Employee-Owned Device Wireless Network Access Guidelines –School Year

The Red Hook Central School District maintains a wireless network for the purposes of augmenting its wired network for instructional and administrative use. Employees wishing to connect personally-owned devices to the school's wireless network should understand the following:

1. All of the terms stated in the district's existing Acceptable Use Policy also apply to the use of personal devices on the district wireless network.
2. Connection of personal devices to the network is provided as a convenience to aid instructional activities. Acceptable devices include laptops, tablets and smartphones, but not devices such as printers, game systems or video players like a Roku, AppleTV or Chromecast. Unauthorized devices connected to the network by employees will be removed from the network.
3. The district is not responsible for loss of or damage to personal computing devices and other equipment connected to the wireless network.
4. You are responsible for all activity associated with your account. Infractions will result in an account being suspended at the discretion of the Superintendent and/or Director of Technology. Repeated or egregious infractions may result in permanent revocation of personal-device wireless network access privileges.
5. Do not share your wireless account credentials with anyone. Sharing of personal-device account credentials with others (students, spouses, children, etc.) will result in wireless access revocation.
6. Devices must be compatible with all network requirements. Network upgrades in our buildings may result in personal-device connection incompatibilities. The district's network will not be reconfigured nor downgraded to accommodate incompatible devices.
7. Support from the district's technology department for personal devices will be limited to "over-the-shoulder" assistance ONLY for the purpose of connecting to the wireless network.
8. Any employee's personally-owned device detected as being compromised or otherwise causing trouble on the network will be disconnected from the network. Windows computers in particular must be running some form of active antivirus or preferably a more comprehensive malware protection suite.
9. Personal devices will not be allowed to connect to any internal district systems except for email and eventually SAFARI Montage. Printing, access to network file shares (My Documents), etc. will not be permitted from personally-owned devices across the wireless network.
10. District-owned software will not be installed on personally-owned devices.
11. Use of Internet-based streaming media and other high-bandwidth activities is prohibited to ensure general Internet performance. These services include, but are not limited to: Netflix, Hulu, HBO GO, ESPN Now, Pandora, Spotify and iTunes Radio.
12. The connection speeds on the personal-device portion of the network may be reduced in times of heavy use to ensure a minimum performance level of the instructional network.

Employees wishing to receive a personal wireless key passcode must return a signed copy of this form to Michelle Lowney. The passcode will be sent via an email. Please keep a copy of these guidelines handy for future reference.

Employee First and Last Name (PRINTED): _____

Employee Location: _____ Date: _____

Employee Signature: _____

Employee email: _____