KSD Wireless Network Guidelines

The Kellogg School District Technology Department’s goal for wireless access in district facilities is to protect district technology resources, while providing the best user experience possible. The wireless network is not meant as a replacement for the wired network and is not to be used as a primary network connection. The wireless network is meant to extend the wired network for use in areas or on devices where wired network access is unavailable.

Support

The District Technology Department does not have the necessary resources to troubleshoot issues with devices not owned by the district. Users are responsible for configuring their personal devices to access the district wireless network. Wireless network access and device specific technical issues need to be resolved independently.

General Use

It is the intention of the Technology Department to provide reliability and privacy when using the wireless network. Wireless access points are installed to provide an acceptable level of service and availability. Wireless access points are a shared resource; as the number of users increases, the available bandwidth per user decreases. As such, everyone is asked to be considerate and refrain from using high bandwidth applications (ex. downloading large files, streaming music and video from the Internet).

Network reliability is determined by the level of user traffic and accessibility. In order to provide an acceptable level of reliability, bandwidth will be regulated according to user role and location.

KSD cannot guarantee the confidentiality of any information stored on any device connected to the KSD Wireless Network; therefore the wireless network should not be used to transmit critical or sensitive information (ex. social security and credit card numbers). Individuals assume full responsibility for their actions.

Access

Access to the “KSD_Guest” network will be subject to approval by the Technology Department and will be evaluated on a case by case basis. Unauthorized devices will be disabled upon discovery. Only KSD owned devices will be permitted on the “KSD_Wireless” network.

Access to the “KSD_Guest” network is provided for visitors to the district and district authorized personal devices for Internet access. Users will need to authenticate after joining the “KSD_Guest” by opening a browser to be directed to the login page and entering the username and password provided by the Technology Department. (subject to frequent change)

Access to the “KSD_Student” network is provided for authorized KSD Students only for Internet access. Users will need to authenticate after joining the “KSD_Student” by opening a browser to be directed to the login page and entering the username and password provided by the Technology Department.

Wireless connectivity is available wherever the “KSD_Wireless” and “KSD_Guest” signals are present.

By connecting to any of the KSD wireless networks you agree to the terms of use addressed in this guideline and the Computer and Network Services: Acceptable Internet Use Policy #667.

Expectations

Users with personal computers on the wireless network are expected to take reasonable precautions to ensure the security of their systems. Individuals are responsible for any violation of KSD guidelines or policies that occurs on their personal device.

The following guidelines further supplement the "Computer and Network Services: Acceptable Internet Use Policy #667."

1. The district is not responsible for lost, stolen or damaged devices.

2. Users may not extend or modify the network in any way. This includes adding access points and installing bridges, switches, hubs, or repeaters. The school district reserves the right to remove or disable any unauthorized access points.

3. Any attempt to break into or gain unauthorized access to any computer(s) or system(s) from a wireless connection is prohibited.

4. Running any unauthorized data packet collection programs on the wireless network is prohibited. Such practices are a violation of privacy and constitute the theft of user data.

5. The district reserves the right to limit bandwidth on a per-connection basis on the wireless network, as necessary, to ensure network reliability and fair sharing of network resources for all wireless users.

6. Any effort to circumvent the security systems designed to prevent unauthorized access to any Kellogg School District wireless network may result in the suspension of all access and may result in disciplinary action by the school district.

7. All devices connected to the KSD network, whether personally owned or owned by KSD, should be running anti-virus software with the latest virus updates, personal firewall, operating system updates, and patches.

8. Users must comply with all district policies, procedures, local, state, and federal laws pertaining to the security of sensitive and confidential data on district networks.

9. Personal devices connected to the wireless network may be monitored and reviewed at anytime by designated technology staff.

10. Personal web accounts visited while connected to the wireless network maybe monitored and reviewed at any time by designated technology staff.

11. Users must report violations of the wireless network guidelines and policies to the Technology Department.

For security and network maintenance purposes, the Technology Department may monitor individual equipment, or wireless network traffic. KSD reserves the right to audit networks and systems on a periodic basis to ensure compliance with this guideline.

The Technology Department has the authority to disconnect any device from the wireless network that violates the practices set forth in this policy or any other related policy. It is the responsibility of the user to be knowledgeable of the information set forth in district policy.