

SOUTHERN TIER LIBRARY SYSTEM
INTERNET SAFETY POLICY

APPLIES TO: Board of Trustees
Member Libraries
Public Information

REFERENCES: NYS DLD Internet-Ready Libraries Program
Consolidated Laws of New York State: N Y Civil Practice Law and
Rules, Section 4509.
www.ftc.gov. (Federal Trade Commission Website, 2012)
*Children's Internet Protection Act (CIPA); Neighborhood Children's Internet
Protection Act (NCIPA)* US Congress 2000.
STLS Information Security Policy

INTRODUCTION:

The Southern Tier Library System, a regional consortium of public libraries, works in partnership with its members to support and strengthen them through clearly defined, cost-effective services that make possible the coordination and sharing of resources, enabling all individuals in the five-county region to have equal access to excellent library services.

Southern Tier Library System (STLS) supports the goals and objectives of the New York State Division of Library Development's Internet-Ready Libraries Program. To assist individual System members to use computers and telecommunications technology, access a full range of library resources, and provide the services of skilled library personnel needed in order to be an Internet-Ready Library and an integral part of the statewide electronic learning community, STLS:

1. operates an Integrated Library System (ILS), currently Sirsi/Dynix, that allows member libraries to participate in a shared patron database and the shared online catalog (STARCat) as well as to circulate materials electronically;
2. provides member libraries with technical assistance on the use of hardware, software and peripherals used to access the STLS automated network;
3. maintains a wide-area network that provides access to the Internet for libraries that have no other high-speed access, and connects libraries to the STLS ILS for sharing of library resources.

PRIVACY:

The Southern Tier Library System will take reasonable and prudent measures to protect the privacy of data provided by patrons and generated by the System and its member libraries when using the System's Integrated Library System (ILS) and the shared wide-area network. The contents of the STLS wide-area network and ILS are confidential; unauthorized users are prohibited from attempting to gain access to the network, or stored information. STLS uses firewall equipment, software and other means to protect the confidentiality of library records. However there is no absolute guarantee of the privacy of personal information stored on STLS network servers and no guarantee of the privacy of information and communications, including e-mail, that travels across the STLS wide-area network. STLS maintains personal information only

as long as needed to conduct library business. Library records are legally confidential under New York State law:

New York Civil Practice Law & Rules Section 4509 Library Records.

Library records, which contain names or other personally identifying details regarding the users of public, free association, school, college and university libraries and library systems of this state, including but not limited to records related to the circulation of library materials, computer database searches, inter-library loan transactions, reference queries, requests for photocopies of library materials, films or records, shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.¹

INTERNET ACCESS:

The Internet is a global electronic network, mostly unregulated, on which anyone may place any content or communicate any content. The STLS and its member libraries do not endorse and do not assume responsibility for any content found or any communications made on the Internet.

The STLS maintains an Internet filtering mechanism for use on all computers in the STLS Service Center and in its member libraries. The filtering mechanism will, at a minimum, block access to the three categories of visual depictions specified by the Federal Children’s Internet Protection Act (CIPA)—visual depictions of material deemed child pornography, obscene, or any material deemed harmful to minors.² The filtering mechanism can be disabled on individual computers as needed by local libraries. STLS has evaluated various filtering mechanisms before choosing the most appropriate method; however, the System does not warrant the effectiveness of Internet filtering.

It shall be the responsibility of the member libraries on the STLS wide-area network to supervise and monitor the usage of the online computer network and access to the Internet in accordance with this policy and the Children’s Internet Protection Act.

ACCESS BY MINORS:

The valuable information, opportunities for learning and interactions available on this world wide network far outweigh the possibility that users may obtain information that is not consistent with the educational and research goals of this service.

Parents or legal guardians must assume responsibility for deciding which library resources are appropriate for their own children, guiding their children in the use of the Internet and informing them about materials they should not use.

While STLS affirms and acknowledges the rights and responsibilities of parents and guardians to monitor and determine their children’s access to materials and resources, including those

¹ Civil Practice Laws and Rules, Sec. 4509. Consolidated Laws of New York State. NYS Code website 2012.

² www.fcc.gov. Children’s Internet Protection Act, 2012

available through the Internet, the System has taken certain measures designed to assist in the safe and effective use of these resources by all minors.

1. To address the issue of safety and security of minors when using e-mail and other forms of direct electronic communications, as well as the unauthorized disclosure, use and dissemination of personal identification information regarding minors, STLS urges minors and their parents or guardians to keep in mind the following safety guidelines:
 - a. Never give out identifying information such as home address, school name, or telephone number.
 - b. Let parents or guardians decide whether personal family information such as age, marital status, or financial information should be revealed.
 - c. Never arrange a face-to-face meeting with someone via the computer without parents' or guardians' approval.
 - d. Never respond to messages that are suggestive, obscene, threatening, or make one uncomfortable. Tell a parent, guardian or library staff member if you receive such a message.
 - e. Have parents or guardians report an incident to the National Center for Missing and Exploited Children via www.cybertipline.com or call 1-800-843-5678 if one becomes aware of the transmission of child pornography.
 - f. Remember that people online may not be who they say they are.
 - g. Remember that everything that one reads online may not be true.
 - h. Don't open e-mail, files or website pages sent to you by people or organizations that you don't know or trust.
2. To address the issue of unauthorized access, including so-called "hacking" and other unlawful activities by minors online, minors and all other users of STLS libraries are hereby advised that any unlawful activity is strictly prohibited.
3. Assist member libraries to create and post an introductory web page (splash) for wireless Internet access which requires a patron to verify that he or she will accept the library's terms for using that access. Unless the patron agrees to this verification, he or she will be blocked from using the library's wireless Internet connection.

PROHIBITED LIBRARY ACTIVITY:

Any user of electronic STLS services in any location is strictly prohibited from any illegal activity or unlawful purpose, including but not limited to:

1. hacking;
2. harassing or invading the privacy of other users;
3. attempting to degrade the network or disrupt its performance;
4. using the network for commercial purposes;
5. sending "spam" or unsolicited advertising of any kind;
6. violation of copyright law, including downloading copyrighted works without authorization by the copyright owner.

Adopted by the STLS Board of Trustees May 14, 2003; Revised by the STLS Board of Trustees June 15, 2004; Revised by the STLS Board of Trustees June 19, 2012.