Computer and Network Use Policy (CNUP)

Keene State College Policies and Procedures

Computer and Network Use Policy

Section Menu

Summary

The Information Technology Group (IT Group) has developed the Computer and Network Use Policy (CNUP). This policy is designed to guide individuals in the acceptable use of computers, information systems, and networks owned by Keene State College. More importantly, it is meant as an application of best practices to ensure availability, integrity, reliability, privacy, and confidentially of college owned computers, information systems, and networks. Keene State College makes computing and network resources available to faculty, staff, students, and the general public to support the educational, scholarship, research, and service mission of the college.

Scope

The Computer and Network Use Policy establishes policy for the use of Keene State College IT and network resources by authorized individuals. It is not designed to cover any situations and circumstances beyond this scope. CNUP supplements other more specifically targeted USNH and KSC policies. The function of this policy is to supplement other USNH and KSC policies and procedures. In cases where multiple policies and/or laws apply these other documents take precedence over CNUP and CNUP will supplement and support them. IT resource owners have the authority to manage their resources to best fit their needs and have the right to establish more restrictive policies and procedures governing their use.

User Responsibilities

The computing and network resources and services owned by Keene State College are limited and should be used wisely and carefully with consideration for the needs of others. By using computers, information systems, and networks owned by Keene State College, you assume personal responsibility for acceptable use and agree to comply with this policy, other applicable KSC and USNH policies, as well as applicable federal, state, and local laws and regulations. Failure to uphold CNUP acceptable uses constitutes a violation of this policy and may be subject to disciplinary procedures applicable to students, staff, and faculty.

Acceptable Uses

All users may…

- Use computing or network resources to support the educational, scholarship, research, and service mission of the college.
- Use computing or network resources for personal computing in compliance with this policy.
- Use only approved computing devices when connecting to the KSC network.

The following unacceptable uses apply to all uses of KSC technology resources. In the constantly changing world of information technology, it is impossible to enumerate all non-acceptable uses of KSC computers, information systems, and networks. All users are expected to conduct themselves within acceptable use boundaries and may not infringe on the following examples of unacceptable use.

Unacceptable Uses

All users may not…

- Use IT resources without proper authorization
- Attempt to monitor, intercept, analyze or modify network traffic or transactions not specifically addressed to your computer

- Harass, defame, intimidate or threaten anyone through the use of computing or network resources For sexual harassment issues, see KSC Discrimination & Discriminatory Harassment or the USNH Complaint & Grievance Policy.
- Use computing or network resources for profit, commercial use or for the purpose of lobbying that connotes College involvement or endorsement of any political candidate or ballot initiative
- Attempt to alter or reconfigure any KSC IT resources, e.g. network infrastructure, servers
- Attempt to obtain privileges for which you are not authorized
- Attempt to access, modify and/or delete another user's files, configuration or software without the expressed agreement of the owner
- Attempt to learn another user's password(s) or personal information
- Attempt to alter or obscure your identity or your computer's identity, including but not limited to IP Address and email address, while communicating on any network
- Interfere with or disrupt computer or network accounts, services or equipment of others including but not limited to consumption of excessive IT resources, (e.g. local area network or Internet bandwidth) through the propagation of worms or viruses or the inappropriate sending of broadcast messages to large number of hosts
- Interfere with or circumvent the IT Group's responsibilities and procedures
- Consume excessive IT resources, e.g. Local Area Network or Internet Bandwidth
- Abuse email privileges - see email policy
- Download and/or share copyrighted material for which you do not have the proper authorization
- Use unauthorized computing devices when connecting to the KSC network

Federal, State and Local Laws

All computer and network users are bound by federal, state, and local laws relating to harassment, copyright, security, and privacy relating to digital

media. The IT Group will cooperate fully, upon the advice of college legal counsel, with any local, state or federal officials investigating an alleged crime committed by an individual using Keene State College information technology resources. (more...)

Policy Enforcement

IT Group system administrators or network administrators may be required to investigate violations of this policy in order to ensure compliance. The IT Group may restrict the use of computers and networks when faced with evidence of violation of this policy or federal, state, or local laws. The IT Group is sensitive to these issues and will remain professional and conscientious while evaluating potential violations. When violations do occur, the IT Group follows the CNUP violation process.

IT Group Responsibilities

Beyond controlling access and protecting against unauthorized access and computer or network threats, the IT Group plays a proactive role in implementing and enforcing security or network procedures by following higher education best practices. Using hardware infrastructure and software tools, utilities and applications, the IT Group will maintain a network and computing environment enabling authorized campus users secure, reliable access to internal and external networking resources and applications.

Shared and limited technology resources often require prioritization, the IT Group will assign these priorities while managing the network:

1. Highest: Applications and services directly associated with the college mission. Applications and services supporting the college’s business functions.
2. Medium: Non-academic residential personal computing.
3. Lowest: Personal activity, not related to college business, academic and research functions.

The IT Group will respect and strive to ensure users’ privacy and intellectual

property while managing the computing and network infrastructure and information application transactions and data. The IT Group does not actively monitor network traffic or view content. However, while researching computing and/or network issues, system administrators or network administrators may need to use tools or utilities that expose content or users' internet habits. Under these circumstances, the IT Group will hold this information and knowledge in strictest confidence.

The IT Group will not intentionally release or expose a user's personal information, e.g. name, SSN, Date of birth, etc. to anyone external to KSC or to unauthorized KSC employees. There are many laws and regulations concerning this issue. (more.....)

At times the IT Group may need to reconfigure network and/or computing resources to mitigate situations that negatively impact access to IT resources. These actions include, but are not limited to, temporarily disabling access to an individual system, temporarily disabling access to/from a specific segment of the LAN or modifying priorities. Though rare and short in duration, these steps are necessary to isolate problems and enable a quick resolution.

To report a CNUP violation and/or suspected CNUP violations, contact the Security Manager.