COMPUTER RELATED ACCEPTABLE USE POLICY

Preamble

Those who do not abide by the policies listed below should expect suspension of computer privileges and referral to the Committee of Discipline. Offenders may also be subject to criminal prosecution under federal and state law, and should expect the Office of Computer and Information Services (OCIS) to pursue such action. As an example, under New Jersey law: "A person is guilty of a crime of the third degree if he purposely and knowingly accesses and recklessly alters, damages, destroys or obtains any data, database, computer, computer program, computer software, computer equipment, computer system or computer network [2C:20-26 para b.]."

The Office of Computer and Information Services should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of its computer system and networks. The user community is expected to cooperate with the Office of Computer and Information Services in its operation of computer systems and networks as well as in the investigation of misuse or abuse.

The computer resources and facilities of Kean University are solely for the use of Kean University (registered) students, faculty and staff.

Individuals using these computers systems without authority, or in excess of their authority, are subject to having all of their computer actives monitored and recorded by OCIS personal.

In the course of monitoring individuals improperly using a computer system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using any of the computer facilities at Kean University expressly consents to such monitoring and is advised that is such monitoring reveals possible evidence of criminal activity. OCIS personnel may provide the evidence of such monitoring to law enforcement officials. The legality of such monitoring is governed by 18 U.S. section 2510 et seq.

POLICIES

The Kean University policies on Computer and Information Resources include but are not limited to the list below:

1. You must not use a computer ID that was not assigned by the Kean Office of Computer and Information Services (OCIS). You may not try in any way to obtain a password for another's computer ID. You may not attempt to disguise the identity of the account or machine you are using.

2. You must not us the OCIS resources to gain unauthorized access to remoter computers. If you abuse the networks to which the University belongs or the computers at other sites connected to those networks, the University will treat this matter as an abuse of your Kean University computing privileges.

3. You must not deliberately perform an act that will impact the operation of computer, terminals, peripherals or networks. This includes, but is not limited to, tampering with the components of a local are network (LAN) or the high-speed backbone network, otherwise blocking communication lines or interfering with the operation readiness of a computer.

4. You must not run or install on any university computer system or network, or give to another, a program that could result in the eventual damage to a file or computer system and/or the reproduction of itself. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horse and worms.

5. You must not attempt to circumvent data protection schemes or uncover security loopholes.

6. You must abide by the terms and conditions of all software licensing agreements and copyright laws.

7. You must not deliberately perform acts that are wasteful of computing resources. These acts include but are not limited to: sending mass mailings or chain letters, obtaining unnecessary output, creating unnecessary multiple jobs or processes, or creating unnecessary network traffic.

8. The following types of information or software cannot be placed on any system on or off campus:
   That which infringes upon the rights of another person.
   That which is abusive, profane or sexually offensive to the average person.
   That which consists of information which may injure some else and/or lead to a lawsuit or criminal charges.
   Examples of these are: pirated software, destructive software, pornographic materials or libelous statements
   That which consists of any advertisements for commercial enterprises.

9. You must not harass other by sending annoying, threatening, libelous, or sexually, racially or religiously offensive messages.

10. You must not attempt to monitor another user's data communications, nor may you read, copy, change, or delete another user's file or software, without the permission of the owner.

11. You must not use any of the University's micro-computers, workstations or networks for other that a Kean University course, research project or departmental activity. These resources must not be used for personal gain unless in support of Kean University research of a departmental project.

12. You must not use a computer account for work not specifically authorized for that account. A University-funded account may not be used by its requestor for personal financial gain.

13. You must not play games using any of the University's computers or networks, unless for instructional purposes specifically assigned by a professor.

Kean University is a member of JvNCnet. JvNCnet provides Kean University with computer data connectivity to other member organizations and the Internet.

Examples of using JvNCnet are: sending electronic mail to a site off-campus, ftp and telnet sessions which leave Kean University's computing facilities and connect to computing facilities at another site.

When such activities are engaged, the JvNCnet acceptable use policy must be adhered to (attached).

JvNCnet ACCEPTABLE USE POLICY

This statement represents a guide to the acceptable use of JvNCnet use. In those cases where data communications are carried across other regional networks or the Internet, JvNCnet users are advised that acceptable use policies of those other networks apply and may limit use.

JvNCnet member organizations are expected to inform their users of both the JvNCnet and the NSFNET acceptable use policies.

1. JvNCnet Primary Goals

1.1 JvNCnet, the John von Neumann Computer Network, has been established to:

1) provide the highest quality and optimum access of networking services to the research and educational community of the United States and internationally,
2) offer network resources at the maximum level of cost-efficiency, and
3) promote and facilitate innovation and regional and national competitiveness.

These goals remain the standard for excellence in service and price and should not be comprised.

2. JvNCnet Acceptable Use Policy

2.1 All use of JvNCnet must be consistent with JvNCnet's primary goals.

2.2 It is not acceptable to use JvNCnet for illegal purposes.
2.3 It is not acceptable to use JvNCnet to transmit threatening, obscene or harassing materials.
2.4 It is not acceptable to use JvNCnet so as to interfere with or disrupt network users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms and viruses, and using the network to make unauthorized entry to any other machine accessible via the network.
2.5 It is assumed that information and resources accessible via JvNCnet are private to the individuals and organizations which own or hold rights to those resources and information unless specifically stated otherwise by the owners or holders of rights. It is therefore not acceptable for an individual to use JvNCnet to access information or resources unless permission to do so has been granted by the owners or holders of rights to those resources or information.

3. Violation of Policy

3.1 JvNCnet will review alleged violations of Acceptable Use Policy on a case-by-case basis. Clear violations of policy, which are not promptly remedied, be member organization may result in the termination of JvNCnet membership and network services to members.