Information Technology Resources Acceptable Use

Information Technology Resources Acceptable Use Policy

Approved by and date:
Board of Trustees *09/18/2017*
Executive Leadership Team *09/01/2017*

Policy:

Kilgore College provides information technology resources to employees and students to support the College's mission. Access to Kilgore College's (KC) information technology resources is a privilege, not a right. All users are required to acknowledge receipt and understanding of all administrative regulations governing use of KC's information technology resources and will agree in writing to allow monitoring of their use and to comply with such regulations and guidelines annually. Noncompliance will result in suspension of access or termination of privileges and other disciplinary action consistent with KC policies. Violations of law may result in criminal prosecution as well as disciplinary action by KC.

Procedures:

Approved by and date:
Executive Leadership Team *09/01/2017*

Electronic files created, sent, received, or stored on information technology resources owned, leased, administered, or otherwise under the custody and control of Kilgore College are the property of Kilgore College unless a written agreement exists otherwise. All messages, files and documents – including personal messages, files and documents – located on Kilgore College information technology resources are owned by Kilgore College, may be subject to open records requests, and may be accessed by the Director of Information Technology in accordance with this policy.

Definitions

a. Information technology resources are defined as any and all computer and peripheral devices capable of receiving, storing, managing, or transmitting electronic data, the wired and wireless networks that connect these devices, and the information stored on those devices.
b. A user is defined as an individual or an automated application process that is authorized to access Kilgore College Information Technology Resources.

Procedures

a. All wireless access points/routers accessing Kilgore College's network must be owned or approved, in writing, by Kilgore College.
b. Users must not share their Kilgore College account(s), passwords, personal identification numbers (PIN), security tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.

c. Users must report any weaknesses in College computer security and any incidents of possible misuse or violation of this policy and its procedures to the appropriate supervisor.
d. Users must not download, install, or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, College users must not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on College information technology resources.
e. Users must not attempt to access any data or programs contained on College information technology resources for which they do not have authorization or explicit consent.
f. Users must not make, acquire, or use unauthorized copies of copyrighted software on Kilgore College information technology resources.
g. Users must remove disruptive software, shareware, or freeware installed on College information technology resources when requested by appropriate management personnel.
h. Users must not purposely engage in any activity that may do any of the following: harass, threaten, or abuse others; degrade the performance of information technology resources including downloading large files from the Internet that are unrelated to the academic or administrative functions of Kilgore College; deprive an authorized Kilgore College user access to a Kilgore College resource; obtain extra resources beyond those allocated; or circumvent Kilgore College computer security measures.
i. Users must not intentionally access, create, store or transmit material which Kilgore College may deem to be offensive, indecent, or obscene (other than in the course of academic research where this aspect of the research has the explicit written approval of the Kilgore College vice president of instruction).
j. Kilgore College information technology resources must not be used for personal business or benefit.
k. Kilgore College owned software will not be installed on personally owned equipment.
l. Users must not otherwise engage in acts against the aims and purposes of Kilgore College as specified in its governing documents or in rules, regulations, and procedures adopted from time to time.
m. As a convenience to the Kilgore College user community, incidental personal use of information technology resources is permitted. The following restrictions apply:
    1) Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to Kilgore College approved users; it does not extend to family members or other acquaintances.
    2) Incidental personal use must not result in any direct costs to Kilgore College.
    3) Incidental personal use must not interfere with the normal performance of an employee's work duties.
    4) No files or documents may be sent or received that may cause legal action against, or embarrassment to, Kilgore College.
n. Storage of personal email messages, voice messages, files, and documents within Kilgore College's information technology resources must be nominal. Violation of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Kilgore College information technology resources access privileges, as well as, civil, and criminal prosecution.