Policy for Connecting Hardware to KSC Network

Keene State College Policies and Procedures

Policy for Connecting Network Devices to the KSC LAN

Section Menu

Background

Managing access to a Local Area Network is an important step to maintaining a secure, accessible and efficient network environment. Finding balance between ease of access to the network and responsible, secure network use is a difficult and ever changing challenge. New hardware and software technologies enable network users to connect devices that may negatively impact their and other user’s network service.

Network Services of Information Technology Group (ITG) is responsible for installing and maintaining the network infrastructure at KSC, enabling students, faculty and staff access to the KSC LAN. The infrastructure includes, but is not limited to, network equipment, switches, routers, hubs, inter/intra building cabling, wireless access points and individual jacks (LAN connections points).

Policy

Individual network jacks must be used to connect a single computing device to the network, such as printers and computers. Network Services is solely responsible for connection and management of network infrastructure devices or systems (switches, wireless and wired hubs, etc) on the KSC Local Area Network. Network infrastructure devices or systems are characterized as devices that enable more than one computing device to share an individual network jack. Connecting these devices is prohibited unless approved by Network Services.

Rationale

Currently, there are a number of such network devices that enable multiple devices access through a single network connection point. Wired switches and hubs and wireless access points are such devices.

These devices expose the network to utilization levels it was not designed to handle. Users of these unauthorized network devices possibly degrade network service for others while not receiving a reliable service themselves.

Wireless access points, while inexpensive, easy to install, setup and use pose another more serious issue. Access to a wireless access point, and therefore the LAN to which it is attached, can be made without a physical connection to the device. Anyone, whether an authorized KSC user or not, within broadcast distance can contact the wireless access point and gain access to the network. Without proper installation, setup and maintenance, this type of unauthorized access to the KSC LAN creates a serious security exposure and may potentially impact overall network performance.

Managing these types of devices connected to the network enables Network Services to maintain a consistent and reliable level of service and plan for future capacity.

Exceptions

Exceptions inevitably occur. Network Services will carefully review individual situations and address them fairly. Recommendations will be made to accommodate the user’s needs.

Enforcement

Network Services monitors network utilization with a variety of tools and procedures. Periodic monitoring can reveal an unauthorized network device connected to the LAN. The CNUP Violation process will be followed for these situations.

Consideration will be given to the impact on the users of the device as well as the impact on the network in general prior to taking any action. However, Network Services reserves the right to terminate the access to the LAN at the individual jack level for any of these devices if the impact poses a severe threat to security or service.