X. TECHNOLOGY

Electronic Communications and Security Policy

All uses of your computer system must conform to this policy. Violations of this policy will result in disciplinary action up to and including termination. The computer system is the property of Simpson College and is for authorized users only. It is intended to be used for employer-related business. Users are only allowed to access data which they have been specifically authorized to access by management that pertains to their specific job function. Individuals using this system are subject to having their activities on the system monitored and recorded or examined by authorized personnel, including law enforcement personnel. By accessing this network, you agree the College may download, print, inspect, monitor, copy or disclose any e-mail, electronic communication or other data contained in this system at any time without further notice.

Statement of Principles. Simpson College provides information technology resources to a large number of users, both students and employees. As members of the campus community, all users have the responsibility to use those services in an effective, efficient, ethical, and legal manner. While freedom of expression is recognized, users of institutional computer accounts are reminded that certain categories of speech - defamation, obscenity, and incitement to violence - are not protected by the Constitution. Users are encouraged to respect the privacy of others, and are prohibited from engaging in harassment on the basis of race, color, national origin, religion, sex, gender identity, sexual orientation, age, disability, and all other characteristics protected by law or otherwise covered under the College's anti-discrimination and anti-harassment policies. Simpson College reserves the right to monitor the use of technology-related resources for the purpose of determining compliance with this policy.

Computer Systems and Software

All employees, except adjunct faculty, are issued College-owned laptop computers for their work. Installation of software must be performed or approved by the College's systems administrator and approved in advance by an employee's supervisor. The installation, modification, or relocation of computer hardware or other electronic equipment must again take place only with the approval of the systems administrator or applicable supervisor.

Only approved software which is licensed to the College may be used on College-owned computers. All terms of the software license agreements shall be adhered to by employees, including, but not limited to, copy, transfer, and use restrictions. Approved public domain or College-provided software must be used in accordance with the restrictions and requirements for each software package. To prevent computer viruses from being transmitted through the system, software or other applications may not be downloaded from the Internet without advance approval. All downloads must be scanned for viruses.

Any information stored on, created on or transmitted by a College-owned computer or using College technology or systems is considered the property of Simpson College. Employees have no legitimate expectation of privacy in regard to system usage, and all communications and use of

College systems, hardware, and software are subject to review, interception, and monitoring in the ordinary course of business. The College may use, review, or monitor any information created with, saved in, sent by, or received from a College-owned computer at any time, or transmitted through a College system with or without notice to employees.

The following policies are aimed to protect the integrity of Simpson College's data and ensure it remains safe and secure under College control.

- All College-owned laptops must have a pin or password protection, per rules established by the Information Technology Department.
- Your laptop must be set to lock no later than 10 minutes or less of inactivity or leaving the app, requiring reentry of the password.
- The password must conform to the rules established by the IT Department.
- Your device will be wiped if:
    - You lose your device;
    - IT detects a data or policy breach or virus; or
    - In the event IT detects a policy breach or virus, the College will notify you prior to wiping your device to allow you to retain personal information.
- Upon termination of employment with the College, voluntary or involuntary, your device(s) must be returned to IT. Should you refuse, your laptop will be remotely wiped, which will result in loss of any personal information and a reset to factory defaults.

E-mail System

The e-mail system is provided to facilitate business-related communication both internally and with our employees, students and their families, alumni, benefactors, and the greater Simpson community. The e-mail system should be used primarily for College business as it relates to the duties of your position. Information on the e-mail and computer system is considered proprietary and belongs to Simpson College. E-mail users should understand that information transmitted over the Internet may not be greatly protected and highly confidential and sensitive material should not be sent via the e-mail system and should be sent by encrypted email or communicated directly to the applicable parties by other means. While the College recognizes that in limited, unusual and unique situations, primarily of an emergency nature, employees may need to use the College's email system for a personal reason, such occasions are to expected to be unusual and limited.

Internet Policy

Access to the Internet has been provided to staff members for the benefit of the institution and its students. The College Internet is intended for business purposes only. No illegal or inappropriate sites should be accessed at any time over the College's Internet.

Acceptable Use of the Internet. Employees accessing the Internet on a College computer or through a College computer system are representing the College. All communications should be for business reasons. You are responsible for seeing that the Internet is used in an effective, ethical and lawful manner.

Unacceptable Use of the Internet. Simpson College's Internet connection may not be used for personal gain or advancement of individual views. Use of the Internet must not disrupt the operations of the College network or the networks of other users. It must not interfere with your productivity or that of others. **Nothing in this policy shall be interpreted or applied to preclude, restrict, or interfere with employees' rights under the National Labor Relations Act.**

Sending, saving, or viewing offensive or pornographic material is prohibited. Offensive material includes, but is not limited to violence, vandalism, pornography, sexual comments, jokes or images, racial slurs, gender-specific comments, jokes or images that would offend, intimidate or threaten someone based on race, color, creed, religion, sex, sexual orientation, gender identity, age, national origin or ancestry, physical or mental disability, military veteran status, as well as any other category protected by federal, state, or local laws.

Network Security

You are responsible for any misuse of the Network by your account. Therefore, you must take steps to ensure that others do not gain unauthorized access to the Network through your account. Passwords should not be printed, stored online, or given to others.

The Network may not be used to breach the security of another user or to attempt to gain access to any other person's computer, software or data, without the knowledge and consent of such person. They also may not be used in any attempt to circumvent the user authentication or security of any host, Network, or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other Networks. Use or distribution of tools designed for compromising security, such as password guessing programs, cracking tools, packet sniffers or Network probing tools, is prohibited, unless expressly permitted in writing as part of the College's computer science and related disciplines' curricula or for use in connection with the College's cyber-security program.

Users must not disrupt the Network. The Network also must not be used to interfere with computer networking or telecommunications services to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abuse of operator privileges and attempts to "crash" a host. The transmission or dissemination of any information or software containing a virus or other harmful feature also is prohibited.

Users must not extend the Network by attaching networking devices to the Network. Networking devices include but are not limited to hubs, routers, bridges, and switches. All networking devices are to be under the authority of Information Systems and secured in the appropriate data closets. Unauthorized devices will be denied access to the Network by port deactivation and/or confiscation of the equipment.

Copyright Infringement Policy

It is the policy of Simpson College to comply with all copyright laws. No employee and/or user of the College's computer systems shall store or otherwise make unauthorized copies of copyrighted material on or using College computer systems, networks, cell phones or storage media. No College computer system user and/or employee shall download, upload, transmit, make available or otherwise distribute copyrighted material using the College's computer systems, networks, internet access or storage media without prior written authorization from an officer of the College. College employees and computer system users shall not use or operate any unlicensed peer-to-peer file transfer service using College computer systems or networks or take other actions likely to promote or lead to copyright infringement. Questions concerning whether an employee or computer user properly may copy or otherwise use copyrighted material should be raised before proceeding with the Head Librarian, who will either research the issue and/or direct the user to the appropriate College personnel.

The College reserves the right to monitor its computer systems, networks and storage media for compliance with this policy, at any time, without notice, and with or without cause, and to delete from its computer systems and storage media, or restrict access to, any seemingly unauthorized copies of copyrighted materials it may find, at any time and without notice.

College employees who violate this policy are subject to discipline, as appropriate under the circumstances, up to and including termination.

Software Usage Policy

Software piracy is both a crime and a violation of Simpson College's Software Usage Policy.

Employees are to use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except for backup and archival purposes by the software manager or designated department head) is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to Simpson College's standards of employee conduct.

To ensure compliance with software license agreements and the organization's Software Usage Policy, employees are required to follow these procedures:

All software used on organization-owned computers will be purchased through appropriate procedures.

Employees must use software in accordance with license agreements and Simpson College's Software Usage Policy. Employees acknowledge they do not own software or its related documentation. Unless expressly authorized by the software publisher, employees may not make additional copies of software, except for archival purposes.

All employees, including adjuncts using personal laptops, have access to download and install Microsoft Office via their Simpson account, to three personal devices. Other software packages

require annual licensing and will expire if not updated the following year. College-owned software cannot be taken home and loaded on an employee's home computer for personal use.

The College prohibits the use of unauthorized software or fonts. Employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment. Employees and managers should not condone the illegal copying of software under any circumstances. Employees who make, use, or otherwise acquire unauthorized software will face disciplinary action, up to and including termination.

Employees are prohibited from giving software or fonts to students, alumni, vendors, and other outsiders. Employees are not permitted to load any software without prior approval of the College's IT personnel. Under no circumstances will the College use software that has been brought into the organization from an unauthorized source, including, but not limited to, the Internet, home, friends, and colleagues. Employees should exercise caution in using files that have been created outside of Simpson College's network, including student, alumni, and vendor supplied files.

Employees who suspect or become aware of software misuse are required to notify IT Personnel, the Human Resources Director, or their department manager.

Social Media Policy

Definitions

For purposes of this policy, "online activity" includes, but is not limited to, wired or wireless communications, access to, use of, or communications stored, sent, or received over the Internet, e-mail, or any interactive online media, tool, or function (such as social or professional networking sites like Facebook or Linked In; microblogging services like Twitter; weblogs; chat rooms; listservs; and other online profiles or online forums), as well as text, photo, or data messaging. Online activity includes all such communications, access, use, storage, and messaging, whether over a fixed or mobile electronic device.

For purposes of this policy, "electronic device" includes, but is not limited to, desktop computers, laptops, landline phones, cell phones, smart phones, web-enabled handheld devices, networks, servers, technology systems, and other communications and computer equipment.

Policy

Simpson College takes no position on your decision to participate in personal online activities. To the extent you choose to engage in personal online activity, such activity must comply with these guidelines and all other Simpson College policies. In your online activity, you may not represent that you are speaking on the College's behalf unless you have been given written authority from your supervisor to engage in the activity or the activity is clearly required by your job duties and expressly authorized by Simpson College.

In your online activity, you may not use or disclose student information or the College's trade secrets, or confidential and/or proprietary information, including College marketing and

recruitment strategies, financial information, or other confidential information. **Pursuant to the National Labor Relations Act, this prohibition is not and will not be interpreted or enforced to extend to the terms and conditions of your employment.**

In your online activity, you must not engage in communications that are vulgar, obscene, threatening, intimidating, defamatory, harassing, or a violation of the College's workplace policy against illegal discrimination, harassment, or hostility because of a person's sex, race, color, religion, national origin, age, pregnancy, disability, military service, genetic information, sexual orientation, gender identity, or any other characteristic protected by applicable federal or state law.

You may not use Simpson College's logo when you are engaged or depicted in online activity that violates Simpson College's policies, is illegal, or is otherwise unrelated to communications regarding the terms and conditions of employment.

When using the College's provided electronic devices for online and other activity, you must enable and comply with the College's security procedures, including use of approved anti-virus software.

Scope

Although this policy may touch upon specific technologies used today, the policy must be interpreted broadly, as changes to and uses of such technologies have been and will continue to grow so rapidly that no policy can keep pace with individual developments.

This policy is not intended to interfere with or restrain employees' rights to engage in protected concerted activity under the National Labor Relations Act, or any other activity protected under the law, and will not be interpreted or applied to limit such protected activity.

Disciplinary Action

Violations of this policy may result in disciplinary action, up to and including termination.

Personal E-Mail Accounts

Simpson College provides most employees with an e-mail account to be utilized for business purposes only. Employees should not access their personal e-mail accounts during working time or send personal e-mail messages over Simpson College's network during work time. Similarly, employees are prohibited from conducting College business using personal e-mail accounts.

Personal Telephone Calls, Cells, Cell Phones and Text Messages

Simpson College recognizes that employees must occasionally place or receive personal phone calls and text messages while at work. However, the telephone system is intended primarily to serve the business needs of the College, and it is essential that we keep personal use from interfering with that purpose. If you have a personal call to make on either the business phone or your personal cell phone or send a text message, please do so during non-work personal times such as breaks and lunches. Employees should not be receiving personal phone calls or text messages

at work, except in emergency situations. Personal cell phones / smart phones may be carried. The College may take disciplinary action against any employee if the College finds that the employee's excessive personal calls are interfering with College work.

Employees must adhere to the state laws as it relates to cell phone usage while driving. Texting and email usage are strictly prohibited in all states. Cell phones can only be used via Bluetooth or hands-free mode while operating a College, personal or rented vehicle for College business, regardless of whether the employee is on College or personal time. The exception is in an emergency situation, an employee may use the cell phone for the purpose of dialing 911 or another number to reach an emergency service provider. However, such telephone calls must be made while the vehicle is not moving. Distracted driving may cause circumstances that put employees or others at risk.

Use of Personal Electronic Devices for Work Purposes (Bring Your Own Device Policy)

As the usage of individual mobile devices accessing employer applications and data continues to grow within the workplace, Simpson College embraces this trend with a Bring Your Own Device (BYOD) policy.

The use of personal cell/smart phones and tablets in connection with College business is a privilege granted to employees through approval of their management and is based on job function, geography, and exempt status. Simpson College reserves the right to revoke these privileges in the event users do not abide by the policies and procedures set forth below.

The following policies are aimed at protecting the integrity of Simpson College's data and ensure it remains safe and secure under College control.

- All devices must have a pin or password protection.
- Your application will lock no later than 10 minutes or less of inactivity or leaving the app, requiring reentry of the password.
- The password must be a minimum of four characters.
- Upon termination of employment with the College, voluntary or involuntary, your device(s) must be given to IT for the removal of exchange, College e-mails and contacts, and College confidential information. Should you refuse, the College may take legal action against you to recover such information.

In addition to the above security settings, all users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed.

Employee Responsibility: A personal smartphone can be connected to the College's infrastructure, but the user is personally liable for the device and carrier service costs. Users of personal smartphones are only eligible for expense reimbursement of hardware or carrier service through management approval. Users of personal smartphones must agree to all terms and conditions in this policy to be allowed to use those services.

Employees who want to purchase a personal device that will be used for work purpose and connected to the College's infrastructure are *strongly encouraged* to consult with the College's IT Department *before making the purchase* to determine whether the contemplated device can be supported by IT. Furthermore, the College reserves the right to disable or disconnect some or all services without prior notification.

Employees must notify the IT department as soon as practicable, but no later than the next business day, of a lost/stolen smartphone or tablet.

Employer Support: The IT department will provide application setup and account lock-up support on approved mobile devices. ***The BYOD policy is limited to cell phones and tablets– no personal computers are set up on the domain.***

Release of Liability and Disclaimer to Users: Simpson College hereby acknowledges that the use of a personal smartphone and/or tablet, in connection with College business, carries specific risks for which you, as the user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors that could render a device inoperable.

Furthermore, depending on the applicable data plan for phones and tablets, the software may increase applicable rates. You are responsible for confirming any impact on rates as a result of the use of College-supplied applications that you will not be reimbursed by the College, unless authorized by management. Finally, the College reserves the right, at its own discretion, to wipe data from any College-supplied application as a result of an actual or deemed violation of this Bring Your Own Device Policy, or any other related policy of the College.

Safe & Effective Performance. Notwithstanding anything else in the policy, employees may not use a mobile electronic device at times when doing so would pose a safety risk or interfere with work performance. When driving a vehicle while using a mobile device for work purposes, employees must also be aware of and obey the laws of the state in which they are driving regarding cell phone use, including but not limited to laws prohibiting text messaging while driving.

No Interference. **This policy is not intended to interfere with or restrain employees' rights to engage in protected concerted activity under the National Labor Relations Act or any other activity protected under the law, and will not be applied to interfere with such protected activity.**