APPROPRITAE USAGE (INFORMATION TECHNOLOGY)

1. Appropriate Usage

PURPOSE:

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

POLICY:

Access to KSU networks and computer systems is granted subject to University 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 toprivacy, freedom of speech, and freedom from intimidation, harassment, and unwarrantedannoyance. While respecting individuals' confidentiality and privacy, the University reserves the right to examine all computer files.

The University is not responsible for unacceptable or unethical use of the information technology environment including computer and computer networks or electronic communication system. The University may restrict the use of its computers and networksystems or electronic communications when faced with evidence of violation of University policies, or federal or local laws. The University reserves the right to limit access to its networks through University-owned or other computers, and to remove or limit access to material posted on University-owned computers. The University will limit access to any and all machined attached to the University network that does not have up- to-date Anti-virus protect to the internet, no access to the internal network or intranet willbe allowed. The University will limit access to any activity that interferes with academic or administrative use by others of computer

resources. The University will limit access to the following category of internet sites known to cause malicious activity, phishing,malware and known legal sharing sites.

Appropriate Use

Appropriate use of information technology resources includes instruction; independent study; authorized research; independent research; and official work of the offices, units,recognized student and campus organizations, and agencies of the University.

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

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

Acceptable conduct in and use of this environment must conform to: existing University policies, guidelines, and codes of conduct; KSU's Internet, Intranet, E-mail, Intellectual Property and Information Resource Policies; KSU Board of Regents policies and guidelines; the usage guidelines of other networks linked to KSU's networks or computersystems, and existing local, state, and federal laws.

Employees must acknowledge the potential for and possible effects of manipulating information, especially in electronic form, understands 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 University information and all such information should be stored on University servers, Network storage devices or University approved Cloud Storage and not stored on their individual desktop or laptop computing systems. A password protected screen saver with a maximum time of 5 minutes is required for all employee PC's. Employees are also responsible for NOT storing personal files (pictures, music, videosetc.) on any University network resource.

Examples of Prohibited Use

Use of KSU network and computer systems is conditioned upon compliance with this andother university policies and all applicable laws. Though not exhaustive, the following list is provided to emphasize that these activities are NOT allowed on KSU network or computer systems:

- Using facilities, accounts, access codes, privileges, or information to which access isnot authorized;
- Viewing, copying, altering, or destroying any files without explicit permission;
- Falsely representing one system user electronically as another user;
- Cheating and/or forwarding chain letters;
- Possessing, posting, accessing or distributing obscene materials. Examples includebut are not limited to materials that contain pornography, racial slurs, expletives;
- Abusing, harassing, threatening, stalking or discriminating against others by use ofcomputing resources;
- Game playing that interferes with academic or administrative use by others;
- Making, distributing, or using unauthorized copies of licensed software (seeComputer Software Policy and Copyright and Educational Fair Use Policy);
- Obstructing workflow by consuming large amounts of system resources, such as diskspace, CPU time, etc.
- Introducing destructive software, e.g. "virus" software, or precipitating systemcrashes;
- Running or otherwise configuring software or hardware to intentionally allow accessby 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 destroyingequipment, software, or data belonging to KSU or other users;
- Using computing resources for unauthorized monitoring of electroniccommunications;
- Employees are also responsible for NOT storing personal files (pictures, music,videos etc.) on any University network resource.

Reporting Violations

Any misuse or violation of KSU's information-technology environment will be judged inaccordance with those published polices and rules of conduct. Such policies include but are not limited to, the KSU Student Handbook, the Faculty Handbook, and the UniversityPolicy and Procedures Manual.

All users and department units should immediately report any discovered unauthorized access attempts or other improper usage of KSU computers, networks, or other information processing equipment. Any observations or reports of security or abuse problems with any University computer or network facilities, including violations of thispolicy, should be immediately forwarded to the Information Technology Help Desk or other appropriate administrator.

Sanctions

System users in violation of this policy are subject to the full range of sanctions, including the loss, without notification, of computer or network access privileges, disciplinary action, dismissal from the University, and legal action. Some violations mayconstitute criminal offenses, as outlined in Kentucky statutes and other local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

In instances of unauthorized use, departmental leaders have the authority to deny accessto KSU's computers and network systems under their control.

Questions regarding this policy should be directed to the Information Technology HelpDesk.

2. Entities Affected

- Information Technology
- Student Engagement and Campus Life
- Office of Human Resources

3. Policy Owner/Interpreting Authority

Executive Vice President for Finance and Administration
Chief Information Technology Officer

4. Related Policies

List number(s) and name(s) of related policies or manuals

5. Statutory or Regulatory References