



TO: ALL STAFF

FROM: PAUL ALEX BRISENO, INSTRUCTIONAL TECHNOLOGY ADMINISTRATOR

RE: WIRELESS ACCESS POLICY

DATE: AUGUST 31, 2011

The Technology Department maintains strict standards for the deployment of wireless devices at the campus & department level in order to promote an efficient and secure wireless network. Wireless "access points" located in many areas of the campuses & departments allow configured computers equipped with wireless network cards to make wireless connections to the Internet. The following are policies and procedures for wireless equipment that will be connected to the district network. (Examples include: Palm PDA, Laptops, PC Tablets, etc.)

- Reasonable and reliable performance requires that we minimize interference by controlling the devices that provide or use wireless services. Distance from the access point, buildings or objects shielding the access point, signal interference, quality of equipment, battery power, and other factors may also impact performance.
- The wireless network's maximum data speed is less than 1/10th the speed of the campus wired network. High bandwidth applications like large file transfers and Microsoft Windows system updates are not supported.
- Broadcast frequencies used by the wireless network will be monitored on campuses and departments. Devices that interfere with the wireless network will be subject to restriction or removal. A first-time violation will result in the wired network port associated with an unauthorized device being immediately disabled without warning. An attempt will be made to identify the owner of the unauthorized device and inform him/her of the violation. Subsequent violations may result in more serious measures including the extended loss of access to the network.
- It is the responsibility of the user to maintain latest virus definitions, operating system service packs, and spyware removal software; failure to comply will result in removal of wireless access for that equipment.
- Only one active MAC address can be used by each user.
- South San ISD does not allow Network Sniffing software on the wireless network. Users found using this type of software will be removed from wireless network. Logs may be used for assessing network problems or identifying unauthorized or unacceptable use of the wireless network.
- Supported systems must meet district's minimum hardware and software requirements for access to the network. Off-campus connections to the wireless network are not supported.
- Access to the district's wireless network is only permitted after submission of the Wireless Access Policy Form.

After turning in the form to Technology, a 24-hour minimum turnaround time will be applied to the request. Notification for completion will be done so via e-mail and phone call.



Wireless Access Policy Form

Campus/Department/Company: _____ Room/Office : _____

Employee Name: _____ Title/Position: _____

MAC Address: _____ Computer/Device Name: _____

Employee Email: _____ Employee Phone#: _____

Kaspersky Agent Installed: Yes Notes: _____

The Kaspersky Agent will be installed on your personal wireless device giving us the ability to track your device on the South San Antonio ISD network. This agent will only give us tracking capabilities on the district network; it does not allow us to track you on your home network or wireless access card.

Any user found to have violated the Wireless Access Policy may be subject to loss of certain privileges or services, including but not necessarily limited to loss of wireless services. The Technology Department will monitor the local wireless network for unauthorized access points and other unauthorized wireless network devices that pose security risks.

Employee Signature

Date

All items must be completed fully before request will be honored.