KENTUCKY STATE UNIVERSITY

KENTUCKY STATE UNIVERSITY POLICIES AND PROCEDURES

POLICY TITLE:

Appropriate Use of Technology Policy

VOLUME, SECTION & NUMBER:

ENTITIES AFFECTED:

Faculty
Staff
Students

ADMINISTRATIVE AUTHORITY:

Information Technology

APPROVED BY:

Office of the President

EFFECTIVE DATE:

July 8, 2024

REVISED FROM:

May 2013 Version of Policy

POLICY STATEMENT:

This policy details the appropriate use of all Kentucky State University (KSU) computing and network resources. It is intended to provide effective protection of all individual users, equitable access, proper management of those resources, and the data residing thereon. These guidelines are intended to supplement, and not replace, all existing applicable laws, regulations, agreements, and contracts that currently apply to those resources. Access to KSU's technology resources is a privilege, and all users have the responsibility of using these resources in an efficient, ethical, and legal manner.

Access to KSU networks and computer systems is granted subject to KSU policies and local, state, and federal laws. Appropriate use should always be legal and ethical, reflect academic honesty and community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; copyright laws; ownership of data system security mechanisms; and individuals' rights to privacy, freedom of speech, and freedom from intimidation, harassment, and unwarranted annoyance. While respecting individuals' confidentiality and privacy, KSU reserves the right to examine all computer files.

KSU is not responsible for unacceptable or unethical use of KSU technology resources, including computers, computer networks, and electronic communication systems.

KSU may restrict the use of its computers and network systems or electronic communications when presented with evidence of an individual's violation of KSU policies or federal or state laws.

KSU reserves the right to limit access to its network through KSU-owned or personal computers, and to remove or limit access to material posted on KSU-owned computers. KSU will limit access to any and all devices attached to the KSU network that do not have up-to-date anti-virus protection. KSU will limit access to any activity that interferes with the academic or administrative use of technology resources by others. KSU will limit access to internet sites known to cause or have malicious activity, phishing, and malware.

Individuals utilizing technology resources are required to exclusively use accounts, passwords, and authentication credentials that have been officially sanctioned for their respective roles within KSU. Additionally, users are obligated to safeguard their KSU-assigned accounts and authentication credentials to prevent unauthorized use or access by others.

Users must adhere to the security measures implemented on all technology resources used for KSU-related activities, regardless of whether the resources are KSU-owned or personally owned.

Users must take accountability for the content within their personal communications and acknowledge the potential personal liability that may arise as a consequence of such use.

Questions regarding this policy should be directed to Information Technology (IT).

APPROPRIATE USE:

Appropriate use of technology resources includes instruction; independent study; authorized research; independent research; and official work performed by the recognized offices, units, organizations, and agencies of KSU.

Authorized use of KSU-owned or operated computing and networking resources is consistent with the education, research, and service mission of KSU. All other use not consistent with this policy may be considered unauthorized use.

Authorized users include: (1) faculty, staff, and students of KSU; (2) and others whose access furthers the mission of KSU (i.e., consultants, colleagues with system access for specific projects) and whose use does not interfere with other users' access to resources.

Acceptable conduct must conform to all University policies and federal and state laws.

Employees must acknowledge the potential for, and potential effects of, manipulating information, especially in electronic form, understand the changeable nature of electronically stored information, and continuously verify the integrity and completeness of information that is compiled or used. Employees are responsible for the security and integrity of KSU information, and all such information must be stored on KSU servers, network security devices, or KSU-approved cloud storage. Therefore, employees must not store information solely on their individual desktops or laptops. A password-protected screen saver with a maximum lock-out time of 15 minutes is required for all employees' computers. Employees must also not store any personal files on any KSU technology resources.

INAPPROPRIATE AND PROHIBITED USE:

Access to KSU networks and technology resources is conditioned upon compliance with this policy and all other KSU policies, as well as state and federal laws. Though not exhaustive, the following list provides examples of use that is strictly prohibited.

- Using facilities, accounts, access codes, privileges, or information to which access is not authorized.
- Sharing authentication details or granting access to KSU accounts to unauthorized individuals.
- Viewing, copying, altering, or destroying any files without explicit permission from a supervisor and IT.
- Falsely representing one system user electronically as another user.
- Creating or forwarding chain letters.
- Possessing, posting, accessing, or distributing obscene materials (e.g., pornography, racial slurs, expletives).
- Abusing, harassing, threatening, stalking, or discriminating against others through use of technology resources.
- Non-academic or non-administrative use that interferes with the academic or administrative use by others.
- Making, distributing, or using unauthorized copies of licensed software.
- Obstructing workflow by consuming large amounts of system resources, such as disk space, CPU time, etc.
- Introducing destructive software (e.g., virus software)
- Running or otherwise configuring software or hardware to intentionally allow access by unauthorized users.
- Attempting to circumvent or subvert any system's security measures.
- Advertising for commercial gain or distributing unsolicited advertising.
- Disrupting services, damaging files, or intentionally damaging or destroying equipment, software, or data belonging to KSU or other users.
- Using computing resources for the unauthorized monitoring of electronic communications.

REPORTING VIOLATIONS:

Any misuse or violation of KSU’s technology resources will be judged in accordance with published policies and rules of conduct. Such policies include, but are not limited to, Human Resources policies and Codes of Conduct.

All users and department units should immediately report any discovered unauthorized access attempts or other improper use of KSU computers, networks, or other information-processing equipment. Any observations or reports of security or abuse problems with any KSU computer or network resources should be immediately forwarded to the Information Technology Help Desk and other appropriate administrators.

SANCTIONS:

System users in violation of this policy are subject to a full range of sanctions, including the loss of computer and network access privileges, disciplinary action, dismissal from KSU, and legal action. Some violations may constitute criminal offenses as outlined in state statutes and federal laws. KSU will carry out its responsibility to report such violations to the appropriate authorities.

In instances of unauthorized use, department leaders and supervisors have the authority to deny access to KSU computers and network systems under their control.

RELATED POLICIES:

Email Policy

Internet Policy

Software Policy