

NORTH SUBURBAN LIBRARY SYSTEM
POLICY UNDER USA PATRIOT ACT OF 2001

Public Law 107-56, commonly known as the "USA Patriot Act," became law on October 26, 2001. The USA Patriot Act contains a number of provisions intended to expedite law enforcement. Several sections of the USA Patriot Act may implicate information generated and or retained by the North Suburban Library System ("NSLS") and its member libraries, particularly in terms of law enforcement access to library records, and the use of library facilities for surveillance and wiretapping purposes.

Many of these provisions of the USA Patriot Act will "sunset," that is, cease to have legal effect, unless renewed by Congress, on December 31, 2005; but these provisions will remain applicable to on-going investigations which had begun before that deadline. In other words, even after 2005, law enforcement officials will be able to request library records if their cases were already open prior to January 1, 2005.

NSLS and its member libraries are subject to the Illinois Library Records Confidentiality Act (75 ILCS 70/1 *et seq.*) This Act forbids publishing or making public, except pursuant to court order, any information contained in the "registration records" or "circulation records." For purposes of this Act, a valid subpoena or search warrant would constitute a "court order."

This Policy refers to some of the provisions of the USA Patriot Act and describes the NSLS protocols which are to be followed.

1.

Required Disclosures of Electronic Communications

Under existing federal law, knowing disclosure of the contents of any transmitted or stored electronic communication may be illegal. A number of statutory exceptions already exist, and the USA Patriot Act has created a further exception for "required disclosures" involving law enforcement. These exceptions expand the scope of obtainable materials and the grounds upon which law enforcement officials may obtain and serve authorizations for their disclosure.

If an individual states to an NSLS employee that the individual is a law enforcement agent, and requests the NSLS employee to provide the contents of electronic communications or any information about users of library materials or facilities of NSLS or any of its member libraries, do not disclose any information. Instead, contact the NSLS Privacy Officer; and if the NSLS Privacy Officer is not available, contact one of the Assistant Directors.

2.

Emergency Disclosures

The USA Patriot Act added a new voluntary disclosure exception for emergency situations. Under this exception, if a provider of electronic communication services reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies the disclosure of certain information, the provider may disclose that information to a law enforcement agency.

If an NSLS employee in the course of NSLS business operations reasonably believes that the NSLS employee has accessed information about an emergency involving immediate danger of death or serious physical injury, contact the local police immediately. After contacting the local police, report that contact and the underlying information immediately to the NSLS Privacy Officer; and if the NSLS Privacy Officer is not available, contact one of the Assistant Directors.

3.

Computer Trespass

Under the USA Patriot Act, owners or operators of electronic systems may authorize federal law enforcement agencies to investigate computer trespass. A "computer trespasser" is defined as the person who accesses a protected computer without authorization and, thus, has no reasonable expectation of privacy in any communication transmitted to, through or from the protected computer.

Any NSLS employee who knows or believes that the NSLS computer system has been compromised by a computer trespasser should first report this information to the NSLS Privacy Officer. If the NSLS Privacy Officer would like to have a law enforcement agency investigate the matter, the NSLS Privacy Officer will either contact the law enforcement agency or decide which NSLS employee should do so.

4.

General Protocols

The following protocols are applicable generally with respect to the USA Patriot Act:

- A. If anyone claiming to be a law enforcement official approaches an NSLS employee to request information, do not disclose any information to that individual. Immediately contact the NSLS Privacy Officer.
- B. The NSLS Privacy Officer will ask to see official identification of the alleged law enforcement official, and will make a photocopy of the alleged official's ID.

- C. If anyone claiming to be a law enforcement official presents a subpoena or a search warrant, do not provide any information whatsoever. Instead, the NSLS employee should direct that person to the NSLS Privacy Officer or to the employee's Supervisor or one of the Assistant Directors.
- D. The NSLS Supervisor, Assistant Director or Privacy Officer will make a photocopy of the subpoena or search warrant (and of the law enforcement official's ID), and then will contact the Attorney for NSLS (currently, Gerard E. Dempsey, Klein, Thorpe Jenkins, Ltd.; Telephone: 312/984-6412).
- E. If anyone claiming to be a law enforcement official asks for information but does *not* present a subpoena or a search warrant, the NSLS Privacy Officer must not disclose any information. Instead, the NSLS Privacy Officer will explain the requirements of the Library Records Confidential Act.
- F. Each NSLS employee, including the Privacy Officer, must keep a log of his or her contacts by law enforcement officials, including a record of all requests for information and all costs incurred in connection with any search or seizure, or in providing other information (written or oral) to any law enforcement official.
- G. On or after December 31, 2005, the scheduled expiration date of Section 215 of the USA Patriot Act, or at such earlier or later time as permitted by law, each NSLS employee must deliver his or her log to the NSLS Executive Director for review and photocopying.