Wireless Access Policy

Lawrence Public School·255 Essex Street ·Post Office Box 1498 Lawrence, MA 01842

This Policy applies to:

Any and all users of the LPS wireless network, this includes, but is not limited to, all employees, and guests.

Overview:

Due to the increasing demands for wireless access to LPS network, this policy acts as an addendum to the General Acceptable Use Police by including specific information regarding the use of wireless networking and Internet access. Please note that many items listed here may already be in the General Acceptable Use Policy for the redundant purposes. If you have questions or comments, please feel free to let us know. This policy is designed to protect wireless users and to prevent inappropriate use of wireless network access that may expose LPS to multiple risks including viruses, network attacks and various administrative and legal issues.

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 increase 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.

All general policies contained within the current Acceptable Use Policy of Technology for Lawrence Public Schools also apply to all wireless network users.

As the deployment and usage of the LPS wireless network progresses, we reserve the right to adjust the access and usage policies, and guidelines as necessary, for the sole benefit of LPS wireless users to provide a safe and reliable computing environment and ensure high quality secured services. It is the responsibility of all persons using the Wireless Internet Access network to be familiar with this policy and the Internet Policy.

Note

Connecting to a LPS printer to a personal device is not allowed. If you want to print, copy the file to a thumb drive or email it to yourself to open on the school issued computer to print. Please note that it should be school related material only.

Any LPS issued Laptop regardless of Operating System and Wireless location that has been refurbished over the summer of 2011 should automatically connect at these locations. If you cannot connect to the wireless from a School Issued Laptop please contact the help desk with your computer name, IP/VNC and the Windows username that you are using.

Please have it plugged into the network when giving us the VNC.

At the end of every school year the Wireless Access list will be purged and reinstated after reapplication the following school year. This helps us ensure that you are in the proper access groups with the correct rights. Guest ID's will be created as requested and will remain available for the time required. Anyone needing a wireless ID or having problems connecting to the wireless network should contact the Help desk for support during the hours of Monday-Friday 8AM–4:30PM. Or call us at 978-975-5952 or Ext. 25368 from any district phone. Please give us prior notification if you are requesting temporary access for a guest.

Requirements

Understanding and agreement of the Wireless access policy

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.

Procedures

After reading the policy and signing the form you will be given online instructions on how to connect to the LPS wireless network after you turn it in.

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.

Acceptable Wireless Use

Wireless access is limited to web browsing and email access. The filter level will be the same as a student PC. If you would like a website to be unblocked, please send a request to the help desk.

Unacceptable Wireless Use

Downloading copyrighted materials or items like music, videos, games, programs, etc., from file sharing sites or applications such as Itunes, Kazaa, Napster, eMule, Limewire, bit torrent, or any other P2P software

Online gambling or gaming

Viewing or downloading pornography

Running servers, daemons, or proxy services on the wireless network is prohibited. Any other such arrangements to enable more than one computer to access the network via your connection is prohibited, each use is limited to one connection.

Users may not use the network to access computer files not belonging to them.

Any type of service which might negatively impact the overall performance of the network (RF jamming, DoS attack) using the wireless network will not be tolerated

Running any unauthorized data packet collection programs on the wireless network to intercept or attempt to intercept other wireless transmissions is prohibited. Practices such as these are a violation of privacy and constitute as theft of user data and is punishable by law.

Mass emailing, or spamming, will not be tolerated on the wireless network. Such practices are an unnecessary use of bandwidth resources and are socially improper.

Harass, cause annoyance, nuisance or

inconvenience to others. Any other type of

illegal activity

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.

If anyone is found using your account, then the account will be disabled and you will be contacted. 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 for a certain amount of time depending on the infraction.

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 standard wired network connections as well.

Run running updates and virus scans weekly

Conclusion

Use of the Wireless Internet Access network is entirely at the risk of the user. LPS disclaims any and all liability for loss of confidential information or damages resulting from that loss, or any and all damages resulting from use of the wireless network.

LPS will not be responsible for any personal information (e.g. credit card) that is compromised, or for any damage caused to your hardware or software due to electrical surges, security issues or consequences caused by viruses or hacking.

Laptops and other devices should never be left unattended, even for brief periods of time. We assume no responsibility for damage, theft, or loss of any kind to a user's equipment, software, data files or other personal property brought into or used at the District's facilities.

All Unauthorized connections to the LPS network will be banned if they do not have permission from the LPS IS&T Department. Please help keep our network safe!