SBIC TECHNOLOGY USE POLICY
2019 –2020

TECHNOLOGY PURPOSE STATEMENT

Southern Bible Institute & College believes that technology is an essential part of advancing the mission of our school. We also believe that technology can be used in our educational environment with sound ethical practices and the Bible as the cornerstone for all that SBIC undertakes even in the Digital Age. Since technology has become a pervasive and intricate part of everyday life providing a varied spectrum of modern tools for such ministry areas as outreach and biblical higher education. In addition to these modern tools -computerized records, digitalized information and instant global communication bring the need for school policies to manage our technology resources as they evolve.

SBIC provides all members of its campus learning community with technology resources focused on transforming students into competent servant leaders. This technology opens doors to opportunities for learning and utilizing up-to-date skills applicable in a highly technical world. Access to a contemporary network infrastructure has been established here at SBIC. Southern Bible Institute & College provides connections to electronic information in a variety of formats in order to assist community members with employment responsibilities, personal and professional development, and educational outcomes. While allowing our academic community access to these shared resources we must also strive to ensure that the privacy and rights of all faculty, staff and students are protected and that local, state and federal laws are obeyed. The purpose of this document is to provide basic guidelines for safe, considerate, ethical and legal use of Southern Bible Institute & College's technology resources. This document layouts school wide policies for the appropriate use of SBIC computing and network resources. Issues not specifically addressed by this document, but deemed an inappropriate use of school resources will be considered on an individual case-by-case basis.

USE OF TECHNOLOGY RESOURCES

Technological learning resources are an integral part of the educational process contributing to measurable outcomes appropriate for the school's mission statement. Faculty, Staff and Students are granted access to use Southern Bible Institute & College owned equipment and resources within the policies and procedures established in this policy document. This access is a privilege intended to benefit all SBIC students' not just particular individuals. As a result it is imperative that all SBIC computer users understand that this access also brings certain responsibilities and possible liabilities. Understanding these responsibilities and liabilities is essential to the successful utilization of available system resources.

Understanding of responsibilities is also demonstrated in the appropriate use of technology resources for example adhering to policies regarding other system users, confidential data, ownership of data and compliance with system security boundaries. Southern Bible Institute & College is not responsible for the unacceptable, unethical or illegal use of its computer systems or network resources by individuals. Students, staff and faculty desiring access to SBIC's technology resources must signed the *SBIC Technology Use Policy.* By signing this agreement individuals acknowledge that they understand and are personally responsible for following SBIC's policies and procedures for technology use. Southern Bible Institute & College reserves the right to limit, restrict, or deny computing resources for those who violate school policies, procedures, local, state or federal laws. Misuse or violation of SBIC's technology environment will be judged in accordance with those published policies and rules of conduct included in the Student Development Handbook, Faculty Handbook, Employee Handbook, and Academic Catalog. In cases of illegal activity utilizing campus technology resources SBIC will enforce its own disciplinary processes and also cooperate with appropriate authorities outside of the immediate institutional community.

CAMPUS TECHNOLOGY RESOURCES

MySouthernBible Portal

MySouthernBible Portal is an information management system that serves as the technology hub for all student, faculty, development, and education activities. The functionally of MySouthernBible Portal allows students to better plan academic choices and monitor their academic program completion progress, manage their student account, pay tuition/fees online, send/receive e-correspondence to/from faculty/staff, real-time access to available information for completing course requirements and participation in course dialog among peers delivered by synchronous technology.

Computer Lab

State of the art computers with Microsoft Office Suite, other software and internet connections are available to Southern Bible Institute & College students. The lab is open from 9am -2pm and from 4pm – 6:45pm Monday-Thursday unless a class or other activity is scheduled. Students are not allowed in the Lab when there is a scheduled class. Lab computers are provided to allow students a central location to study, research, write and print school assignments. While on campus teachers should utilize assigned devices, the faculty lounge computer or their own devices to access student information, not lab computers. While off campus faculty should only access student information from secure locations. Faculty members can schedule technical classes in the lab when needed. LCD TV's, laptops and projectors are also available to Faculty members for classroom use. These resources are scheduled and distributed on a first come first serve basis. Students are expected to behave in a professional manner in the computer lab. Noise should be keep to a minimum, silence phone ringers, step outside the lab to take calls and listen to audio with headphones. Food and drinks are not allowed in the lab. A lab printer is also available for students. Tony Myers will supply students with paper to print class related material or students can bring their own paper. Please help maintain the lab by making sure your work area is clean before you leave, using the trash can and ensuring equipment and furniture are properly arranged.

Logos Bible Software

Students can schedule a time to use Logos Bible software for study and research in the computer lab. Logos provides students access to a library of biblical information. Bible Commentaries, Bible References, Maps, Photos, Media, Language Lexicons and various Bible Translations are some of the tools available. All SBIC students taking credit courses are required to have this software package.

Internet Connection

Southern Bible Institute & College maintains access to the World Wide Web in order to expand tools available to students for study and research pertaining to school activities. Providing students with access to global, national and local information via a readily available internet connection was one of the key components in SBIC's strategic initiative to advance its technological environment. Internet access is provided to student in order to aid in their completion of assigned task and also for student's professional development. Proper use of the internet is critical to maintaining a safe networking environment for all SBIC students. Alongside policy and procedure- honesty, integrity and moral values should guide all SBIC members in the ethical use of internet. Some basic guidelines for internet use on campus are laid out in other sections of this document. Questions and concerns about internet use should be directed to the IT Manager.

AUTHORIZED AND APPROPRIATE USE

Authorized use of SBIC-owned technology resources is consistent with the education, research, and service mission of the school, and consistent with this policy.
Once this SBIC Technology Use Policy is signed by a Faculty, Staff or Student member access is granted authorizing use of SBIC technology resources. This includes lab computers, lab printers, software tools, internet connection and MySouthernBible Portal etc. Passwords required for access are not to be shared with other users. Use of technology resources at SBIC shall in no way impose added cost on the school, should not be harmful to the school, should not hinder daily operations or have adverse effects on individual's jobs or educational performance.

Authorized users are: (1) faculty, staff, and students of the school; (2) others whose access furthers the mission of the school and whose usage does not interfere with other users' access to resources. In addition, guest users must be specifically authorized to use a particular computing or network resource by the IT Manager.
Appropriate use of information technology resources includes instruction; independent study; authorized research; independent research; and official work of the offices by recognized students, campus groups and staff of Southern Bible Institute & College.
Acceptable conduct in the use of SBIC technology resources must conform to existing school policies, guidelines, and codes of conduct and other applicable laws, such as the Family Educational Rights and Privacy Acts (FERPA), SBIC's Technology Use policies and guidelines in addition to existing local, state and federal laws.

UNAUTHORIZED USE

Unauthorized use of SBIC's technology resources includes but is not limited to: Illegal activities; failure to comply with laws, violations of license agreements and policies governing network software and hardware use; abuse of shared resources; use of computing resources for unauthorized commercial purposes or personal gain; failure to protect user passwords or use of another user's account; breach of computer security, harmful access, or invasion of privacy; use of computing resources for anonymous or identity masked messages to others; or unauthorized encryption.

User may not install any software on SBIC computers without prior written approval from the IT Manager. Approval is granted at the discretion of SBIC and will not be given unless the software has been properly licensed and installation of software will not create any potential for disruption of school technology resources.

PERSONALLY OWNED TECHNOLOGY RESOURCES

Southern Bible Institute & College has no obligation to repair or replace any personal hardware or peripherals that are damaged, lost, or stolen while on campus or when using school technology resources. Therefore users bringing their personally owned technology on campus do so at their own risk.

CONFIDENTIALITY AND PRIVACY

Protecting official student, financial and other sensitive data submitted to SBIC is one of the school's highest priorities. Authorized access to official school data is one of the measures taken to ensure confidentially and privacy of electronic data. Security standards and policies are established in order to protect data such as Personally Identifiable Information, transcripts and financial records submitted to Southern Bible Institute & College. Student data is protected by the Federal Family Education Rights and Privacy Act (FERPA) and therefore not shared with other entities without student consent or unless we are legally required to do so in connection with legal proceedings, law enforcement investigations, or state law. Any known or suspected privacy breeches or unauthorized use should be reported immediately to an institutional administrator. All reports will be thoroughly investigated and appropriate actions taken regarding official school data. However, there is no expectation of privacy, confidentiality or preservation for personal documents and messages stored on school-owned equipment such as lab computers. Computers in the lab are available to all authorized users as a result personal data should not to be left on these computer. User should save their individual class work, notes and documents etc. to a personally owned storage device. Information placed or stored on a school owned or school provided computer is subject to review by the IT Manager at any time. Personal data left on lab computers is deleted on a regular basis.

Along with Faculty and Staff, Students can help safeguard their confidential information by never sharing their "MySouthernBible Portal" password with anyone. If you have problems with your password or your password may have been compromised contact Educational Support Services Coordinator immediately for assistance. Another way students can help protect their data is to ensure that they sign out of and close all programs accessed before exiting the computer lab. Failure to exit programs may result in personal information being viewed by someone else using the same computer.

SBIC CYBERSECURITY

Practical and reasonable measures are taken to safeguard pertinent digital information submitted to Southern Bible Institute & College. Students, donors, faculty and staff entrust private digital personal information to the school and as such the school has implemented policies, procedures and processes to safeguard submitted digital information. This Technology Policy provides a framework for some of the guidelines, processes and laws the school adheres to in order to protect data that is private and critical to the operation and business activities of the school. In addition day to day operations are built upon an infrastructure designed to utilize current cybersecurity features that control access, monitor connections and send notifications of issues.

Some key internal cybersecurity features of Southern Bible Institute & College include designated access levels for students, faculty and staff members. Audit and computer logs time/date stamp user logins and user transaction entries and/or changes. We have current protection against viruses, malware and spyware. Staff computers are keep up to date with the latest security patches. Staff members report unusual emails, possible computer or data compromises and out of the ordinary computer behavior. Strong passwords and or biometric devices are uses to secure staff office devices. Firewall settings, traffic logs and real time intrusion/risk detection alerts help protect against network threats. Network connections can be monitored and restricted from unauthorized users and devices. Offsite backups are set to run automatically, continuously and incrementally as changes are made to working files. This backup data is transmitted using Transport Layer Security (TLS/SSL) to offsite secure data centers. Onsite security protocols are in place to physically secure staff work areas. An uninterruptible power supply (UPS) allows for an orderly shutdown is case of a power outage. Entryways are monitored via security cameras.

TECHNOLOGY POLICY STANDARDS

You can do your part as students, faculty and staff to support the guidelines, processes and laws the school adheres to for the safety of all by understanding and following the following established standards. Use of SBIC's network and computers is predicated upon compliance with this and other school policies and all applicable laws. The following is not meant to be exhaustive, but a general guideline to help users stay within the boundaries of appropriate use and avoid inappropriate technology resource use while using SBIC's network and computers. Areas not specifically mentioned here will be addressed on a case by case basis.

1. Actively protect your "MySouthernBible Portal" information by not sharing your password with anyone; you are accountable for all actions taken with your user name

2. All confidential information must be stored on a secured device, loss or theft of such devices must be reported immediately

3. Do not attempt to access information or secure content you are not authorized to access or circumvent system policies and/or permissions

4. Attempting to circumvent or subvert any SBIC system security measures is prohibited

5. Obtain explicit written permission before viewing, copying, altering or destroying data files that belong to someone else

6. Do not represent yourself as another user electronically

7. Do not harass, threaten or bully others electronically

8. Do not create, send or participate in the forwarding of chain letters, unsolicited advertising, virus creation or propagation

9. Do not post or email extremist, obscene or inappropriate material

10. Honor and abide by copyright and trademark laws by not copying, reproducing or distributing text, photos, video, graphics, designs, music or other information formats that you did not create or do not own, copyright violations are subject to civil and criminal penalties and/or disciplinary action by the school

11. Documents created electronically must give due credit to authors and creators in order to comply with plagiarism policies and academic integrity

12. Do not use SBIC resources to make, distribute, share or use unauthorized copies of licensed software, respect the rights of other users by complying with laws, license agreements, and contracts

13. For licensing and security reasons personal software may not be installed on SBIC lab computers

14. Do not perform unauthorized testing of system or system resources, introduce viruses or intentionally attempt system crashes

15. Faculty members should utilize the faculty lounge computer or their own device to access student information

16. IT Manager maintains the computer network and lab computer, do not attempt to repair equipment yourself, if there is a problem such as an error message, a web site offer, a strange e-mail, a hardware malfunction, etc… report the issue to the IT Manager

17. Do not run software or configure software/hardware allowing unauthorized users to access the system

18. Do not attach unauthorized or remote devices to SBIC network

19. Do not uninstall SBIC software or remove hardware from SBIC computers

20. Do not download and install software from the internet, if a site automatically installs software, notify the IT Manager as soon as possible

21. SBIC's network and computers are not to be used for illegal activities, personal financial gain, gambling or commercial advertising

22. SBIC's technology is not to be used for disrupting services, damaging files, intentionally damaging or destroying equipment, software or data belonging to SBIC or other users

23. SBIC's technology in not to be used in violating any SBIC policy or any local, state or federal law.

24. When attaching personal computers and mobile devices to SBIC's network, user are responsible for making sure these devices are properly updated with security patches and current virus protection

25. Report improper use of computer resources such as breaches of computer security, unauthorized access, exposed passwords or stolen confidential information
    Policy guidelines and documentation are continually being reviewed and updated in order to stay current with technological advancements. If users have questions, concerns or doubts about the permissibility of their actions involving technology resources, these concerns should be directed to the IT Manager. Users bear the responsibility of clarifying the permissibility of their actions before they act.

CONSEQUENCES OF TECHNOLOGY POLICY STANDARDS VIOLATIONS

All faculty, staff, students and others using SBIC Technology resources are expected to be responsible for their own behavior on the computer systems provided, including the internet. We ask that all users become vigilantly aware that their actions represent and reflect upon the entire SBIC community. Actions, words, thoughts and deeds carried out using SBIC technology resources must remain within the boundaries of these policies and safeguards as we strive to equip men and women to become competent servant leaders with a bible centered world view.
Violations or misuse of SBIC's information-technology environment will be judged in accordance with these published policies and guidelines and those policies included in, but not limited to the SBIC Student Handbook and SBIC Catalog.

Consequences for technology standards policy violations vary depending on the misconduct. Particularly damaging violations such as- viewing inappropriate web sites or security violations will result in immediate restrictions. Other violations may result in a verbal or written warning.

GENERAL PROCESS FOR TECHNOLOGY POLICY VIOLATIONS

Level 1 (minor infraction(s)) - Verbal or written warning

Level 2 (repeat offense(s)) – restriction to instructor supervised computer use while on campus or suspension of all computer privileges for a specified time

Level 3 (unethical or criminal) – to be handled by Student Development Committee or legal authorities as appropriate; Disciplinary Probation, Suspension, and Dismissal or criminal charges

Pursuant to SBIC'S effort to provide a learning environment that is conducive to achieving our stated mission Southern Bible Institute & College makes technology resources available to authorized users. However there is no implied or guaranteed expectation of availability of these resources. Access to these resources is a privilege, not a right. Authorization to use these resources is granted with restrictions and responsibilities for their proper use. Southern Bible Institute & College reserves the right to restrict or deny access to its technology resources as it deems appropriate. Misuse of SBIC technology resources can result in restricted privileges, disciplinary action or criminal charges. All activities engaged in using SBIC technology resources must comply with SBIC policies, local, state and federal laws.

SOUTHERN BIBLE
INSTITUTE & COLLEGE

Acceptable Use of Information Technology Resources

Student Policy Agreement

I acknowledge that I have received a copy of the SBIC Technology Use Policy to read and am obligated to abide by this policy when using any technology resource owned, leased, or operated by Southern Bible Institute & College. Furthermore I understand that any violation of the established policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated.

If you need to review the SBIC Technology Use Policy it can be found on the school website (www.southernbible.org) under the About us\Downloads section.

_____ _____

Student Name (please print) Date

_____ _____

Student Signature Date

Student official contact email _____

(Please print)