WiFi Policy

The Carnegie Public Library of Steuben County provides public wireless access to the Internet. Patrons must provide their own computer or device to connect to the wireless hotspots. Limited technical support is available to users. Users of the wireless hotspots are subject to the terms of this policy, however a library card is not required to access the wireless network.

The library cannot guarantee the privacy or safety of data and communications while using either wired or wireless service. Patrons need to be aware that wireless networks are inherently insecure and it is strongly recommended that they secure their computers with firewall software and data encryption.

While the library uses filtering software to attempt to prevent direct access to materials that would generally be unacceptable in a public library, it is technically impossible to prevent access to all objectionable resources.

No password is required to access the wireless network. The network's SSID, or name, is CarnegieLibrary. Remote printing is available. Library staff can provide general information or handouts for connecting your device to the network, but cannot troubleshoot problems related to your wireless device or assist in making changes to your device's network settings and/or hardware configuration.

WIFI FAQ and Troubleshooting

Q: Where is wireless access available?

Public Internet Access is accessible from all of the public areas of the library.

Q: What kind of equipment do I need to access the service?

A wireless network-enabled portable computer or mobile device.

Q: Will the information on my laptop be safe from hackers?

The security of your laptop will be your responsibility.

We recommend that you keep up to date with security patches that are released from various software vendors.

You may also wish to run one of the firewall packages obtainable from the internet. You may also wish to install an anti-virus software package to protect yourself from the many varied forms of computer virus. The Library does not provide anti-virus software – this is your responsibility.

Q. Is the wireless network secure from someone "eavesdropping"?

The security of your laptop will be your responsibility. A VPN (virtual private network) app can help keep your information private when using public WiFi.

We run the wireless network in what is referred to as "Open Mode". We do not use any encryption between the wireless Access Point and your wireless device. Anyone using "wireless packet sniffing" software may be able to "see" what you are viewing or sending. What this means is if you are working on a web-based email client or even client-based email and you don't want someone to see the content you either need some form of encryption for your client-based email or use SSL when connected to a web-based email server. We do not provide any form of encryption software for your use.

It is your responsibility to protect any "sensitive" information you may send or receive through our system.

Think of the wireless system as being similar to a "party line" where someone could "listen in" on the conversation. If you are accessing online banking services make sure it is running in encrypted mode (the padlock at the bottom of the browser is in the "locked" position.) Most all online banking services run SSL encryption as the default but it is better to be safe than to find out your information was compromised because of a lack of security by a financial institution or otherwise.

Q. Will I be able to print a document while I'm connected to the network from my laptop or device?

Remote printing is available. Ask the staff for assistance.