Arkansas State University-Beebe

COMPUTER AND NETWORK USE POLICY

PREAMBLE

ASU-Beebe makes every reasonable effort to protect the rights of the users of its computing facilities while balancing those rights against the needs of the entire user community. Computing and networking resources are provided to support the academic instruction, research, and service components of this campus. These resources are for the sole use of ASU-Beebe students, faculty, staff, and other authorized users to accomplish the mission of the university. In accordance with the university mission and the Code of Conduct, it is assumed that expectations established for behavior will also be applied to the world of cyberspace.

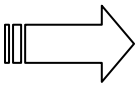
RIGHTS AND RESPONSIBILITIES

ASU-Beebe expects that users of campus computing and network facilities will respect the rights of other users as well as the integrity of the systems and related physical resources. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws. Because ASU-Beebe is a state agency, all information stored in computers owned or operated by ASU-Beebe is presumed to be a public record and subject to disclosure under the Arkansas Freedom of Information Act unless exempt under the law. Users do not own accounts on university computers, but are granted the privilege of exclusive use. The Electronic Communications Privacy Act authorizes system administrators and other university employees to access user files. By utilizing ASU-Beebe computing and network resources, you give consent to accessing and monitoring by system administrators and other university employees of any electronic communications, including stored communications, in order to enforce this policy or to protect the integrity of computer systems or the rights or property of the university. System administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information that may be used as evidence in a court of law. In addition, student files on university computer facilities are considered education records under the Family Educational Rights and Privacy Act (FERPA) of 1974 (Title 20 U.S.C. Section 1232(g)). See the University catalog for further information of FERPA.

ENFORCEMENT

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the person administering the accounts or network. This may be done through electronic mail or in-person discussion, education and documentation. Repeated minor infractions or misconduct may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior. In addition, offenders may be referred to their sponsoring advisor, department, employer, or other appropriate university office for further action. If the individual is a student, the matter may be referred to the Vice Chancellor of Student Services for disciplinary action. Any offense that violates local, state, or federal laws may result in the immediate loss of all university computing privileges and will be referred to the University Police office and other law enforcement authorities.

Continued on back



STANDARDS

Conduct that violates this policy includes, but is not limited to, the activities in the following list:

- Overloading the network with non-work related activities such as:
  - Internet Radio
  - Personal use of Social Networking Sites (Facebook, MySpace, etc)
  - Playing games
  - Watching movies
  - Using file sharing applications (Peer-to-Peer) for personal use or illegal copyright infringement activities
- Unauthorized use of a computer account
- Using the campus network to gain unauthorized access to any computer systems
- Connecting unauthorized equipment to the campus network
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage, or to place excessive load on a computer system or network. This includes, but not limited to, programs known as computer viruses, Trojan Horses, and worms.
- Deliberately wasting/overloading computer resources, such as printing too many copies of a document.
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.
- Using university resources for commercial activity such as creating products or services for sale.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- Initiating or propagating electronic chain letters.
- Inappropriate mass mailing. This includes multiple mailings to news groups, mailing lists, or individuals, (e.g. spamming, flooding, or bombing).
- Forging the identity of a user or machine in an electronic communication.
- Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing laws or university regulations.
- Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be in view of others.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

I have read the Network and Computer Use Policy. I agree to abide by the policy and understand that my computer privileges can be revoked.

_____ _____

Signature Date

Arkansas State University-Beebe
COMPUTER AND NETWORK USE POLICY

PREAMBLE

ASU-Beebe makes every reasonable effort to protect the rights of the users of its computing facilities while balancing those rights against the needs of the entire user community. Computing and networking resources are provided to support the academic instruction, research, and service components of this campus. These resources are for the sole use of ASU-Beebe students, faculty, staff, and other authorized users to accomplish the mission of the university. In accordance with the university mission and the Code of Conduct, it is assumed that expectations established for behavior will also be applied to the world of cyberspace.

RIGHTS AND RESPONSIBILITIES

ASU-Beebe expects that users of campus computing and network facilities will respect the rights of other users as well as the integrity of the systems and related physical resources. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws. Because ASU-Beebe is a state agency, all information stored in computers owned or operated by ASU-Beebe is presumed to be a public record and subject to disclosure under the Arkansas Freedom of Information Act unless exempt under the law. Users do not own accounts on university computers, but are granted the privilege of exclusive use. The Electronic Communications Privacy Act authorizes system administrators and other university employees to access user files. By utilizing ASU-Beebe computing and network resources, you give consent to accessing and monitoring by system administrators and other university employees of any electronic communications, including stored communications, in order to enforce this policy or to protect the integrity of computer systems or the rights or property of the university. System administrators may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information that may be used as evidence in a court of law. In addition, student files on university computer facilities are considered education records under the Family Educational Rights and Privacy Act (FERPA) of 1974 (Title 20 U.S.C. Section 1232(g)). See the University catalog for further information of FERPA.

ENFORCEMENT

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the person administering the accounts or network. This may be done through electronic mail or in-person discussion, education and documentation. Repeated minor infractions or misconduct may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior. In addition, offenders may be referred to their sponsoring advisor, department, employer, or other appropriate university office for further action. If the individual is a student, the matter may be referred to the Vice Chancellor of Student Services for disciplinary action. Any offense that violates local, state, or federal laws may result in the immediate loss of all university computing privileges and will be referred to the University Police office and other law enforcement authorities.

STANDARDS

Conduct that violates this policy includes, but is not limited to, the activities in the following list:

- Overloading the network with non-work related activities such as:
  - Internet Radio
  - Personal use of Social Networking Sites (Facebook, MySpace, etc)
  - Playing games
  - Watching movies
  - Using file sharing applications (Peer-to-Peer) for personal use or illegal copyright infringement activities
- Unauthorized use of a computer account
- Using the campus network to gain unauthorized access to any computer systems
- Connecting unauthorized equipment to the campus network
- Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage, or to place excessive load on a computer system or network. This includes, but not limited to, programs known as computer viruses, Trojan Horses, and worms.
- Deliberately wasting/overloading computer resources, such as printing too many copies of a document.
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.
- Using university resources for commercial activity such as creating products or services for sale.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- Initiating or propagating electronic chain letters.
- Inappropriate mass mailing. This includes multiple mailings to news groups, mailing lists, or individuals, (e.g. spamming, flooding, or bombing).
- Forging the identity of a user or machine in an electronic communication.
- Transmitting or reproducing materials that are slanderous or defamatory in nature or that otherwise violate existing laws or university regulations.
- Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be in view of others.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

I have read the Network and Computer Use Policy. I agree to abide by the policy and understand that my computer privileges can be revoked.

_____ _____

Signature Date