Computer Services Policy

Computer Accounts

Computer accounts for Southern Arkansas University users are created and assigned for the purpose of fulfilling the University mission statement. Accounts will be created for SAU full-time employees and students. In addition, limited access may be granted to individuals with special, unique, or circumstantial needs or requirements relative to the University. Any such request will be reviewed on a case-by-case basis with the user agreeing to follow University guidelines.

Users must not share accounts. User accounts and/or administrative systems are not to be used for any unethical, illegal, or criminal intent or purpose. If a problem exists with an account, please contact ITS at extension 4083.

Computer hardware, software, and application resources are the property of SAU. Therefore, any information stored on University resources is owned by and is the property of SAU and must be in compliance with local, state and federal laws and University policies. Every effort will be made to maintain privacy and security of user files. Inspection of the account content (including e-mail retrieved and restored from backup files, mailbox contents, public folder postings, files saved to local hard drives, etc.) may occur in accordance with applicable state and federal laws and University policies.

Misuse of Accounts

SAU supports the statement on software and intellectual rights adopted by EDUCOM, a consortium of several hundred colleges and universities with active interest in the educational uses of accounts and computers:

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

Users should also be aware that some types of computer abuse are not only against University policies but are also in violation of state and Federal criminal codes (unauthorized reproduction of copyrighted software, intentional damage to hardware or accounts, and unauthorized alteration or access to computer systems).

Students

SAU students finalized for the fall semester will have an account automatically created the day before classes begin. All new SAU students finalized for the spring and summer semester will also have an account automatically created the day before classes begin for the given semester. Students who finalize registration after automated creation of accounts must complete an account request form in the Magale Library. Every effort will be made to create the account within two working days of the request (receipt of a large number of requests may lengthen the time frame). Format of student account name will be first letter of first name, middle initial, last name, and four random numbers with no spaces. For example, the account for John David Student will be JDSTUDENT4321. Student accounts will remain accessible during semesters for which students are actively enrolled.
Students enrolled and finalized during the fall, spring, and summer semesters will keep their account intact during the academic year. Exceptions include students that are completing graduate papers or fulfilling the requirement of an incomplete grade.

**Electronic Messaging**

**E-Mail**

E-mail is an integral part of communications on campus. The purpose of e-mail is to electronically communicate effectively with students, employees, peers and/or other individuals within the higher education infrastructure. All correspondence from the Financial Aid office and the Students Accounts office will be sent to the student’s e-mail address. Therefore, it is imperative that each student regularly check this e-mail and review completely the information transmitted.

SAU users must adhere to the following guidelines:
1. Appropriate standard of civility must be used in electronic communications with other users.
2. Contents must not include rude, obscene or harassing contents.
3. Any potentially offensive e-mail content must not be sent or forwarded to other users.
4. Messages must not be used to intimidate, insult and/or harass other users.
5. Chain letters, mail-bombs, junk letters, classified ads, and other forms of mass electronic mailings are not permitted.
6. Electronic communications must not be used for solicitation purposes.
7. Personal for-profit use of e-mail is not permitted.

**Quotas**

E-mail quotas limiting the amount of space utilized to store e-mail messages will be assigned to all users. When a quota has been exceeded, it will result in users not being able to send e-mail messages until the quota has been met. In addition to the amount of storage allocated for e-mail messages, a quota has been assigned to the size of an e-mail message being sent from or received on campus as a security measure. Disk quotas have also been set to limit the amount of data storage that students can use on the SAU file storage server. An e-mail message will be sent to the user’s SAU e-mail address when the user exceeds this disk quota and the user will not be able to save any more data files until the user deletes the amount of stored data to within the quota limit.

**Violations**

Violations of these policies and procedures are subject to disciplinary actions.

**Pornographic/Obscene Material**

Pornographic/obscene material is prohibited on computer equipment in the SAU Computer Commons. Material of this nature may be accessed only when the material is to be used for academic research that has been approved by the dean of the appropriate school. No research of this nature will be allowed in the Computer Commons or computer classrooms. Research must be done from an alternate site on campus.

Any pornographic/obscene material that is received on the SAU campus should be forwarded to the Director of Information Technology Services for further investigation and reporting to the appropriate senior administrator.
Student Computer Commons (located on 2\textsuperscript{nd} & 3\textsuperscript{rd} floors of Magale Library) and Classroom Policies

Introduction

The University operates and maintains an information network to allow students, faculty and staff to complete assignments and work in pursuit of the University mission. Each student will receive an account and password, which allows student access to the appropriate computing resources to complete academic goals. The university supports the intellectual property right of information regardless of storage media utilized by the student.

The University abides by all state and federal laws applicable to copyright issues. Licensed software is not to be copied or duplicated. Any violation of the intellectual rights of published or unpublished authors, students, faculty, or staff of SAU is a serious offense and will be treated accordingly. Students should utilize appropriate standards of civility when using computing systems to communicate with other individuals.

University Responsibility to Student

SAU provides all currently enrolled students with information technology equipment in support of educational and instructional purposes. A quiet serene atmosphere with student assistance, if needed, can be found in our computer facilities.

Computing facilities are made available to the students, faculty and staff of the University. Only properly authorized persons may access SAU computing facilities. Proper authorization is provided to students in the form of a computer account and password. Assigned accounts are to be used only by the user to which the account has been created. Users should not share their accounts and password information with other users.

Student Responsibilities

It is the responsibility of each student to adhere to all ITS student computer policies while in computer facilities as follows:

General

1. Technology resources are to be used only in the pursuit of academic or other University purposes.
2. Food and drink should be consumed outside computer classrooms
3. Printers are to be used for hard copy of instructional assignments. Copiers should be utilized in making multiple copies of printed materials.
4. Pick up after yourself. Keep workspace clean since there will be others using the same equipment later.
5. Be sensitive to the needs of others.
6. Respect the privacy and personal rights of others. Do not access or copy another user’s electronic mail, data programs or other files.
7. The University’s is the owner of computing resources in computer classrooms.
8. Electronic communication used for fraudulent, harassing or obscene messages is prohibited.
9. Students should respect system integrity and resources by not developing or executing programs that could harass other users, degrade performance or damage software or hardware components.
10. Chain letters and other forms of mass mailings are prohibited

Access

1. Students are responsible for any and all activity initiated in or on SAU computing facilities by their computer account.
2. Students are responsible for selecting secure passwords for their computer accounts and for keeping those passwords secret at all times. Passwords should not be given to other users.
3. Students are responsible for their data files and creating appropriate backup files.
4. Students should report any system security violation, or suspected system security violation to any of the lab assistants and/or lab coordinator.
5. University licensed software should not be copied or reproduced in any capacity.
6. Students are responsible for obeying all official notices posted in computer labs, attached to SAU equipment, and posted via e-mail or login entry screens.

**Hardware/Software**

1. Report hardware, software and printer problems to the student workers on duty.
2. Student should log out of their account when finished with University computing resources.
3. Students are not to access restricted portions of the operating system, security software or accounting software unless authorized by the appropriate university administrator.

**Web Pages**

**General Guidelines**

The following guidelines apply to all electronic document publications, whether on the Internet or the Intranet. Electronic publications should follow the same University policies and standards as print publications.

Applicable issues include nondiscrimination, academic freedom, proper use of computer resources, copyright laws, and authorized use of the University’s logo and other graphic elements.

In any form of publishing, nothing must be published which might bring SAU into disrepute.
- Publications must be legal, decent, and accurate.
- Publications should be consistent with the standard and style of SAU’s official publications.
- Where they might influence the public perception or image of SAU, the publications’ tone should be positive.
- Personal opinions must not be published in a way that might make them seem to be the University’s views.
- Publications that may be regarded as publicity for potential students must be approved in the Communications Center.
- Publication should not compromise SAU’s symbols, seal, logo, and name.
- Publishers will be held personally responsible for any cost or other legal liability that they incur as a result of publishing, unless the University has previously agreed in writing to exonerate them.

If you have any doubt about the suitability of material to be published, contact the director of the Communications Center at extension 5011.

**Personal Web Pages – Students, Faculty, or Staff**

Personal web pages may not contain the University or campus logos or other symbols of the University or the campus.

Copyright laws apply to electronic publishing as well as to print publishing. Be sure to have permission to publish the information, graphics, or photographs on pages if you are not the author or creator. Photographs of an individual or personal information about an individual must not be included without the written permission of the individual.

Students’ web pages will be deleted at the end of the spring semester.

University Web servers must be used for educational purposes and cannot be used for profit or commercial purposes.

**Usage of the University Logo**

The Southern Arkansas University logo is a registered trademark of the University. Its usage is limited to official University entities, including Schools, programs, departments, offices, centers or student Organizations recognized by the Office of Student Life. Call the Communications Center at (870) 235-4026 for a copy of the University Logo—do not copy the logo located on the University’s web page.

- Do not hang the logo off the page.
- Avoid using the logo against graphic backgrounds that are busy and make the logo compete for visibility.
- Do not alter, stretch, or redraw the logo in any way. The logo must be placed right side up and never at an angle. Be sure the word “Magnolia” is legible.
- Non-official web pages should NOT use the University logo.
- Do NOT use the University seal.
Consequences of Misuse
An enforcement policy will be followed that allows for immediate action in extreme cases or when requested by external sources. Minor infringements, particularly in terms of design or technical issues, will be dealt with by a request to the author to withdraw or modify offending material. The University retains the right to withdraw any material that breaks existing law or University regulations. Serious infringements will be considered a disciplinary matter.

Policy/Procedure
The following student actions are prohibited. Students will be held accountable for any such actions and will be subject to student discipline procedures through the Office of Vice President of Student Affairs.
1. Negligently degrading, intentionally degrading or attempting to degrade the performance of any University system or any system available through the Internet.
2. Penetrating or attempting to penetrate the security of the University system or any system available through the Internet.
3. Depriving or attempting to deprive other students of resources or access to computer resources.
4. Using any computer system or network to send unsolicited, offensive, abusive, obscene or otherwise harassing communications.
5. Using a computer account belonging to another individual without the explicit permission of that individual and the Director of Information Technology Services (students are responsible for all activity originating from their accounts as well as for their safeguard and use).
6. Negligently, or intentionally and without authorization, accessing, altering, interfering with the operation of, damaging or destroying all or part of any computer, computer system, computer network, computer software, computer program or computer database.
7. Failing to protect any password or other confidential information about a computer, computer system, computer network or computer databases.
8. Inspecting, modifying or copying programs, data, or electronic mail without authorization.
9. Placing any information in the University's computer system(s), computer network, or any system available through the Internet, which is not in keeping with the educational purposes of the University, such purposes being determined solely by the University.
10. Specifying false or misleading information when being investigated for computer misuse under this policy.