KENTUCKY STATE UNIVERSITY

Policies and Regulations

POLICY TITLE:

Appropriate Use of Technology

APPLIES TO:

Students, Faculty, Staff, Administration, and other authorized users of KSU technology resources

ADMINISTRATIVE AUTHORITY:

Chief Information Officer (CIO)
Department of Information Technology (IT)

APPROVED BY:

Kentucky State University Board of Regents

EFFECTIVE DATE:

August 8, 2025

NEXT REVIEW DATE:

August 8, 2028

POLICY STATEMENT:

This policy details the appropriate use of all Kentucky State University (KSU) computing and network resources to ensure the protection of individual users, equitable access, and proper management of university data. 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, consistent with the university's mission. While respecting individual privacy, KSU reserves the right to examine all computer files and to limit or restrict access to its network to protect the security and integrity of its resources.

DEFINITIONS:

Technology Resources

All university networks, computer systems, accounts, passwords, authentication credentials, software, and data, whether accessed on KSU-owned or personally-owned devices.

Authorized Users

Faculty, staff, and students of KSU, as well as others such as consultants or project colleagues whose access furthers the mission of KSU.

PROCESS:

Appropriate Use and User Responsibilities

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

- **Accountability:** Users must use only the accounts and credentials officially sanctioned for their role and are obligated to safeguard them from unauthorized use. Users are accountable for all activities conducted under their credentials and for the legal consequences of any misuse.

- **Acknowledgement of Responsibility:** Users, particularly students, may be required to sign an agreement acknowledging their understanding of and responsibility to comply with this policy and applicable state laws.

- **Security Measures:**

    - A password-protected screen saver with a maximum lock-out time of fifteen (15) minutes is required for all employee computers.

    - Users must ensure any device connected to the KSU network has up-to-date anti-virus protection. KSU will limit access for non-compliant devices.

- **Data Security for Employees:** Employees are responsible for the security and integrity of KSU information. All such information must be stored on KSU servers or KSU-approved cloud storage, not solely on individual desktops or laptops.

- **Personal Files:** Employees must not store any personal files on any KSU technology resources.

Inappropriate and Prohibited Use

Access to KSU technology resources is conditioned upon compliance with university policies and law. Prohibited uses include, but are not limited to:

- Using facilities, accounts, or access codes without authorization, or sharing authentication details with unauthorized individuals.

- Viewing, copying, altering, or destroying files without explicit permission.

- Falsely representing one user as another.

- Distributing obscene materials, or abusing, harassing, threatening, or discriminating against others.

- Making or distributing unauthorized copies of licensed software.

- Intentionally introducing destructive software (e.g., a virus) or circumventing system security measures.
- Using resources for commercial gain or distributing unsolicited advertising.
- Intentionally damaging equipment, software, or data belonging to KSU or other users.

Reporting Violations
All users should immediately report any discovered unauthorized access attempts or other improper use of KSU technology resources to the Information Technology Help Desk.

Sanctions for Violations
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. KSU will carry out its responsibility to report such violations to the appropriate authorities.

REFERENCES AND RELATED MATERIALS:

- KSU Email Policy
- KSU Software Policy
- KSU Information Technology Security Policy
- KRS 434.840–434.860 (Unlawful Access to a Computer)

CONTACTS:

Subject	Office	Telephone	E-mail
General Questions	Office of the CIO	(502) 597-7000	Wendy.Dixie@kysu.edu

HISTORY:

Revision Type	Date of Issuance/Revision	Drafter(s)/Editor(s)
Issued (New Policy)	August 2024	Wendy Dixie and Zach Atwell
Revised (New Template and Minor Revisions)	June 2025	Wendy Dixie and Zach Atwell