SPOKANE COUNTY LIBRARY DISTRICT

**POLICY: Computer, Wireless Network and Internet Use**
APPROVAL DATE: September 18, 2012
REVISION DATE: January 17, 2023

RELATED POLICIES:
Children's Safety in Libraries
Collection Development
Code of Conduct
Customer Privileges and Responsibilities
Social Media

STATUTORY REFERENCE: RCW 9.68.130

**Purpose:**
To define the conditions and responsibilities associated with use of Spokane County Library District ("District") provided public access computers, internet access, and wireless hotspots in Spokane County Library District facilities and remotely.

**Definitions:**
Compromising Computer or Network Security: Conducting activities that will alter, damage, disable, vandalize, or otherwise harm computer equipment, hardware, software or networks.

District Network and Hardware: Includes all District provided hardware (such as computers and wireless hotspots), network access, and internet access.

Filter Categories: Groupings of online information to which access can be blocked.
Terminology used to describe filter categories are set by the provider(s) of filtering software.

Illegal Activities: Activities in violation of federal, state, or local law.

Sexually Explicit Material: Images which fall under the definitions of sexually explicit material as stated in Washington Statute, RCW 9.68.130(2).

**Background:**
Spokane County Library District (the District) makes Internet resources, together with a collection of physical library materials and access to licensed electronic resources, available to customers in support of the District's mission.

The District offers materials and information in a variety of formats and media, with selection guided by the Collection Development policy. Internet resources enhance the collection in size, depth, and breadth. The District provides public computers with standard computer software that can be used to access the Internet. In addition, customers may use their own devices to access the Internet on the library's public wireless network. In compliance with the Children's Internet Protection Act (CIPA) and subsequent court rulings, the District employs Internet filtering software and other technology protection measures on all District public computers and the District's public wireless network.

**GENERAL POLICY:**
The District prohibits the following while using any District resource, including District Network and Hardware (District public computers, the District's public wireless network, and District-provided wireless hotspots): engaging in illegal activities; accessing, viewing, or printing any illegal, obscene, or sexually explicit material, or engaging in activities that compromise computer or network security.

**Filtering**
For all District public computers and the District's public wireless network, the District utilizes filtering technology as required by the Children's Internet Protection Act (CIPA) which mandates that any public library using federal funding must filter Internet access to visual depictions that are (a) obscene; (b) child pornography; or (c) harmful to minors (as defined in the United States Code[1] and case law) for any person under the age of 17 years. Just as with the physical collection, not all Internet sites are suitable for all ages. Therefore, the District provides two levels of filtering: "basic" and "enhanced."

All customer accounts, all library computers, and the public wireless network are filtered at the "basic" level. The following categories of information are blocked with "basic" filtering: Illegal, Compromising Computer or Network Security, Sexually Explicit Material.

Additionally, all accounts for customers under the age of 13, and library computers located in the children's area, are set to the "enhanced" filtering level. In compliance with CIPA and guided by the Collection Development policy and related procedures, the "enhanced" filtering level blocks all of the same categories of information that are blocked with "basic" filtering, as well as other categories, as determined by District staff, to be for adult audiences only.

For both the "basic" and "enhanced" filtering levels, the District will utilize categories provided by the filtering software provider that best match the District's intentions.

**Requests to "block" or "unblock" an Internet site**
No filter or technology is 100% effective and may still allow access to information or sites that are objectionable or potentially harmful. Conversely, filters may inadvertently block sites that do not fall within the categories defined above.

A customer may request that an Internet site be blocked or unblocked for "bona fide research or other lawful purposes"[2], by completing an Internet site review form or by contacting library staff. The site will be reviewed in a timely manner. Decisions about whether to block or unblock a site will be made in accordance with District guidelines within three (3) business days.

**Computer and Internet Safety**
The District respects the rights and responsibilities of parents or guardians in determining and monitoring the use of the Internet by their children under the age of 18. The District advises parents/guardians that it cannot assure children's safety and security while using the Internet in the library. When children use social networks, electronic mail, chat and other forms of direct electronic communication, the District cannot protect against unauthorized access, including "hacking," and other unlawful online activities. Furthermore, the District cannot protect against unauthorized disclosure, use and dissemination of personal identification information regarding children if children provide such information while using the Internet.

It is the responsibility of parents or legal guardians to monitor Internet use of their minor children.

**Network and Computer Security**
The District employs measures designed to prevent access to sites or functions that would compromise District computer or network security or would alter, damage, disable, vandalize, or otherwise harm computer equipment, hardware, software or networks. District computers provide basic software and the ability to transfer content to mobile storage. The District is not responsible for data that may be lost or damaged while using library computers.

---

[1] The Children's Internet Protection Act (CIPA) provides United States Code citations for the definitions of "obscene" (18 U.S.C. § 1460) and "child pornography" (18 U.S.C. § 2256). The Act itself defines "harmful to minors" in Section 1703 (b)(2). Full text of CIPA from US Government Printing Office: http://www.gpo.gov/fdsys/pkg/PLAW-106publ554/pdf/PLAW-106publ554.pdf
[2] Federal Communications Commission's Children's Internet Protection Act (CIPA) Guide: http://www.fcc.gov/guides/childrens-internet-protection-act

The District's public wireless network is an open, unsecured network. The District advises users not to transmit personal information (e.g., credit card numbers, passwords, and any other sensitive information) while using any wireless access point. Furthermore, the District advises public wireless network users to take appropriate precautions when using this service, and to have up-to-date virus protection on their devices.

The District is not responsible for any information that is compromised or for any damage caused to hardware or software due to security issues.

For security and network maintenance purposes, the District may monitor individual equipment or network traffic on all District public computers and the District's public wireless network at any time. The District has the authority to disconnect any device from the District's public wireless network for suspected and/or actual violation of this policy or any other related policy.

When using District Network and Hardware, individuals are expected to use the Internet in a manner consistent with the purpose of the library and with respect and consideration for other customers.

**Wireless Hotspots**
The District may offer wireless hotspots or other similar devices that customers can borrow to access the internet via a third-party vendor. While the District provides the devices, the network over which customers can access the internet using these devices is provided and managed by the third-party vendor. The District requires that these devices be borrowed by District residents 18 years of age or older, who are responsible for the use of these devices in compliance with all applicable District policies and local, state, and/or federal laws.

Violation of this or any related policy may be cause for a temporary or permanent prohibition from future use of library equipment or facilities. Illegal activities may be reported to law enforcement.

---

The Executive Director will establish administrative procedures necessary to implement this policy. Any appeal of an administrative action under this policy will first be made in writing to the Executive Director and then to the Board of Trustees.

The District will make a good faith effort to implement this policy in a fair and consistent manner.