility for a set of data, e.g., Human Resources Director for personnel and payroll data, Registrar for student records.

Institutional policy - A succinct and cogent written document bearing the approval of the President's Cabinet of the university that clearly defines faculty, staff, student, and institutional responsibilities within a prescribed area of campus existence.

Property - Anything of value, including but not limited to financial instruments, information, electronically produced data, computer software, and computer programs.

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 ACU.

Technology resources - Any and all computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data.

User - Any faculty, staff, student, or any person authorized to access and use the information technology resources at ACU.

User account - Any logical access on any ACU computer system that has been specifically established for a particular user. A user account may have a dedicated logical area on one or more ACU computer system also associated with it.

IV. PROCEDURE (OR PROCESS)

1. SECTION ONE – GENERAL

1.1. Access & Privileges

1.1.1. User Accounts

Users are provided access as outlined in ACU's Account Management Policy to various information systems and technology based upon their individual role and need. Access is a privilege, not a right, and may be revoked for any reason, including non-compliance with ACU's Account Management Policy.

1.1.2. ACU ID:

Users are responsible for all activity performed with their ACU ID. ACU IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their ACU IDs without the express permission of Information Technology. Similarly, users are forbidden from performing any activity with ACU IDs belonging to other users. Any suspected unauthorized access of a user account should be reported immediately to the Chief Business Officer or their designee.

1.1.3. Passwords

Passwords must never be shared or revealed to anyone else besides the authorized user, unless authorized by the Chief Business Officer or the Executive Director of Information Technology. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. Users may share data by electronic mail, public directories on local area network servers, and other mechanisms, in compliance with policies, regulations or practices related to PII, FERPA or HIPPA. All users are responsible for both the protection of their user account passwords and the data stored in their user accounts.

1.1.4. System Privilege Deactivation

All accounts may be deactivated if account privileges are no longer commensurate with a user's function at the university or their need to know due to a change in their status. See employee specific and student specific deactivation policies in the Account Management Policy.

1.1.5. No Responsibility for Personally-Owned Devices

ACU cannot provide, and will not be responsible for, software or data kept on personally-owned computers, nor is it responsible for the installation, repair, maintenance, or upgrade of personally-owned hardware (e.g., computers, game consoles, TVs).

1.2. Acceptable Use

1.2.1. Acceptable Uses of Information and Technology Resources

Priority is given to all information and technology resources at ACU that provides users in acquiring and disseminating information related to the performance of regularly assigned job duties, classroom assignments, or scholarly research.

1.2.2. Unacceptable Uses of Information and Technology Resources

Any information, data, or programs not aligning with the mission of ACU must not be created, stored, transmitted, viewed, or manipulated using ACU-owned technology or information systems.

This is a non-exhaustive list of unacceptable uses of information and technology resources at ACU:

- A) Transmitting any material, or engaging in any other activity in violation of any federal, state, or local laws, including U.S. and international copyright law or trade agreements.
- B) Transmitting or accessing information containing harassing material. Electronic harassment includes, but is not limited to:
 - i. communication with the intent to harass, terrify, intimidate, threaten or offend another person
 - ii. contact of another person with the intent to harass, whether any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease
 - iii. the disruption or damage of academic, research, administrative, or related pursuits of another
 - iv. invading the privacy, academic or otherwise, of another, or the threatened invasion of the privacy of another
- C) Transmitting, receiving, displaying, or viewing offensive content in violation of the code of conduct set forth in the [Employee](#) and [Student](#) Handbook, which includes, but is not limited to:
 - i. sexual comments or images
 - ii. racial slurs
- D) Disseminating or printing copyrighted materials, including computer files, articles, and software, in violation of U.S. and international copyright laws or trade agreements
- E) Attempting forgery of email messages
- F) Physical or electronic interference with other users

- G) Any other practice or activity that management judges to constitute irresponsible behavior, promote illegal activities, result in the misuse of resources, or jeopardize the operation of information and technology resources at ACU.

1.2.3. Prohibition Against Commercial Use of Information Resources

ACU users must not use ACU information and technology resources for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by ACU leadership. Prohibited activity includes, but is not limited to operating a business, usurping business opportunities, or soliciting money for personal gain.

1.3. Privacy and Data Ownership

1.3.1. Legal Ownership of Information Systems Files and Messages

ACU has legal ownership of the contents of all files stored on its information and technology resources as well as all content transmitted via these systems. ACU reserves the right to access all such information without prior notice whenever there is a genuine business need.

1.3.2. No Responsibility for Monitoring Content of Information Systems

ACU reserves the right to remove any message, file, database, graphic, or other material from its information and technology resources. At the same time, ACU has no obligation to monitor the information content residing on or flowing through those systems.

1.3.3. Privacy Expectations and Information Stored on ACU Systems

At any time and without prior notice, ACU reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on ACU information and technology resources. Similarly, at any time and without prior notice, ACU reserves the right to examine or monitor any device attached, for any reason, to the ACU network. This examination is performed to ensure compliance with internal policies, to support the performance of internal investigations, to comply with legal requirements such as a subpoena or court order, and to assist with the management of ACU's systems. It is also possible that other individuals, organizations, and agencies, with permission from ACU administrators, may likewise access or monitor these same systems whenever ACU has a legitimate business need for them to do so.

1.3.4. Disclaimer of Responsibility for Damage to Data and Programs

ACU uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by information and technology resources. In keeping with these objectives, ACU maintains the authority to:

- A) restrict or revoke any user's privileges
- B) inspect, copy, remove, or otherwise alter any data, program, or other resource that may undermine these objectives
- C) take any other steps deemed necessary to manage and protect those systems. This authority may be exercised with or without notice to the involved users. ACU disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

1.4. Intellectual Property

1.4.1. Software and Copyrights

Unauthorized copying of software is strictly forbidden by ACU. Additionally, ACU constituents are expected to adhere to current Copyright Laws.

1.4.2. Fair use

Unless permission from the copyright owner(s) is first obtained, making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

2. SECTION TWO – SPECIFIC POLICIES FOR STUDENTS

2.1. Student Specific Privileges

2.1.1. System Privilege Activation

ACU information and technology resources privileges are activated at the time that a student is admitted to ACU. The specific time an account is active may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology.

All normal access, defined as access necessary for an individual to perform the tasks expected of their role at the university, and only normal accesses, are created when the student is admitted to the university and will persist so long as the individual remains an active participant in the ACU community. More specific references can be found in the Account Management Policy.

2.1.2. System Privilege Deactivation

All ACU information and technology resources privileges are deactivated at the time that a student is no longer an active member of the ACU community, except access to email. The time frame for deactivation may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology. All data, files, or messages may be removed from user accounts when account deactivation occurs. More specific references can be found in the Account Management Policy.

2.2. Campus Computing Facilities

2.2.1. Acceptable Use of Facilities

Computer labs on the ACU campus are not available for general use during the periods when the rooms have been reserved for teaching purposes, unless otherwise specified by the professor. Facilities are often made available on an unmonitored basis. It is the responsibility of every user to use these facilities in a responsible manner.

2.2.2. Disruptive Behavior

Students using campus computing facilities must not cause unnecessary noise, display abusive or inappropriate behavior towards other users, or create other disturbances in any campus computing area.

2.2.3. Data Protection

Students using campus computing facilities must not access, destroy or remove data other than their own.

2.2.4. Destruction of Computer Resources

Students using campus computing facilities must not destroy or remove ACU-owned computer resources.

2.2.5. Alteration of Lab Computer Setup

Students using campus computing facilities must not attempt to change the hardware and software configurations on ACU-owned computers.

2.2.6. Damage Reporting

Students using campus computing facilities must report accidental damage or damage caused by other parties to Team55.

3. SECTION THREE – SPECIFIC POLICIES FOR EMPLOYEES (Faculty, Staff and Student Employees)

3.1. Privileges

3.1.1. System Privilege Activation

ACU information and technology resources privileges are activated at the time that an individual is hired as an employee of ACU. The specific time an account is active may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology. All normal access, defined as accesses necessary for an individual to perform the tasks expected of their role at the university, and only normal accesses, are created at the point of hire and will persist so long as the individual remains an active participant in the ACU community. More specific references can be found in the Account Management Policy.

3.1.2. System Privilege Deactivation

All ACU information and technology systems privileges are deactivated at the time that an employee ceases to provide services to ACU. The time frame for deactivation may vary according to the needs of specific systems and are determined by procedures (often automated) established by the Executive Director of Information Technology. (See Exception to System Privileges). All data, files, or messages may be removed from user accounts when account deactivation occurs. More specific references can be found in the Account Management Policy.

3.1.3. Exception to System Privilege Deactivation

ACU retirees are eligible to receive access to an ACU email account using their ACU ID and password. This is a privilege and may be revoked at any time. Retirees must agree to abide by all ACU information policy in order to maintain their account.

3.1.4. Incidental Personal Use of Information Resources

ACU allows computer users to make reasonable and incidental personal use of ACU's information and technology resources. Incidental personal use is permissible if the use does not interfere with worker productivity, and does not preempt any business activity. All such personal use must be consistent with conventional standards of ethical and polite conduct. For example, electronic mail must not be used to distribute or display messages or graphics that may reasonably be considered to be disruptive or offensive (such as sexual jokes or pornography).

3.2. Privacy

3.2.1. Privacy / Administrative Data

Security and confidentiality are matters of concern to all ACU employees who have access to information and technology resources. ACU is responsible for the accuracy, integrity, and confidentiality of its electronic databases. All administrative electronic data must be treated as confidential, other than data that has been designated as approved for release to the public by ACU administrators. By law, certain electronic institutional data are confidential and may not be released without proper authorization. Since conduct, either on or off the job, could affect or threaten the security and confidentiality of this information, each employee who accesses any ACU information and technology resource is required to adhere to the following:

- A) No one shall make or permit unauthorized use of any information in files maintained, stored, or processed by any ACU software.
- B) No one is permitted to seek personal benefit, allow others to benefit personally or to divulge, in any way, the contents of any record or report, to any person except in the conduct of his/her work assignment.
- C) No one shall knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry. No one shall knowingly change or delete or cause to be changed or deleted an entry in any record or report, unless expressly authorized to do so and in accordance with approved policies and procedures.
- D) Once information is downloaded, data should not be altered in word processing documents or spreadsheets in a way that misrepresents the information derived from these data. Downloaded information should be used and represented responsibly.

- E) No official record or report, or copy thereof, shall be removed from the office where it is maintained, copied, or printed via electronic means except in the authorized performance of a person's duties, and in accordance with established procedures. Copies made in the performance of a person's duties shall not be released to third parties except as in paragraph 3.2.1 above applies.
- F) No one is to aid, abet, or act in conspiracy with another to violate any part of these terms and conditions.
- G) Any knowledge of a violation of these terms and conditions must immediately be reported to the employee's supervisor and the Chief Business Officer, the Executive Director of Information Technology or their designee.
- H) Computing devices shall not remain logged on to ACU's campus network when unattended, unless they are logically locked down by a standard operating system lock feature.

3.4. When Making Copies of Software is Permissible

Third party software in the possession of ACU must not be copied unless such copying is consistent with relevant license agreements and either: (a) management has previously approved of such copying, or (b) copies are being made for contingency planning purposes.

3.5. User Profile Groups

Data Stewards are responsible for maintaining security group assignments (user profiles that represent what is needed to perform a general set of related tasks.)

3.4.1. Access to Data

The appropriate Data Steward must approve all access to institutional data. By approving access, the Data Steward consents to the use of these data within the normal business functions of administrative and academic offices. Access to institutional data shall not be granted to persons unless there is documented businesses need to know.

3.4.2. Violation of Access Privileges

The Data Steward reserves the right to determine appropriate use of the data under their control. Usage violations may result in revocation of a user's access to the data.

4. SECTION FOUR – SPECIFIC POLICIES FOR INFORMATION PROFESSIONALS

4.1. Handling of Third Party Confidential and Proprietary Information

Unless specified otherwise by contract, all confidential or proprietary information, including software written by a third party, that has been entrusted to ACU by a third party must be protected as though it was ACU confidential information.

4.2. Confidentiality of ACU Computer Related Software or Documentation

All ACU generated programs, codes, and related documentation is confidential and must not be taken elsewhere when an employee, consultant, or contractor leaves the employ of ACU.

4.3. Removal of Sensitive Information From ACU Premises

Confidential ACU information, no matter what form it happens to take, must not be shared with those outside of ACU, or removed from ACU premises, unless there has been prior approval from the Data Steward.

4.4. Copyright Notices on Computer Programs and Documentation

All computer programs and owned by ACU must include appropriate copyright notices.

5. SECTION FIVE – META POLICY

5.1 Policy Revision and Review

5.1.1 Additions and Deletions

Suggested information policy additions, deletions, or alterations must be submitted to the Chief Business Officer, the Executive Director of Information Technology or their designee.

5.1.2 Policy Review Committee

A policy review committee will be comprised of the Chief Business Officer, the Executive Director of Information Technology, the Provost, the Director of Human Resources and the University Counsel. Any member of this committee may

request additional review by others, but policy acceptance will occur when each of the members comprising this committee have signed in approval. Policy specifically designated for Information Professionals, will be at the approved by the Chief Business Officer and the Executive Director of Information Technology.

5.1.3 Policy File

A file will be kept by the Chief Business Officer maintaining this policy and the approval documents for this policy for at least ten years.

5.1.4 Policy Communication

ACU Information Policy will be available on a web site

5.1.5 Policy Summaries

Condensed versions of this policy or user-specific synopses of these policies may be distributed as needed to adequately implement the policies. Condensed versions or synopses must include information about how to obtain the complete policy or policies.

V. COMPLIANCE

All users of ACU information and technology resources are required to comply with this policy. ACU reserves the right to deny, limit, restrict, or extend privileges and access to its information and technology resources.

VI. MISCELLANEOUS

ACU, through an appropriate review and amendment process, reserves the right to amend this policy at any time and without prior notice in order to provide better information and technology access to users.