Pottsville School District
Wifi Security Policy

Pottsville Public Schools maintains a wireless network among all campuses and buildings including the following: Elementary, Middle Grades, Junior High, High School, Central offices, Agriculture building, PMG gym, and HS credit recovery lab. All users of the district wireless network are subject to acceptable use policies that are signed and dated each school year. Wireless networks are not used for APSCN, Eschool or Nutrikids systems, these services use wired connections.

SWOW- SSID utilizes 802.1x security and is uses enabled Active Directory accounts. Radius server is used to authenticate valid faculty and staff active directory accounts. Active directory accounts are managed by network administrator. Student active directory accounts will not authenticate through the radius server. Student use mobile devices that use AD will connected by technology department personnel.

SWOW-C - SSID will utilize WPA2 security key managed in the pottsvilleschools.org domain will be used for all chromebooks and is be changed every 90 days. This SSID will have a dedicated VLan and the Google admins only will have access to this security key information.

SWOW (guest)- SSID will utilize WPA2 security with a pre-shared key changed at a minimum of every 30 days or more often as needed for security measures. Guests or faculty/staff personal devices will utilize this network with proper documentation of acceptable use policies. This SSID will have a dedicated Vlan.

SWOW (temp)- SSID will use WPA2 security and a pre-shared key, which is changed every 30 days. This SSID will used for devices that are not supported by the radius server and will only be used by the technology department.

All students (K-12) will be instructed annually in an age appropriate manner regarding acceptable online behaviors, cyber-bullying, social networking, chat rooms, and appropriate responses to online etiquette by school faculty each year. All faculty and staff receive information security training annually.

The district will change SSID pre-shared key and the documentation and dates of these changes will be maintained by network admin. This document will be shared only with appropriate administrators as needed for auditing purposes.

The district has changed the default passwords for all access points and will consistently change the default passwords when new access points are acquired.

Security measures include steps to mitigate wireless network risks. These include: Scanning for rogue access points and ad hoc networks regularly and disabling them. Updating device inventory regularly to maintain accurate records of devices accesses wifi network. Installing security patches and firmware on access points monthly and uses a strong admin password.