Appendix H
Computer and Technology Usage Policy

I. PURPOSE

This policy is designed to perpetuate Southwestern Christian University's academic, research, and service mission by defining the appropriate and responsible use of the information and technology resources at Southwestern Christian University. 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 of its users.

II. SCOPE

This policy applies to all faculty, staff, students, contractors, and/or any other individual using information and technology at Southwestern Christian University. Access to Southwestern Christian University-owned hardware, software, and any 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 Southwestern Christian University 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 Southwestern Christian University 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 including all input, output, processing, storage, software, and communication facilities that are connected or related to an electronic system or communication network.

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

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

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

Computer Resources - Any and all computerized institutional data, computer hardware, and computer software owned by or operated at Southwestern Christian University.

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

Computer Supplies - Magnetic tape, tape cartridges, diskettes, floppy diskettes, compact discs, and computer output, including paper, magnetic, optical, or other media.

Computer 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, magnetic storage media, compact discs, and data as stored in the memory of Southwestern Christian University computers. All data is property.
Data Steward - Individual responsible for accuracy and institutional responsibility for specific data (e.g. personnel and payroll data or data concerning student records).
Institutional Policy - A succinct and cogent written document bearing the approval of the President's Cabinet of the university that clearly defines Southwestern Christian University 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 Southwestern Christian University.
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 person/s authorized to access and use the information technology resources at Southwestern Christian University.
User Account - Any logical access on any Southwestern Christian University computer system that has been specifically established for a particular user. A user account may have a dedicated logical area on one or more Southwestern Christian University computer systems also associated with it.

IV. PROCEDURE (OR PROCESS)

1.1 Access & Privileges

1.1.1 User Accounts

Southwestern Christian University faculty, staff, students, contractors, or any other individual/s using information and technology at Southwestern Christian University are provided access as outlined in Southwestern Christian University's Account Management Policy to various information systems and technology based upon their individual role and need. These accounts may include, but are not limited to: individual computers or workstation accounts, personal network file-space accounts, directory services accounts (i.e. AD, LDAP, and SSO), applications accounts (i.e. email, ERP, LMS, CMS, CRM, etc.) and others. Access to these accounts is a privilege, not a right, and may be revoked for any reason, including non-compliance with Southwestern Christian University's Account Management Policy.

1.1.2 Southwestern Christian University ID

Users are responsible for all activity performed with their Southwestern Christian University ID. Southwestern Christian University 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 Southwestern Christian University IDs. Similarly, users are forbidden to perform any activity with Southwestern Christian University IDs belonging to other users. Any suspected unauthorized access of a user

account should be reported immediately to the Chief Information Officer, the Executive Director of Information Technology, or their designee.

1.1.3 Passwords
Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms as long as doing so does not violate any 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 an individual'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 Computers
Southwestern Christian University 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.

1.2 Acceptable Use
1.2.1 Acceptable Uses of Information and Technology Resources
All information and technology resources at Southwestern Christian University are provided to assist faculty, staff, students, contractors, and/or any other individual 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 congruent with the mission of Southwestern Christian University must not be created, stored, transmitted, viewed, or manipulated using Southwestern Christian University-owned technology or information systems.
The following is a list that includes, but is not limited to, unacceptable uses of information and technology resources at Southwestern Christian University.

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:

- Text images intended to harass, terrify, intimidate, threaten, or offend another person

- Contact of another person with the intent to harass or bother, whether or not 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
- The disruption or damage of academic, research, administrative, or related pursuits of another
- Invading the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another

C) Transmitting, displaying, or viewing offensive content. This includes, but is not limited to:

- Sexual comments or images
- Racial slurs
- Gender specific comments or any comments that would offend someone on the basis of their age, sex, national origin, or disability
- Displaying, sending, printing, or storing sexually explicit, graphically disturbing, obscene, pornographic, fraudulent, harassing, threatening, abusive, racist, or discriminatory images, files, or messages in any campus computing facility or at any campus location

D) Disseminating or printing copyrighted materials, including computer files, articles, and software, in violation of U.S. and international copyright laws and/or trade agreements.

E) Attempting forgery of email messages

F) Physical or electronic interference with other computer system/s users

G) Any other practice or user activity that, in the opinion of management, constitutes irresponsible behavior, promotes illegal activities, results in the misuse of resources, or jeopardizes the operation of information and technology resources at Southwestern Christian University.

1.2.3 Prohibition of Commercial Use of Information Resources

Southwestern Christian University users must not use Southwestern Christian University information and technology resources for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by Southwestern Christian University administrators. 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

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

1.3.3 Privacy Expectations and Information Stored on Southwestern Christian University Systems
At any time and without prior notice, Southwestern Christian University reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on Southwestern Christian University information and technology resources. Similarly, at any time and without prior notice, Southwestern Christian University reserves the right to examine or monitor any device attached, for any reason, to the Southwestern Christian University 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 Southwestern Christian University's systems. It is also possible that other individuals, organizations, and agencies, with permission from Southwestern Christian University administrators, may likewise access or monitor these same systems whenever there is a legitimate business need of Southwestern Christian University for them to do so.

1.3.4 Disclaimer of Responsibility for Damage to Data and Programs
Southwestern Christian University 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, Southwestern Christian University maintains the authority to

- Restrict or revoke any user's privileges.
- Inspect, copy, remove, or otherwise alter any data, program, or other resource that may undermine these objectives.
- 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. Southwestern Christian University 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 - Copyright Laws
Unless placed in public domain by its owner(s), Section 117 of the 1976 Copyright Act protects software programs. Software is also protected by the license agreement between the owner and

purchaser. It is illegal to duplicate, copy, or distribute software or its documentation without the permission of the copyright owner.

1.4.2 - Software

Respect for the intellectual work and property of others has traditionally been essential to the mission of academic institutions. As members of the academic community, Southwestern Christian University values the free exchange of ideas. Just as Southwestern Christian University does not tolerate plagiarism, Southwestern Christian University strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If internet users or other system users make unauthorized copies of software, the users are doing so on their own behalf since all such copying is strictly forbidden by Southwestern Christian University.

1.4.3 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.

1.5 Discipline for the Misuse of University Technology

1.5 All technology used on campus is the sole property of SCU. Anyone who accesses any of the following without permission, servers, websites, emails, and computers, will be subject to being disciplined by the University Disciplinary Committee and could be expelled.