KANSAS CITY UNIVERSITY OF MEDICINE AND BIOSCIENCES	EFFECTIVE: **June 1, 2003**	ISSUED BY: Human Resources	POLICY NO. 7.5
STANDARD POLICY: Technology and Software Use	SUPERCEDES: August 1, 2000	APPROVED BY:	

1. PURPOSE

Kansas City University of Medicine and Biosciences recognizes the abundance of technological resources available. It is essential for individuals to have access to the latest technology and information obtainable in order to effectively and efficiently do their jobs, reach their goals, grow professionally, and fulfill their educational requirements. For this reason, through the Information Technology department, KCUMB provides technological access to individuals. Nevertheless, KCUMB must respect and observe the rights and privileges of copyright holders, obey the United States Copyright Act, and preserve the integrity of its internal network systems.

2. APPLICATION

KCUMB employees, faculty, agents, students, and authorized account holders.

3. DEFINITIONS

a. Authorized Equipment — computing equipment, including peripherals, either owned or leased by KCUMB or specifically authorized in writing by KCUMB's Information Technology department for use on KCUMB premises or in connection with KCUMB-related research, education, study, business, or projects. Assignment of an account authorizes the account holder to access KCUMB sponsored applications from a location off KCUMB premises via a non-KCUMB computer. Although such non-KCUMB computers shall not be deemed "Authorized Equipment," the **drive space** allocated to the account holder IS considered "Authorized Equipment," and at all times will be considered the premises of and property of KCUMB.

b. Chain Letter — any electronic communication urging the recipient to forward the message to other users in order to avoid bad luck or other adverse consequences or to receive a benefit or reward for responding and/or forwarding the message or its content.

c. CIO — Chief Information Officer

d. Copyrighted Material — any computer software and documentation and any graphical, textual, video, or musical work bearing a notice of copyright or otherwise appearing to be subject to copyright protection.

e. Peripherals — any piece of hardware connected to a computer; any part of the computer outside the CPU and working memory. Some examples of peripherals are keyboard, mice, monitors, printers, scanners, PDAs, disk and tape drives, microphones, speakers, joysticks, plotters, and cameras.

f. KCUMB— Kansas City University of Medicine and Biosciences and all entities (corporate or otherwise) directly or indirectly controlled by Kansas City University of Medicine and Biosciences.

4. ACCOUNT GUIDELINES

Accounts are automatically created for all registered KCUMB students and employees on an as needed basis for the purpose of performing job duties or for educational requirements. Accounts may be set up for KCUMB partners or other individuals pursuant to special service arrangements. Accounts will remain in effect until graduation, termination, expiration of the account pursuant to the terms of the special arrangement, or when the provisions of this policy have been violated, as applicable.

a. Disk space in students' directories will be limited. Requests for additional space must be directed to the CIO of the Information Technology department. Such requests may be granted only under exceptional circumstances.

b. No disk, tape, or other portable storage medium may be inserted into any Authorized Equipment until it has been checked for viruses.

c. Use of software owned or licensed by KCUMB constitutes the user's agreement to abide by copyright laws, license agreements, and all other appropriate laws and regulations.

d. Only properly licensed software will be considered for installation.

e. Only KCUMB licensed software may be used on Authorized Equipment, unless specific written authorization has been obtained from the CIO of the Information Technology department AND the user can demonstrate that the software is properly licensed.

f. Direct connection of personally owned equipment to KCUMB networks and use of personally owned computer equipment on KCUMB premises will not be permitted, unless the user can assure Information Technology that such equipment is free from viruses or other destructive or disabling code. In addition, the user must provide Information Technology with the estimated duration connectivity is to remain. If equipment is to remain connected for more than 24 hours, the user must demonstrate that all software on such personally owned equipment is properly licensed.

g. It is permissible to download text files ("ASCII" format) or Portable Document Format ("PDF") documents. These files contain no computer code and generally end with the file extensions ".txt," ".pdf.," et cetera. Files with typical word processor file extensions such as ".wpd" or ".doc" should be saved on a floppy disk and scanned for viruses before being loaded on the network or the hard drive of any KCUMB computer.

h. KCUMB cannot and does not make any guarantee, explicit or implied, regarding the privacy of electronic mail or any other KCUMB-sponsored applications. Electronic mail is vulnerable to interception, misdirection and rerouting. Highly confidential materials should be delivered and stored in another manner.

5. USER RESPONSIBILITIES

Individuals who use Information Technology resources at Kansas City University of Medicine and Biosciences are granted such access as a privilege. Everyone is expected to use accounts responsibly, within the KCUMB approved educational, academic, research, and/or administrative guidelines for which such accounts are granted.

a. Individuals shall use only the KCUMB accounts that have been authorized for his/her use.

b. Individuals are responsible for ANY activity conducted on his/her accounts, and should protect his/her accounts by keeping passwords confidential.

c. Users are responsible for ensuring that the Authorized Equipment for which he/she is responsible remains in compliance with this policy.

d. Individuals learning of any misuse of KCUMB equipment or violations of this policy shall notify the CIO of the Information Technology department.

e. The Internet facilities provided by KCUMB are University property. Access to the Internet imposes certain responsibilities and obligations. Use of the Internet (including Internet applications, i.e., Blackboard, etc.) must be ethical and honest with due respect for intellectual property rights, system security, and personal privacy.

f. Users are encouraged to review the Sexual Harassment policy maintained by Human Resources or the Anti-Discrimination policy, maintained by Student Affairs. These specifically address procedures for reporting such incidents and the enforcement of these policies.

6. EMPLOYER MONITORING RIGHTS

KCUMB reserves the right to:

a. Access or monitor (without notice) any use of the KCUMB network, including Internet access, E-mail use, Blackboard access and use, storage of electronic, magnetic, and other files and information, etc. Use of any KCUMB-sponsored applications constitutes consent to such access and monitoring.

b. Request and obtain proof of proper licensing from any user of any software applications found on KCUMB Authorized Equipment.

c. Inspect the drive space of all account holders, any and all other Authorized Equipment, and any equipment on KCUMB premises, which is of a type and general character so as to be likely to be subject to these policies, including, but not limited to, the hardware itself and E-mail messages stored thereon and areas of KCUMB's network and KCUMB-sponsored applications.

d. Monitor and read E-mail messages and discussion boards. All electronic mail accounts and the content of the discussion boards are the property of KCUMB.

e. Periodically audit all Authorized Equipment for software and other materials that may violate this policy.

7. PROHIBITED ACTIVITIES

Be aware that KCUMB's status as an academic institution does not exempt it, its employees, faculty, agents, or its students from laws regarding the use and exploitation of intellectual property. Academic institutions have been and will be held liable for any unauthorized uses of proprietary material. If a particular activity is prohibited by this policy, then it has been determined by KCUMB that such activity is either unlawful or exposes KCUMB to unacceptable potential loss or liability.

Users are strictly prohibited from performing, alone or in conjunction with, any of the following activities. These include, but are not limited to, the following:

a. Sharing of passwords or logins. Allowing friends, family, co-workers, or others to use KCUMB accounts, either locally or through dial-in or Internet connections.

b. Copying software without the proper authorization.

c. Theft of hardware, software (including unauthorized reproduction), supplies, or other property.

d. Installing software (including games, shareware, freeware, careware, etc.) on any KCUMB computer hard drive or network drive.

e. Without proper authorization, attempting to:

   1) access, copy, or destroy programs or files that belong to other users or KCUMB;

   2) disable or overload any computer system or network;

   3) circumvent any system or procedure intended to protect the privacy or security of any person, network, information, data, program, or system; or

   4) place or use, regardless of the means, on KCUMB property or in accounts on any KCUMB equipment of so-called "hacker" files or other computer programs or devices whose principal function is to defeat security or copy protection mechanisms.

f. Modifying or altering KCUMB computing equipment:

1) Computer settings;

2) Introducing viruses, worms, Trojan horses, trap-door programs, or other intentionally destructive or disabling codes into any system running on any KCUMB equipment (this includes the Internet); or

3) Making any changes without written permission from the CIO of the Information Technology department.

g. Attempting to undermine network security, to impair functionality of the network, or to bypass restrictions including, but not limited to, security restrictions set by Information Technology or KCUMB.

h. Assisting others in violating, or negligently allowing others to violate rules.

i. Copying or uploading to, or copying or downloading from, Authorized Equipment copyrighted materials by account holders or other KCUMB personnel other than specifically authorized members of Information Technology.

j. Displaying, storing, and/or using the Internet to view, access, upload, download, store, transmit, create, or otherwise manipulate illegal or unlicensed software, copyrighted material (in the absence of the authorization of the copyright holder), pornographic material, MP3 files (i.e., music, video, etc.) or other unauthorized and/or non-course designated sexually explicit materials on any Authorized Equipment. In addition, such material may not be archived, stored, distributed, edited, or recorded using Authorized Equipment.

k. Messages with sexual, racial, discrimination or harassing content, including any offensive or unlawful remarks, jokes, slurs and obscenities.

l. Electronic chain letters.

m. Use of E-mail or Internet services (including Internet applications, i.e., Blackboard, etc.) for financial gain, business or commercial enterprises, personal use during scheduled working hours (including "surfing the net"), or illegal activities (including use of KCUMB's E-mail address or any part of a KCUMB domain name to solicit or receive solicited commercial-related or illegal communications).

n. Libelous or hateful material.

o. Downloading from the Internet any program, "plug-in," or other binary file to any Authorized Equipment without the prior consent of the CIO of the Information Technology department. (This includes, but is not limited to, files with the extension ".exe" or ".com").

8. DISCIPLINE

Unauthorized or fraudulent use of the University's computing resources is a serious violation of University regulations and may be against the law. **Failure to comply with the stated provisions and applicable local, state, and federal laws may result in disciplinary action and/or civil penalties (including damages, criminal fines and/or imprisonment).** Information derived from system monitoring and/or contained in electronic message or files may be used as a basis for administrative, disciplinary, or criminal proceedings.

a. Individuals who do not comply with the provisions outlined in this policy may have all user privileges suspended, restricted, or terminated. In addition, users may be subject to further disciplinary action, which may result in suspension, expulsion, or termination from KCUMB.

b. Any account holder who knowingly or negligently allows a third party to use his or her accounts to do anything otherwise prohibited by this policy shall be disciplined as if the account holder was the responsible party.

c. In addition to any action which KCUMB may take against the account holder, KCUMB reserves the right to pursue any and all claims (equitable, legal, and criminal) against and remedies to which KCUMB may be entitled to from the account holder and/or the actual third party offender.

d. If any unlicensed Copyrighted Materials or other items in violation of this policy are found on KCUMB premises or installed on any such equipment, the offending materials will immediately be removed and destroyed without warning. Unauthorized equipment may be impounded and held pending disciplinary action against the responsible individual.

e. KCUMB may report to the appropriate law enforcement agencies any actions by account holders that are believed to be against the law.

9. AMENDMENTS

Policies are subject to review and revision as deemed necessary.

Users will be notified in writing, either by E-mail or by posted notices, when changes to this policy are adopted.

10. EXCEPTIONS

Any exceptions to this policy must be approved by the President and Chief Executive Officer.