School District of Poynette

Wireless Network & Device Policy

I. Purpose

The effective management of information technology resources is important to the success of student learning. Wireless networks require increased cooperation and coordination among stakeholders to maximize the technology's benefits to students, faculty and district staff. This document outlines the policies for employing wireless technologies and assigns responsibilities for the deployment of wireless services. This policy is subject to change as new technologies and processes emerge.

The School District of Poynette appreciates and welcomes the fact that staff and students are willing to bring personally owned computer equipment into the schools to be used for assignments and educational purposes. This policy also applies to any wireless use of such devices on district or school property, both inside and outside of buildings. The following items must be addressed when connecting any item to the district wireless network: security, network stability, liability for personal property, virus protection, repairs, filtering and upgrades.

II. Scope

The policy applies to all wireless network devices using the School District of Poynette's internet service provider space, as well as all users of such devices and governs all connections to the district's network backbone and frequency.

III. Authority

Improperly installed and unsecured access points can interfere with wireless network function and be readily exploited to gain unauthorized access to the network. It is critical the District Network Administrator manage wireless access points and its users to ensure the best possible wireless network security and function.

IV. Policy

A. All wireless equipment and users of wireless access must follow the policies outlined in the district's Acceptable Use Policy.

B. Wireless access points shall require user authentication at the access point before granting access to service. Wireless network interfaces and end-user devices shall support such authentication to access wireless networks.

C. All internet traffic must go through the district proxy or filtering system.

D. Users of the wireless network acknowledge that any device employed on the district's wireless network will be viewable and filtered according to local, state and federal policies while accessing the wireless infrastructure.

E. The district retains the right to determine where and when privately owned equipment may be attached to the network.

F. Staff and students are not allowed to attach to any other wireless networks that may be unsecured in the neighborhood of the schools. Failure to comply with this policy will result in the termination of right to use a wireless device in the schools.

G. Privately owned devices must be running current virus detection software prior to accessing the network or internet.

H. Students and staff who bring in privately owned equipment to school are personally responsible for the equipment as well as all security, maintenance and repairs.
I. Users are responsible for obtaining a valid network ID account and password.
J. Users are responsible for their personal equipment. The School District of Poynette is not responsible for lost, stolen or broken personal devices used on the district's wireless network.

V. The following special conditions apply for privately owned technologies being used in district facilities and on district property. The School District of Poynette reserves the right to:

A. Monitor all activity
B. Make determinations on whether specific uses of the technologies are consistent with the district's Acceptable Use Policy and other relevant district policies.
C. Log network use.
D. Deem what is appropriate use.
F. Remove the user's access to the network and/or suspend the right to use the privately owned technology in district facilities, if at any time it is determined that the user is engaged in unauthorized activity or violating the Acceptable Use Policy.

VI. Consequence of Non-Compliance
Not following this wireless network policy will result in an unreliable and unsecured campus network, prone to interference and abuse. Violations of this policy will result in the loss of network access, disciplinary action or other consequences as deemed appropriate by district administration.