Southwest Baptist University
Acceptable Use Policy

Information technology resources, services, and facilities of Southwest Baptist University are provided to support the mission of the University. Access to such resources increases the potential for improved instructional effectiveness and increased information availability. This Policy has been written to ensure both wise and fair decision making regarding access priorities and user behavior. Please note that computing support services are provided to faculty, staff and students, to the extent that personnel and funding are available, by the University's technology service unit(s) for all computing resources and facilities and networking resources. The Policy will be reviewed and may be revised at any time.

I. University Computing Resources

In this Policy the term "computing resource(s)" includes all computing resources available through the University for access and use by students and University personnel. The Technology Council and appropriate departmental personnel, with administrative approval, may, within budgetary limits, restrict or otherwise organize the use of any computing facility or site according to the special needs of each facility or site and the availability of resources at each facility or site.

The provisions of this Policy apply to all use of computing resources regardless of the location of those resources.

II. Wide-Area Networks and Network Resources

Training, orientation or evidence of proficiency in the use of networks and network resources may be required as a condition for access. Otherwise, all of the provisions of this Policy that pertain to computing resources and its use also apply to the use of wide-area network resources accessed through computing resources.

Access to wide-area networks and resources through computer facilities is provided primarily to address the computing and information needs associated with the educational and the scholarly activities of the University. Access depends upon availability of necessary resources and personnel.

III. Computing Resource Users

Currently enrolled students are allowed to use appropriate University computing resources as a privilege subject to: availability; current academic priorities; adherence to this and subsequent computing resource policies; and where appropriate, the payment of lab or technology fees.

University personnel have access to University computing resources where appropriate as long as they comply with the terms of this Policy.

Faculty, staff and students of SBU have priority access to SBU computing labs.

Group users, such as schools or libraries, may be allowed access to some specific computing resources on a case-by-case basis depending upon the satisfactory completion of arrangements with appropriate University personnel.

When necessary, restrictions may be placed on any user's access to ensure the proper functioning and security of the computing resources.

IV. Expectation of Privacy
The University will attempt to provide a normal level of security to user accounts. However, due to the nature of computer resources and electronic transmissions of information, all users should have no expectation of privacy in connection with the use of the University's e-mail, Internet, network or computer resources.

V. Acceptable, Unacceptable and Illegal Use
Computing resources are only provided for genuine academic and educational research activities and for other activities necessary to support the mission of the University. All users are expected to abide by all applicable laws and legislation pertaining to the use of these resources. It also is the responsibility of users to conduct their use of these resources in an ethical manner and to refrain from any activities that might adversely affect other users or the computing resources belonging to the University or accessed through the University system. Uses of computing resources that are deemed inconsistent with the mission of the University will not be allowed.

Acceptable uses of computing resources include (and may not be limited to):

- instructional use in University courses;
- faculty research and consulting;
- faculty directed student research;
- genuine scholarly activities;
- administrative support functions of the University.

Unacceptable use or abuse of the privilege of using the computing resources includes, but is not limited to:

- cheating, plagiarism or information theft;
- unauthorized, intentional copying, sending or receiving of any file, data, or computer program when the user does not have the legal right and institutional authorization to do so;
- playing games in SBU computing labs or via the dial-up resources;
  accessing, examining or attempting to examine the files, mail, or accounts of other computer users or the system management directories, files or resources without the appropriate authorization;
- sending unsolicited, annoying, harassing or obscene messages to other computer users;
- use of technology resources for outside business interests, private consulting, solicitation, or personal gain except as outlined in the University’s Intellectual Property policy;
- unauthorized altering or attempting to alter hardware or software configurations and/or system files;
- violating any rules or regulations posted in University computing resource facilities and sites; using technology resources for purposes which violate:
    - civil or criminal laws of local, state or federal jurisdictions;
    - the University’s statement of Principles and Expectations;
    - other institutional rules for that particular user (i.e., student handbook, faculty handbook, personnel handbook, etc.);
    - the mission of the University.

These uses would include, but not necessarily be limited to:

- access to pornography or gambling;
- violation of copyrights;
- counterfeiting of government documents including currency;
- access to information on the construction of explosive devices;
- creation or distribution of hate speech;
- creation of any forged document or use of a forged signature for any purpose when the reasonable inference is that the document or signature will be presented as authentic

Illegal Use:
Certain activities that are possible with computing resources are illegal. Sending threatening or harassing electronic messages is an example. The University expects all computing resources users to abide by all applicable laws. It is the responsibility of each user to know and comply with such laws. Ignorance of such laws does not affect the user's responsibility or liability. Offenses may be prosecuted and the appropriate authorities may enforce legal and/or civil penalties.

Federal law has established penalties for infringements upon copyrights, intellectual property rights, and privacy rights of individuals. The Revised Statutes of the State of Missouri have established penalties of tampering with intellectual property, tampering with computer equipment, or tampering with computer users. Penalties range from one-year (1) sentence and fine of $1,000 to a five-year (5) sentence with a $5,000 fine. Depending on the damage caused by the offense the penalties may be higher.

Computing resources users must not: make copies, use or distribute software, electronically or otherwise, unless the user can show compliance with copyright and licensing agreements; use other user's accounts or files without authorization; allow other persons to use their account under any conditions; make any fraudulent use of resources; send any illegal messages such as harassing or obscene messages; or use the resources for any other illegal activities.

VI. User Responsibility and Liability
In order to maintain the integrity and security of computing resources, the Internet and other wide-area networks, it is the responsibility of all users to make sure their use is appropriate, ethical, legal, and secure. All computing resources users are responsible for maintaining the security of their access points including passwords and login identification.

Any liability incurred through access from the user's account is the user's responsibility and not that of the University. Each user is specifically responsible for:

- the security and use of their personal account(s), login id(s) and password(s);
- all activity performed on their account(s);
- any penalties, fines, damages or liability caused by their abuse of privileges or failure to maintain the security of their password(s) or login id(s);
- all membership requirements or financial commitments made with commercial or noncommercial entities accessed through their account(s);
- refraining from use of any account(s) other than the one assigned to them;
- not allowing others to use their account(s);
- compliance with all applicable laws;
- backing up personal files;

- cooperating with requests and directives from appropriate University personnel concerning University computing resources.

VII. University Responsibility

The University seeks to enable users to make the most effective use of computing resources by providing orientation, training and support as resources are available. The University will offer training and orientation to the resources as deemed appropriate and as resources and personnel are available. It is the responsibility of the user to obtain such training, if necessary, before using these resources.

The University is responsible for periodic or emergency maintenance that may require full or partial shutdown of computing resources. Planned maintenance that takes place during open lab times should be advertised to all users via posted announcements.

Security and security systems management will be maintained by network services personnel who will monitor the use of computing resources, including individual accounts as deemed necessary to ensure the integrity and security of the resources. Even though computer users should have no expectation of privacy, University personnel will not allow outside governmental or investigative agencies unauthorized access to individual accounts or files. Generally such authorization will be in the form of a court order from a court of competent jurisdiction. However, the University's president reserves the right to authorize such access in particularly egregious circumstances.

The University is not responsible for the activities of the user or for any damage caused by or liability incurred by a user or for any financial commitments made through a user account. The University does not guarantee access, does not make any claims as to the accuracy of information accessed, or guarantee security for any information sent or accessed through the computing resources available to the user.