

SUBJECT: WIRELESS INTERNET ACCESS

EFFECTIVE: MARCH 1, 2016

SUPERSEDES: 8/2010

1. PURPOSE:

- A. To provide library customers with wireless Internet access within the Tampa-Hillsborough County Public Library (the Library) facilities in order to expand the capacity of the library to make available subscription and free Internet-based resources to customers using their own laptop computers or other mobile devices.
- B. To provide wireless Internet access for use in conducting public computer programming and training on the use of subscription and free Internet-based resources.

2. POLICY:

- A. Wireless access is provided in accordance with current industry standards.
- B. Wireless access is provided with the same access and content restrictions and limitations as library-provided Internet access computers.
- C. Hillsborough County Information & Innovation Office (IIO) is responsible for the installation and maintenance of the wireless network.
- D. Security is not guaranteed or implied. Users are expected to provide for their own security while connected to the library's wireless network.
- E. Users are expected to adhere to existing [LS502, Library Code of Conduct](#) and [LS306, Access to Electronic Resources \(Internet Use\)](#), policies while utilizing the library's wireless network.
- F. Basic troubleshooting is expected from staff at all levels to provide optimal service resolution.

3. PROCEDURE:

- A. The library's wireless network is built around current wireless standards and guidelines provided by the Information & Innovation Office (IIO).
 - (1) 802.11n with backwards compatibility to 802.11a, 802.11b, and 802.11g
 - (2) The library openly broadcasts its service set identifier (SSID) as "HCPLC". Authentication is required on the hidden HCPLC-Mobile SSID and WPA2 is used to encrypt from the device to the access point.
- B. The limitations and restrictions placed on the library's wireless network access include:
 - (1) Software to monitor or restrict the use or access to applications, the network, or the Internet.
 - (2) Restrictions regarding access via specific ports, which may affect public use of the Internet or our wireless infrastructure. These blocks include, but may not be

limited to, SMTP and other non-port 80 traffic.

- (3) Content filtering software to prevent access to legally proscribed content and services (i.e., obscenity).
- C. Wireless access points are regularly maintained to ensure appropriate hardware firmware and software updates are applied. These are handled and coordinated by the IIO.
- D. While utilizing the library's wireless network, security is the customer's responsibility. To the extent possible, through firewall and content management protections, a base level of security is achieved. There is no security between the customer's equipment and the wireless access point (WAP).
 - (1) Users are responsible for installing wireless security programs on their personal laptops or wireless device before connecting to the library's wireless network.
 - (2) The library is not responsible for damage that occurs to customer provided hardware or software while utilizing the library's wireless network.
- E. For guidelines on the misuse of the library's wireless Internet access, see [LS306, Access to Electronic Resources](#).
- F. Assistance does not extend to operation of advanced configuration for, or instruction on, software installed on the customer's wireless enabled device. Troubleshooting technology hardware, or the configurations, on a wireless enabled device is not supported. Staff can readily assist wireless customers by utilizing the information provided on the [library's website](#).

4. AUTHORITY:

Pursuant to Section 5(1) of [Chapter 84-443, Laws of Florida](#), the Library Board has the duty and the responsibility, among others, to serve in a recommending capacity to the Director of Library Services and to the County Administrator in respect to all matters pertaining to the public library.

Approved:

Andrew Breidenbaugh, Director