LAWRENCE PUBLIC SCHOOLS
Information System & Technology Department

help@lawrence.k12.ma.us 70-71 N. Parish Rd., Lawrence, MA 01843 (A217) Ext: 978-975-5952 Int:25368

# Wireless Usage

*Overview:*

It is the intention of the IS&T Department of Lawrence Public Schools to provide a high level of reliability and security when using the wireless network. Wireless Access Points provide shared bandwidth and so as the number of users increases the available bandwidth per user decreases. As such, please show consideration for other users and refrain from running high bandwidth applications and operations such as downloading large music files and video from the Internet. Network reliability is determined by the level of user traffic and accessibility. Wireless networking is to be considered supplemental access to the LPS network. Wired access is still the preferred way for connectivity.

*Note:*

Connecting to a LPS printer from a personal mobile device is a case by case basis. It is highly recommended that if you want to print, copy the file to a thumb drive or email it to yourself or save it to your Google Drive/Microsoft Onedrive and open on the school issued computer to print. Please note that it should be school-related material only. There are too many different types of devices and setups that we do not have specific instructions for everything and some may require more customization than others.

Any LPS issued laptop regardless of Operating System should automatically connect to LPS-Wireless Network where visible. If you cannot connect to the wireless from a LPS issued laptop please contact the Help Desk.

The majority of wireless home printers, smart devices and projectors will not work with WPA2-Enterprise due to the security level of our Enterprise Network.

*Requirements:*

To connect to the wireless access points, you need a wireless network adapter capable of supporting at least 802.11g. 802.11n adapters will work because they are backwards compatible. 802.11b will not work.

The latest Microsoft Windows Updates or Apple Updates.

The latest anti-virus definitions (Anti-virus software is required on all laptops connected to the LPS wireless network) Operating System of Windows Vista or newer and up or Mac 10.4 or newer.

Ability to follow the instructions provided to make sure their computer has the correct settings and necessary hardware.

### *Security and Monitoring:*

Wireless Internet Access connections are not secure. Cautious and informed users should not transmit personal information (credit card numbers, passwords and any other sensitive information) while using any wireless “hot spot” or unsecured network. Please take appropriate precautions when using this service.

As with most wireless "hot spots," there can be non-trustworthy third parties between the user and anybody with whom the user communicates. Any information being sent or received could potentially be intercepted by another wireless user.

All installed wireless access points and antennas are the property of LPS. Do not tamper with, adjust, abuse, repair, or otherwise touch these access points and their antennas.

We reserve the right to monitor and log communications on a per connection basis to ensure proper usage of network resources.

### *Risk of Non Compliance:*

If a virus is found on our network that is originating from your PC, we will terminate your wireless access without notification. If you find that you can no longer connect to the wireless, please contact the Help Desk. It is up to you to remove the virus.

If anyone is found using your account, then the account will be disabled. Sharing your account information is a security risk and is prohibited.

If you are found using someone else’s wireless account you will not be allowed back on the wireless network. Network access may be suspended for a specified period of time until the situation is rectified.

### *Proper Computing Habits:*

When submitting a username and password on a web site, make sure it is SSL encrypted. SSL, or Secure Socket Layer is an encryption protocol drafted by the Netscape Communications Corporation to protect data being sent back and forth between a client user and a web site. For example, the PowerSchool is SSL encrypted. We recommend that wireless network users do not submit important information such as passwords and credit card numbers on a web site form unless the web site form uses SSL encryption.

Turn off any drive sharing on a computer using the wireless network. If sharing of drives and files is necessary, use a password to protect the drive shares.

These same habits not only apply to wireless networks, but should also be considered when using anything on the network/internet.

Run updates and virus scans weekly.