SCLS as ISP

Last updated 02/12/2020

In the past, the SCLS network was available exclusively for use by SCLS-supported computers.

With the approval of the SCLS Technology Committee, SCLS has added an "SCLS as ISP" option which is designed to allow libraries to connect non-SCLS supported devices into the SCLS network. In this scenario, SCLS will act as the Internet Service Provider (ISP) only, providing the library-supported device with access to the internet and select network resources. It will be the responsibility of the library to configure and support devices on SCLS as ISP connections.

If libraries wish to use the SCLS network as ISP, the director must sign a Memorandum of Understanding as there is some risk associated with allowing non–SCLS supported PCs to access the SCLS network.

Libraries are welcome to use library-supported devices on the public "Library-Wireless" signal, but the devices will not have access to network printers or other resources on the SCLS network.

Options for "SCLS as ISP"

Wired

Examples: HVAC PCs, security systems, Macs

With a wired connection to the SCLS network, libraries can configure library-supported devices to access:

- The Internet
- Network printers on the SCLS network
- File shares hosted by SCLS network staff PCs

Wireless

Examples: wireless security cameras, wireless digital displays, library-owned MacBooks

With a connection to the "SCLS as ISP" wireless signal, libraries can configure library-owned devices to access:

- The Internet
- Network printers on the SCLS network
- Devices on a wired "SCLS as ISP" connection
- Other library-owned devices on the same "SCLS as ISP" wireless signal

**Risks*

By adding library-supported devices to the SCLS network and giving them access to other SCLS-supported library staff PCs, the library assumes any risk that may be introduced by these library-supported devices.

For any library-supported PCs used by staff, SCLS strongly recommends that the library:

- install anti-virus software and keep it updated
- keep software programs updated with the latest patches
- install security updates for the operating system
- only use administrator accounts for installing software – never for browsing the internet

If a library-supported device introduces a virus to the SCLS network or SCLS-supported PCs, SCLS reserves the right to remove the device's network access. Any cleanup of SCLS-supported PCs resulting from the virus infection will be done as SCLS' time permits.

If SCLSasISP is used to connect critical systems to the network, South Central Library System is not liable for any damages or potential outcomes due to a lack of device function as a result of internal or external network service outages. SCLS makes no guarantees about network uptime or service availability. Critical systems include but are not limited to emergency service messaging systems, fire alarms, and security systems.