



## University Policy Acceptable Use Policy

### Purpose

This policy provides guidelines for the appropriate use of information resources. Use of Albany State University's (ASU) network and computer resources should support the basic missions of the University in teaching, learning and research. Users of the ASU network and computer resources are responsible for proper use, protecting information resources, and respecting the rights of others.

### Scope

The policy applies to all ASU students, faculty and staff, and all others using computer and communication technologies whether personally or University owned, which accesses, transmits or stores University or student information.

### Policy

- **General Policy** Users of Albany State University's information resources must protect their online identity from use by another individual, the integrity of computer-based information resources, and the privacy of electronic information. In addition, users must refrain from seeking to gain unauthorized access, honor all copyrights and licenses and respect the rights of other information resources.
- **Access** Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access. Attempts to gain unauthorized access to a system or to another person's information is a violation of University policy and may also violate applicable law, potentially subjecting the user to both civil and criminal liability. However, authorized system administrators may access information resources, but only for a legitimate operational purpose and only the minimum access required to accomplish this legitimate operational purpose.
  - **Sharing ASU User IDs and Passwords;** Sharing of usernames and passwords used to access ASU information systems is prohibited.
  - **Information Belonging to Others;** Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.
  - **Abuse of Computing Privileges;** Users of ASU information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University.
- **Usage** Use of the University's information resources must comply with ASU policies and legal obligations (including licenses and contracts) and all federal and state laws.

- **Prohibited Use** Users must not send, view or download fraudulent, harassing, obscene (i.e., sexually explicit), threatening, or other messages or material that are a violation of applicable law or University policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.
- **Copyrights and Licenses** Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the University's information resources is a violation of this policy.
- **Social Media** Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.
- **Political Use** University information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, and may be used for other political activities only when in compliance with federal, state and other laws and in compliance with applicable University policies.
- **Personal Use** University information resources should not be used for activities unrelated to appropriate University functions, except in a purely incidental manner.
- **Use of University Information** Users must abide by applicable data storage and transmission policies.
- **Integrity of Information Resources** Users must respect the integrity of information and information resources.
- **Modification or Removal of Information or Information Resources Without proper authorization** Users must not attempt to modify or remove information or information resources that are owned or used by others.
- **Other Prohibited Activities** Users must not encroach, disrupt or otherwise interfere with access or use of the University's information or information resources. For the avoidance of doubt, without express permission, users must not give away University information or send bulk unsolicited email. In addition, users must not engage in other activities that damage, vandalize or otherwise compromise the integrity of University information or information resources.
- **Academic Pursuits** The University recognizes the value of legitimate research projects undertaken by faculty and students under faculty supervision. The University may restrict such activities in order to protect University and individual information and information resources, but in doing so will take into account legitimate academic pursuits.
- **Access for Legal and University Processes** Under some circumstances, as a result of investigations, subpoenas or lawsuits, the University may be required by law to provide electronic or other records, or information related to those records or relating to use of information resources, ("information records") to third parties. Additionally, the University may in its reasonable discretion review information records, e.g., for the proper functioning of the University, in connection with investigations, or to protect the safety of individuals or the ASU community. The University may also permit reasonable access to data to third-party service providers in order to provide, maintain or improve services to the University. Accordingly, users of University information resources do not have a reasonable expectation of privacy when using the University's information resources.

**Definitions (Optional)**

Definitions associated with this policy are available in the Information Technology and Data Security Terms Glossary.

**Accountability**

Violation of this policy may subject the user to sanctions, including the loss of computer and/or network access privileges, disciplinary action, suspension, termination of employment, dismissal from ASU, and/or legal action.

**Contacts**

- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

**References**

USG BOR IT Handbook, [http://www.usg.edu/information\\_technology\\_handbook/section5](http://www.usg.edu/information_technology_handbook/section5)

**Last Update**

July 31, 2018