Mobile Device Usage Guidelines for Students

Purpose

The purpose of this document is to define standards, procedures, and restrictions for students using district owned mobile devices from both inside and outside the district's computer network. These guidelines are an addition to the current Acceptable Use Policy found in the student handbook. The overriding goal of the information on this document is to protect Southwest ISD's students by providing a technology environment that is safe and educational and to ensure the integrity of technology-based resources such as district data, computer systems, networks, and databases. Therefore, all students using district provided mobile device-based technology must adhere to district-defined processes for doing so.

Scope

Access to Southwest ISD enterprise network resources is a privilege, not a right. Consequently, being a student at Southwest ISD does not automatically guarantee the granting of these privileges. Addition of new hardware, software, and/or related components to provide additional mobile device-related connectivity within district facilities will be managed by the Information Technology (IT) department. Non-sanctioned installations of mobile device-related hardware, software, and/or related components, or to gain access to district computing resources of which the user has not been provided access, are strictly forbidden. This document is complementary to any previously implemented policies dealing specifically with network access, wireless access, and remote access to the enterprise network.

Supported Technology

All mobile devices and related connectivity points within the district firewall will be centrally managed by Southwest ISD's IT department and will utilize encryption and strong authentication measures. Although IT is not able to manage the public network to which wireless-enabled mobile devices and smart phones initially connect, end-users are expected to adhere to the same security protocols while utilizing this equipment. Changing of district configuration and settings of any district owned device is prohibited. A student is free to enable the device to connect to a home network, but may not remove the existing Southwest ISD network and settings. All networks added to the device by students will need to have specific settings configured in order to help block access to inappropriate material. Please refer to the attached instructions on how to configure these settings.

It is imperative that any district provided mobile device used to connect to the Internet be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

- Remote users using non-district network infrastructure to gain access to district resources via their mobile device must employ a district-approved personal firewall, or any other security measure deemed necessary by the IT department. See attached instructions for setting up a home network to access the Internet via the district's web filter.

- The mobile device-based wireless access user also agrees to and accepts that his or her access and/or connection to Southwest ISD's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with intranet computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

- Any questions relating to this policy should be directed to Joe Martinez in IT, at 210-622-4395 or jomartinez@swisd.net.

- IT reserves the right to turn off without notice any access port to the network that puts the district's systems, data, users, and clients at risk.