

Town of Florida Broadband Committee

Town of Florida Hotspot

Our beta test network contains a wireless hotspot for use by our community. Our hotspot is located at Abbott Memorial School at 56 North County Road. The school computer lab will be open to Town of Florida residents during selected after school hours, and will likely be coordinated with the library's after school open hours (currently Tuesdays and Thursdays from 5 – 8 pm). Additional computer lab hours **may** be available by calling the school ahead of time to make arrangements. For more information on library and computer lab hours, call Abbott Memorial School at (413) 664-6023 or 664-2078.

In addition, Town residents may park in the school parking lot and use their own laptops to connect to FloridaBconnect during these hours:

- 4 pm – 11 pm Monday – Friday
- 8 am – 11 pm Saturdays & Sundays

Parking for after school events takes priority, and during these occasions, wireless broadband users are asked to be considerate.

This privilege is for Town of Florida residents only, and will be extended as long as no issues arise (vandalism or littering, for example). In addition, the school will not be responsible for monitoring the parking lot, so their parent or other responsible adult must supervise children.

User Guidelines

We ask that you please respect the following user guidelines when utilizing the hotspot. We reserve the right to deny users access to the hotspot if these user guidelines are violated.

- All communication using the Town of Florida hotspot must be appropriate, ethical, professional, and lawful.
- Unauthorized peer-to-peer file sharing of copyrighted works, including music, pictures, movies, games, and other published copyrighted materials are prohibited.
- All users of the Town of Florida's hotspot should refrain from littering.

Hotspot Security

Our Beta Test hotspot is "open," or unencrypted, so that new users can connect without having to know a password. Sending unencrypted data through a wireless system leaves it vulnerable to interception. Wi-Fi eavesdroppers can - and do - use readily available tools to access data passing over a wireless network.

We suggest you only use public hotspots for surfing the Internet. We suggest you do not conduct private or sensitive work, such as financial transactions, over our public wireless connection.

If you do have to conduct transactions at our public hotspot, enter passwords only into websites that include an SSL key. This is a symbol that looks like a key and is located on the lower right-hand corner of your web browser. It ensures that the website you are transacting with is legitimate and that data sent between you and it is encrypted with the current industry standard.