

# University of South Alabama Computer Use Policy

---

- I. **Purpose of This Policy**
  - General Policy for Faculty/Staff
  - General Policy for Students
  
- II. **USA Faculty/Staff Computer Use Policy**
  - User Privileges and Responsibilities
  - Authorization
  - IDs/Passwords
    - Administrative Devices
  - E-mail
    - Personal Communication
    - No SPAM
    - Viruses
    - Confidentiality and Security
    - No 'Hacking' or 'Cracking'
  - Internet
  - Web Pages
  - Software Licensing (copyright laws)
  - Violations/Consequences
  
- III. **USA Student Computer Use Policy**
  - Illegal Activity
  - Strictly Prohibited Behaviors/Activities
  - Considerate Use
  - Violations/Consequences
  - Additional Guidelines for Students in Medical Fields
    - Sexually Explicit Material
    - Appropriate Activity
    - Confidentiality
    - Reliability of Information
  
- IV. **Alabama Research and Education Network Acceptable Use Policy**
  
- V. **USA Software Policy**
  
- VI. **Summary**

# University of South Alabama

## Computer Use Policy

### **Purpose of this Policy**

- To educate users about their responsibilities regarding acceptable use of University computers/networks
- To describe and prohibit unacceptable use of University computers/networks

### **General Policy for Faculty/Staff**

The University of South Alabama, through its Computer Services Center (CSC), provides an academic network and multi-user Unix systems to be used by faculty, staff and students for instructional and research activities. The CSC also houses the center of the University networks, including the main campus fiber networks and the wide-area links to the USA Hospitals. Anyone using the campus network, mainframe systems or computer equipment owned by the University must be authorized to do so, and must adhere to all guidelines stated in the **USA Faculty/Staff Computer Use Policy**.

The CSC also complies with the **Alabama Research and Education Network (AREN) Acceptable Use Policy**. The University's gateway to AREN (formerly the Alabama Supercomputer Network) and the Internet is located at the CSC. All users of University network facilities are obligated to adhere to the terms of this policy.

All University employees are required to adhere to the policies listed throughout this document. However, these policies do not preclude individual departments from making more specific guidelines for their employees based on the nature of their work.

### **General Policy for Students**

USA provides student access to computer resources through its departmental labs located throughout campus. Students using these labs must adhere to all University policies regarding the use of computers and computer networks, including the **USA Student Computer Use Policy** and the **Alabama Research and Education Network (AREN) Acceptable Use Policy**. (Guidelines specific to students in medical fields are included in the **USA Student Computer Use Policy**.)

Lab privileges can be denied to anyone using this equipment for illegal or unethical purposes. Any illegal behavior observed in the labs may be reported to appropriate University officials or law enforcement agencies. All students are required to adhere to the policies pertaining to them throughout this document. However, these policies do not preclude individual departments from making more specific guidelines for their students or facilities.

## **USA Faculty/Staff Computer Use Policy**

## User Privileges and Responsibilities

**Authorization.** In general, USA colleges and departments are responsible for the allocation of computer resources for their faculty and staff. **No one should use any University computer or network facility without authorization from the appropriate personnel in that office or department.** University computers and networks are to be used for University purposes, i.e., to further the educational programs of the University. Any attempt to disrupt, degrade or improperly gain access to University computer resources is prohibited. Unauthorized wiring, altering or damaging of University-owned computer equipment, including network hardware and software, is also prohibited.

**IDs/Passwords.** No one should give a computer password to an unauthorized person, nor obtain another person's password by any unauthorized means. Deliberately and inappropriately observing, recording, accessing, using or transmitting passwords, account numbers, e-mail addresses, phone numbers or credit card numbers belonging to other people is strictly prohibited.

**Administrative Devices.** An "administrative device" refers to a terminal or microcomputer used to access administrative computer systems (e.g., Master Student File, Payroll, Financial Aid systems, etc.). Access to administrative devices is limited to individuals engaging in official University business. All persons given unique passwords and sign-ons are required to sign a Statement of Accountability, which states that this information is not to be shared with any other individual. Knowledge of sign-on codes, file access codes, and input transaction codes is also restricted to individuals engaged in official University business. (Authorized personnel should see **Information Systems Security Policy** for further details concerning use and misuse of administrative devices.)

**Email.** The University email systems are to be used for University business only – not personal business or personal gain. Users have full responsibility for all messages they transmit through the University's computers, networks and systems. Consequently, all laws and rules against fraud, harassment, obscenity, etc., which govern all University communications also apply to email. Abuse of the email system may be grounds for disciplinary action, up to and including termination.

**Personal Communication.** As with the office telephone, it may be necessary at times for email to be used for personal communication. Care should be taken not to impede the business operations of the University with personal email. Excessive personal use would constitute abuse of the system and would be grounds for disciplinary action.

**No Spam.** "Spam," the practice of mass-broadcasting unsolicited email (e.g., commercial advertisements, chain mail, pornographic materials, political lobbying, hate speech, racial diatribes, and religious proselytizing), **is strictly prohibited at USA.**

**Viruses.** Users should exercise caution when downloading executable programs via email, as they might interject computer viruses into University computers and/or networks. It is illegal to knowingly replicate or transmit computer viruses, or otherwise deliberately damage the systems or files of other people.

**Confidentiality and Security.** No one without specific authorization may read, alter, or

delete any other person's computer files or email, even if the equipment and software have that capability. **No email system is completely secure.** Consequently, email should not be used to transmit computer passwords, credit card numbers, or other confidential information about students or employees. Routine maintenance of the email systems may require or inadvertently lead to viewing some pieces. The CSC will respect the privacy of such mail, and will not reveal its contents to any other parties. However, if activities in violation of law or University regulations are discovered through this procedure, the CSC may report such information to the appropriate authorities. Departments are advised that information subject to confidentiality regulations should not be transmitted via these electronic media without prior written approval from the appropriate administrative offices.

**No "Hacking" or "Cracking".** Deliberately invading the privacy of others by attempting to gain unauthorized access to any account or system is strictly prohibited.

**Internet.** All computer accounts provided to faculty/staff are intended for the University's work. Many University departments do encourage their employees to use the Internet to educate themselves, *provided* time and equipment are available. As a University employee, you are accountable for how you use your time on the job. In consideration of other network users, employees should limit bandwidth-intensive activities (e.g., playing or downloading network-based games, music or video) to those that are required as part of their employment. University employees are prohibited from using University equipment for private money-making enterprises. Due to the real danger of transmitting computer viruses, extreme care should be taken in downloading executable files from the Internet onto University computers. It is unacceptable to use University equipment or networks to view, download, post, print or send pornography, or other sexually explicit, profane, obscene, hostile, or blatantly offensive and intimidating material, including hate speech, threats, harassing communications (as defined by law), or information that violates any state or federal laws. Using University equipment/networks for the sale of weapons, drugs or illegal substances is strictly prohibited.

**Web Pages.** All web pages running on University-owned servers must adhere to USA's Web Policies, which can be viewed in their entirety from the USA Web Services web site ([www.southalabama.edu/webservices](http://www.southalabama.edu/webservices)). These policies govern the management of those electronic documents that represent USA and are accessible on the Internet. Individual University departments are responsible for the accuracy and integrity of the contents of their web pages, and have full responsibility for what they publish. The Web Services office periodically reviews USA web sites and links to ensure that the University is being represented appropriately and that all official symbols are being used correctly. Any objectionable content found in USA web sites or links will be subject to laws and rules against fraud, harassment, obscenity, etc.

**Software Licensing (copyright laws).** All faculty/staff should be aware that uploading or downloading copyrighted material, violating the intellectual property rights of others, or illegally sharing trade secrets is strictly prohibited at USA. All reproduction and use of

computer software on University equipment or by University employees or students in pursuit of University business or instruction must be in accordance with copyright law (as set forth in Title 17, United States Code) and the manufacturer's condition of sale. (See the **USA Software Policy**, printed in its entirety at the end of this document.)

## **Violations/Consequences**

In addition to all guidelines in the policies stated here, all USA employees are subject to the policies and disciplinary procedures outlined in the **Staff Employee Handbook** and the **Faculty Handbook**. Violations of any USA computer policies incur the same types of disciplinary measures as other University policies or state or federal laws (up to and including criminal prosecution).

## USA Student Computer Use Policy

USA provides student access to computer resources through the email systems, Jaguar1 systems, web servers, and departmental labs located throughout campus. Students using these resources must adhere to all policies of the University of South Alabama, as well as the Alabama Research and Education Network, regarding the use of computers and computer networks.

Lab privileges can be denied to anyone using University equipment for illegal or unethical purposes. Any illegal behavior observed in the labs will be reported to appropriate University officials or law enforcement agencies. Anyone using the lab computers in this way, or any other generally inconsiderate manner, will be subject to appropriate disciplinary action. Such behaviors/activities include, but are not necessarily limited to, the following:

### Illegal Activity

- **Uploading or downloading copyrighted material**, violating the intellectual property rights of others, or illegally sharing trade secrets. (Please note that MP3 and other music files frequently fall into this category.) Accessing, downloading, or printing out articles solely for educational and research purposes, however, may be permissible under the fair use clause of the Copyright Law. See USA Software Policy for more specific guidelines on using copyrighted software.
- **Illegally sharing computer software** via Internet, the local network, personal disks or any other media
- **Copying or transmitting material contained in copyrighted databases** such as Infotrac, without permission from the source.
- **Buying or selling weapons or illegal substances** via computer network.
- **Threatening or “stalking”** others via computer network.
- **Knowingly replicating or transmitting computer viruses**, or otherwise deliberately damaging the systems or files of other people.

### Strictly Prohibited Behaviors/Activities

- **Trafficking in pornography** of any kind via computer network. Please note that *redistribution* of pornography, even through web page links, is often illegal.
- **Activity that violates state or federal law.** This may include viewing, downloading, posting, printing or sending pornography, or other sexually explicit, profane, obscene, hostile, or blatantly offensive and intimidating material, including hate speech, threats, harassing communications (as defined by law), or information that violates any state or federal laws.
- **“Spam,”** the practice of indiscriminately sending unsolicited email (e.g., commercial advertisements, chain mail, pornographic materials, political lobbying, hate speech, racial diatribes, and religious proselytizing) to persons who have not indicated interest in receiving such materials.
- **“Hacking” or “Cracking”**, i.e., deliberately invading the privacy of others by attempting to gain unauthorized access to any account or system.
- **Obtaining/distributing confidential information.** Deliberately and inappropriately

- observing, recording, accessing, using or transmitting passwords, account numbers, e-mail addresses, phone numbers or credit card numbers belonging to other people is prohibited.
- **Downloading executable programs**, which might interject computer viruses into lab computers, is generally prohibited. Further guidance with regard to safe sites and appropriate downloads should be sought from the lab facilitator. (The University takes no responsibility for damage to your work or your own equipment resulting from viruses or files you might download via the Internet.)
  - **Using University equipment, including the University's Internet lines, servers or web pages, for commercial gain.**
  - **Unauthorized wiring, altering or damaging of University-owned computer equipment**, including hardware and software.
  - **Tampering** with lab machine settings.

### Considerate Use

- **"Surfing the Net"** on lab machines for academic enrichment is permitted; however, precedence is always given to students needing access for assigned course work. Classes in the lab with a faculty member also have precedence. Otherwise, lab access is allocated on a first-come basis. Individuals who have been on a computer for more than two hours should yield if others are waiting.
- In consideration of other network users, students should **limit bandwidth-intensive activities** (e.g., playing or downloading games, music, video) to those required by their curriculum.

### Violations/Consequences

In addition to all guidelines in the policies stated here, all USA students are subject to the rules outlined in the **Code of Student Conduct** and the **Student Academic Conduct Policy**, which are both published in *The Lowdown*. Violations of any USA computer policies incur the same types of disciplinary measures as other University policies or state or federal laws (up to and including criminal prosecution).

### Additional Guidelines for Students

**Sexually Explicit Material.** All students are expected to effectively discriminate between professional and unprofessional portrayals of nudity and sexuality. This is an important aspect of professional judgment in many fields of study. Dealing with nudity, the examination of the human body and the full range of human sexuality are relevant and appropriate to those in medical and other professions. A number of Internet sites (e.g., The National Library of Medicine and NIH) portray some such materials. Individuals working in medical school and nursing labs should expect to occasionally encounter nudity and professional portrayals of sexually explicit material.

**Appropriate Activity.** While the full range of free speech is supported and encouraged, USA students should always be mindful of the fact that the computer labs are located in public areas. Materials on screens visible to others working in the lab, materials that are deliberately or inadvertently left behind on the hard drive, and materials posted to the Internet from this lab should reflect well on the professionalism of our programs. Imposing exposure to inappropriate sexual materials upon student or faculty colleagues working nearby (or using the lab at a later time) might be construed as sexual harassment. Those in doubt about appropriate activity should seek faculty advice.

**Confidentiality.** Confidentiality is another issue affecting students using the labs. Under no circumstances should students leave, post or transmit confidential material such as research data, case reports or private notes about patients (or case studies) on these computers. The University takes no responsibility for student work left on lab machines, even if the lab facilitator gave permission for it to be on the machine. Any such work may, at any time, be erased accidentally or in routine clean-up activities. Students should not leave private work or communications on these computers, nor should they read any private information accidentally left by others. No material should be left on these computers without permission from the lab facilitator.

**Reliability of Information.** Students should remember that material on the Internet may or may not be accurate and reliable. It is critical that any information found on the Internet is carefully evaluated, especially with regard to pharmacology and health information.

# **Alabama Research and Education Network Acceptable Use Policy**

The Alabama Research and Educational Network (AREN) and the CSC comply with the following Acceptable Use Policy. **All users of University network facilities are obligated to adhere to its terms.**

## **A. OVERVIEW**

The Alabama Research and Education Network (AREN) is a statewide network administered by the Alabama Supercomputer Authority (ASA). The purpose of this policy is to provide a definition for acceptable use by authorized users of AREN and to indicate recommended action if the policy is violated.

In those cases when information is transmitted across regional networks or Internet, AREN users are advised that acceptable use policies of those networks apply and may limit access.

## **B. ASA PRIMARY GOALS**

The Alabama Supercomputer Authority has been established to:

- \* enhance university research in Alabama;
- \* attract and support high technology industry;
- \* expand knowledge and use of computational science.

## **C. AREN ACCEPTABLE USE POLICY**

- \* All use of AREN must be consistent with ASA's primary goals.
- \* AREN is for the use of individuals legitimately affiliated with member organizations, to facilitate the exchange of information consistent with the academic, educational and research purposes of its member organizations.
- \* It is not acceptable to use AREN for illegal purposes.
- \* It is not acceptable to use AREN to transmit threatening, obscene, or harassing materials.
- \* Access to INTERNET is provided through an ASA statewide contract with a regional network provider. The contract allows ASA to grant access to INTERNET to any governmental, educational and industrial entity through AREN. Charges may be assessed by ASA to facilitate network connectivity. Reselling of the INTERNET connectivity and services is prohibited.
- \* It is not acceptable to use AREN to interfere with or disrupt network users, services or equipment. Disruptions include, but are not limited to, disruption by unsolicited advertising, propagation of computer worms or viruses, and using the network to make unauthorized entry to any other machine accessible via the network.

- \* Information and resources accessible through AREN are private to the individuals and organizations which own or hold rights to those resources and information unless specifically stated otherwise by the owners or holders of rights. It is therefore not acceptable for an individual to use AREN to access information or resources unless permission is granted by the owners or holders of rights to those resources or information.

#### **D. VIOLATION OF POLICY**

All organizations authorized to access AREN are responsible for informing their users of this acceptable use policy. All users of AREN are required to follow the acceptable use guidelines, both in letter and spirit.

ASA reserves the right to monitor and review all traffic on AREN for potential violations of this policy. Violations of policy that are not promptly remedied by individuals and member institutions may result in termination of access to AREN.

Final authority for the determination of violation of the AREN Acceptable Use Policy and subsequent penalty rests with the ASA Board of Directors. It is the responsibility of member representatives to contact ASA, in writing, regarding questions of interpretation. Until such issues are resolved, questionable use should be considered "not acceptable".

# USA Software Policy

*The following software policy was developed by a faculty committee and has been approved by the University Deans and President as a University policy.*

The reproduction and use of computer software on University equipment or by University employees or students in pursuit of University business or instruction shall be in accordance with copyright law (as set forth in Title 17, United States Code) and the manufacturer's condition of sale. Specifically:

1. No University employee or student shall reproduce or allow the reproduction of software in violation of copyright law or the conditions of sale.
2. No University employee or student shall accept or use software which is not known to be provided in accordance with copyright law or conditions of sale.
3. It is the individual responsibility of each user to determine that the use of software is in accord with this policy.

## Practices and Guidelines for the Software Policy

The policy stated above applies to:

1. The use of copyrighted or licensed software by University departments and employees on University equipment.
2. The use of software purchased with University funds on non-University equipment.
3. The use of software for instructional purposes.

The University interprets the copyright laws and manufacturers' terms of sale as described below.

1. **Back-up copies.** You may make as many back-up copies as are necessary to protect your software in the event your original fails. Such copies are NOT to be used simultaneously on another machine. The law permits you to make such back-up copies even if the manufacturer does not provide you a process to make one.
2. **Multiple-loading or booting from one disk into multiple machines at the same time.** You may not simultaneously load one copy of a copyrighted program into a number of different machines, even if it is physically possible. Although you may use your legal copy in different machines at different times (so that you are only using one copy at a time), you may not permit multiple concurrent uses of the package. It would be legal to load and run it on one computer, turn that computer off, and then run it on another computer. For example, **WordPerfect** is sold for use on one computer, but it is possible to sequentially load it into a number of different computers and then run them at the same time. This is a clear violation of the law; you have caused the "proliferation of simultaneous users" (the legal term for this process). The fact that it is physically possible is irrelevant.
3. **Networks.** The concept of "proliferation of simultaneous users" also applies to networks.

Unless you purchased the software with an explicit “network license”, downloading the program to multiple stations at the same time violates the copyright law. As in the preceding example, the fact that it is physically possible to download the software on your network is irrelevant.

### **Instructional Responsibilities**

Academic Departments and individual course instructors should take measures to ensure that students are informed of the legal and ethical issues regarding software copyrighting, as well as University policy on this matter. As a minimum, departments should:

- Post the University policy regarding software copying in a conspicuous location adjacent to any departmental microcomputers which may be accessible to students.
- Include a statement of the University policy in syllabi for courses using microcomputers.
- Read and explain the University policy in any classes using microcomputers.

### **Use of Software in Course Work**

Departments and individual faculty are responsible for insuring that any copyrighted software made accessible to students be done so in accordance with University policy and all legal requirements. Specifically, faculty shall be careful to respect the following points:

- Neither departments nor faculty shall impose requirements which would encourage students to copy software in violation of University policy. Instructors shall not make assignments without verifying that a sufficient quantity of legal copies of software will be readily accessible to students for the completion of course assignments.
- Difficulty or expense involved in acquiring sufficient copies does not constitute a reason for violating University policy.
- Any copyrighted software made accessible to students shall bear the following statement conspicuously placed on both documentation and physical media (University Computer Center will provide labels for this purpose on request):

***This software is issued subject to University policy and may not be copied for any purpose whatsoever. Violation of this policy may lead to either disciplinary or legal action.***

- Software placed on course reserve in the University libraries, computer laboratories, or other campus sites must be in compliance with University software policy. Forms to certify compliance are available at Library circulation units.

**University of South Alabama**  
**Computer Use Policy**  
**Summary**

All persons using University of South Alabama computing and telecommunication resources must comply with the University's Computer Use Policy.

The Policy applies to all computer workstations, servers, network devices, software, databases, and related equipment accessed directly or indirectly through the Internet. The University encourages authorized users to make acceptable use of computer resources, consistent with its educational, research, and service-related mission. Users must also comply with all applicable federal and state laws and University regulations regarding intellectual property, including federal copyright law, and with all applicable licenses or contracts regarding the use of software.

In situations where access to computer resources is limited, priority use of these resources must be granted to educational and research-related activities. Recreational and personal use of University computer resources is permitted only to a limited extent and only when they are not needed for educational research activities.

Certain uses of University computer resources are never permitted. These include the following:

- Interfering with the operation of the USA computer and telecommunications systems, including "hacking" or "cracking"
- Altering or damaging computer hardware or software
- Transmitting obscene communications
- Using unauthorized passwords or circumventing system security
- Broadcasting unsolicited messages ("spamming")
- Invading the privacy of another person
- Using University resources for personal commercial or financial purposes, including the sales of lecture notes or the intellectual property of others
- Intentionally viewing, downloading, printing or sending unlawful material, including pornography, threats, or harassing communications

Users are responsible for the accuracy of all information posted on the Internet or on University-related home pages. In addition, any University web site must be consistent with the guidelines of the USA Department of Web Services, which can be found at <http://www.southalabama.edu/webservices/webpolicies.html>.

The foregoing is a summary of key points of the official University of South Alabama Computer Use Policy. The full text of that Policy can be found at [URL address], and users are expected to be familiar with it. Violation of the terms of the Policy can result in denial of privileges, and other penalties as outlined in the Policy. If there are any differences between this summary and the official Policy, the terms of the Policy shall supersede this summary.