FORT HAYS STATE UNIVERSITY
Forward thinking. World ready.

University Policies
www.fhsu.edu/policies/

POLICY TITLE: **Acceptable Use of Computing Resources**

POLICY PURPOSE: This policy outlines the expectations for the use of computing and electronic information resources at Fort Hays State University (FHSU).

BACKGROUND: KITEC Information Technology Policy 7230 instructs all State of Kansas agencies to implement a policy for acceptable use of information systems.

FHSU provides computing resources to its faculty, staff, and students for legitimate administrative, educational, and research efforts. System Users are expected to exercise reasonable care in the utilization of FHSU information systems or their components. This policy is intended to supplement, not replace, all existing laws, regulations, agreements, and contracts which currently apply to computing resources.

APPLIES TO: This policy applies to faculty, staff, students, official university affiliates, and any other individuals who use FHSU computing resources (hereinafter "System Users").

DEFINITIONS: **Affiliated Organization (or "Affiliates")** Any organization associated with the University that uses university information technology resources to create, access, store, or manage University Data to perform their business functions.

KITEC: Kansas Information Technology Executive Council

System Users: Faculty, staff, students, official university affiliates, and any other individuals who use FHSU computing resources.

TigerNetID: Username and password assigned to System Users upon employment, acceptance to, or the beginning of a business relationship with FHSU.

University data: Electronic information providing support to and meeting needs of the University community. Data includes, but is not limited to:

- Elements supporting financial management;
- Student records;
- Payroll;
- Personnel records;
- Capital equipment inventory; and,
- Any electronic information:
    - Used for planning, managing, reporting, or auditing a major administrative function;

- Referenced or used by a Department(s) or College(s) to conduct University business;
- Included in a University administrative report; or,
- Used to derive a data element meeting any of the criteria above.

CONTENTS:

POLICY STATEMENT:

General Use and Ownership

Computing and information technology resources are the property of FHSU and should be used for the primary purpose of benefiting, enhancing, or furthering the mission of the University.

System Users have a responsibility to promptly report the theft, loss, or unauthorized disclosure of FHSU data or protected information. This includes reporting the theft or loss of devices which may contain FHSU data, such as laptops or cell phones.

Any FHSU-owned laptop, tablet, or other computing device must be checked by Technology Services prior to leaving the United States.

System Users may access, use, or share Internal or Restricted Use Information only to the extent it is authorized and necessary to fulfill their assigned job duties.

Communications made using FHSU computing resources may be subject to access and disclosure pursuant to the Kansas Open Records Act.

Authorized University personnel must have access to e-mail and other data stored on FHSU computing resources and must engage in general monitoring to ensure delivery and security of services. This access is required to troubleshoot hardware and software problems, prevent unauthorized access and system misuse, retrieve business related information, assure compliance with software distribution policies, comply with legal and regulatory requests for information, or comply with local, state, or federal law.

The University, in its discretion decided by President with consultation of General Counsel or as required by law or regulatory order, may disclose data to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings.

System Users will acknowledge review of the Acceptable Use of Computing Resources Policy during initial and annual security awareness training.

Appropriate Use

In making appropriate use of FHSU computing resources, System Users must accept responsibility for their behavior, act in a legal and ethical manner, and:

- Protect their user accounts and passwords from unauthorized use, recognizing that individuals are responsible for all activities conducted with their user accounts.
- Access only files and data that they own, they have been given authorization for, or that are publicly available.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in their use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data (spamming, downloading/uploading personal files, or engaging in peer-to-peer file sharing of non-work-related files), and wasting disk space, printer paper and toner, and other computing resources.
- Comply in all respects with any request by the University to retain certain information, recognizing that information stored on the University's network is ultimately the responsibility of the University.

Examples of Prohibited Use

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

- Accessing another person’s files or data without permission.
- Storing non-public FHSU data anywhere except FHSU file servers or FHSU-provided OneDrive for Business.
- Attempting to circumvent or subvert any system’s security measures.
- Running or otherwise configuring software or hardware to intentionally allow access by unauthorized users.
- Disrupting services, damaging files, or intentionally damaging or destroying equipment, software, or data belonging to FHSU or other System Users.
- Making or using illegal copies of copyrighted software or other copyrighted materials (such as digitized artistic productions and music or video files), storing such copies on FHSU systems, or transmitting them over FHSU networks.
- Using e-mail or message services to harass, intimidate, threaten, or otherwise annoy another person by use of sexual or bigoted content or content which poses an imminent threat to the life or safety of the person or persons receiving the communication.
- Disclosing your passwords or using another person’s user account or passwords.

- Using FHSU systems for commercial use, such as performing work for profit or advertising in a manner not authorized by FHSU.
- Posting web pages that contain material that is illegal or promotes illegal activity (e.g., gambling or child pornography).
- Masking the identity of an account or machine. This includes sending e-mail that appears to come from someone else or impersonating a University office, faculty/staff member, or student.
- Violating any FHSU or Kansas Board of Regents policy or any local, state, or federal law.

Internal and Restricted-Use Information

System Users are expected to exercise judgment and follow the Data Classification Policy and all related policies and procedures when saving, storing, sharing, or otherwise working with Internal or Restricted-Use Information.

Reporting Violations

System Users have a responsibility to report violations of this policy. If you observe, or have reported to you, a security or abuse problem with any FHSU computing resource, you should notify the Information Security Officer or Director of Technology Services.

Consequences of Misuse

Violations of this policy will be investigated as a security event. Individuals who violate this policy will be held accountable for their conduct and may be subject to loss of computer or network access privileges, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, and the University will carry out its responsibility to report such violations to the appropriate authorities.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

Academic Freedom

No provision of this policy shall be construed so as to impose any limit to the academic freedom of faculty in their instructional, research, or service activities.

RELATED DOCUMENTS:

Policies:

Data Classification Policy

Email Policy

Endpoint Protection and Configuration Policy

Information Security Policy

Media Sanitization and Disposal Policy

Physical Security of Data Center and University Data Policy

	Forms:
	Other:
KEYWORDS:	Acceptable use, information technology
RESPONSIBLE OFFICE:	Division of Technology Services
RESPONSIBLE UNIVERSITY OFFICIAL:	Director of Technology Services
ORIGINATION DATE:	*Adopted by President's Cabinet 06/02/99* Revised by President's Cabinet 04/05/06 Revised by President's Cabinet 03/05/08
REVIEW CYCLE:	Every 3 years

POLICY ADDRESS:	
	Adopted by ELT on 3/31/2017
LAST APPROVED ON:	
REVIEW/CHANGE HISTORY:	
	3/2020
NEXT REVIEW DATE:	
