Montgomery County Library & Information Network Consortium

PRIVACY POLICY

To understand this policy, one must understand what MCLINC is and is not.

MCLINC is not a public library. MCLINC is an acronym for the Montgomery County Library and Information Network Consortium, an independent Pennsylvania corporation recognized by the IRS as a §501(c)(3) entity. MCLINC owns and operates the computer network which provides a joint/integrated online library circulation system to all the member public libraries in Montgomery County, PA. For more information about MCLINC, go to http://www.mclinc.org/about.htm. For a list of member libraries, go to www.mclinc.org/members.htm.

As such, this policy applies only to the automated functions and resources of the computer network provided by MCLINC. It does not apply to member library policies, or the policies and practices of outside vendors, unless expressly included.

Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. The right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when an organization is in possession of personally identifiable information about users and keeps that information private on their behalf.

This privacy policy explains:

- Your privacy and confidentiality rights;
- MCLINC's information practices and the choices you can make about the way MCLINC collects and uses your information;
- MCLINC's use of your personally identifiable information;
- What MCLINC will do with respect to a request for personally identifiable information by a third person that is not a part of a legal process; and
- What MCLINC will do with respect to a request for personally identifiable information as part of a legal process.

Your Privacy and Confidentiality Rights

MCLINC will keep your personally identifiable information confidential and will not sell, license or disclose such information to any third party without your consent, unless we are compelled to do so under the law or to comply with a court order.

MCLINC's sole purpose for collecting your personal information is to assist the libraries in the network to provide its services. You entrust MCLINC with personally identifiable information to access its services. MCLINC is committed to protecting your privacy and confidentiality. This commitment is deeply rooted in the ethics and practices of librarianship, and applicable federal/state Constitutions and laws. MCLINC strictly adheres to the Pennsylvania statute for Confidentiality of Library Records:

> ***Records related to the circulation of library materials which contain the names or other personally identifying details*** regarding the users of the State Library or any local library which is established or maintained under any law of the Commonwealth or the library of any university, college or educational institution chartered by the Commonwealth or the library of any public school or branch reading room, deposit station or agency operated in connection therewith, ***shall be confidential and shall not be made available to anyone except by a court order in a criminal proceeding.*** 24 P.S. § 4428

How/When Information Is Collected

MCLINC collects personally identifiable information through many sources when you use its services.

1. If you wish to receive borrowing privileges, MCLINC must obtain certain information about you in order to provide you with a library account.

2. When visiting a member library's website and using MCLINC's electronic services, you may choose to provide your name, e-mail address, library card barcode, phone number or home address.

3. You have the option of providing MCLINC with your e-mail address for the purpose of notifying you about your library account. You may request that MCLINC remove your e-mail address from your record at any time.

4. Automated functions of MCLINC's computer network which collect personally identifiable information include the following:

a. Library business software

MCLINC collects personal information necessary to providing library services such as tracking and reserving materials, issuing library-related notifications by phone or email, etc. Circulation records are maintained based on activity related to the user account. Borrower records are retained for three years after the expiration date with no further activity. Borrower records with unpaid fines, fees or unreturned materials are kept indefinitely. Borrowers who elect to retain reading history consent to this information being stored indefinitely. Once a borrower deletes his or her reading history, it can no longer be accessed by the borrower.

b. Websites

When you browse our website (www.mclinc.org) we gather and store technical information only. For example we count the number of visitors, the type of browser used, the pages viewed, etc.

When you browse the online catalog, we gather usage counts only. The only personally identifiable information available to you appears when you log onto your account with your username or barcode. The online catalog does use cookies to display information and return search results to you more quickly. These cookies are deleted from our system when you log off.

c. Wireless access devices

Some member libraries have wireless access available from the MCLINC network. Users may be prompted to enter a borrower card number at login. MCLINC generates usage reports for Library Directors on a monthly basis and these reports contain the borrower card number and amount of time logged on. No information about sites visited is collected.

d. Public access computers

Public access computers on the MCLINC network are subject to the privacy policies and practices of the library where the machines are located. To learn which information is requested and/or stored for each user, please contact the member library directly. For a list of member libraries, please go to www.mclinc.org/members.htm. To protect your privacy, always log off any account(s) when you leave a public workstation, so your information is not available to the next user.

e. Credit Card Payments – Neither MCLINC nor its credit card payment software retains any personal account numbers. Software used by MCLINC is fully PCI compliant. Contact MCLINC for Attestation of Compliance.

MCLINC's Use Of Personally Identifiable Information

1. Internal Use

User information will be accessed by MCLINC, member library staff and authorized vendors internally only as part of the necessary performance of their job duties.

2. Statistical Reporting

Aggregate user information (not including user borrowing or circulation information) may be compiled for required statistical reporting to federal, state, local and private funding bodies. MCLINC may also use these files for building relationships and communicating with member libraries and their users in order to enhance and improve library services.

Requests For Information From Third Parties Involving A Legal Process

If a member library receives a request for MCLINC records either from a subpoena or by law enforcement agents, MCLINC has established the following procedure for responding to the request(s). Response to requests will depend on the supporting documents presented.

1. Inquiries received by member libraries shall be referred to the System Administrator of MCLINC unless specifically local to the library and not the overall system.

2. If the System Administrator is away from the office and the request is for immediate action, MCLINC staff shall make an attempt to contact the System Administrator. If the System Administrator cannot be reached, the President of the Board of Directors of MCLINC shall be contacted by MCLINC support staff and will advise staff on the appropriate response.

3. If the request does not require immediate action, and the MCLINC System Administrator will return to the office within one business day, MCLINC support staff will defer any action until his/her return.

4. Counsel for MCLINC will be consulted if there are any questions/concerns.

5. MCLINC shall immediately notify the President of the Board when an inquiry is received.

6. The President shall notify the Board of the inquiry and any action taken in response.

Documentation	**Discussion**
None	Consistent with the PA statute quoted above, no information will be provided without a court order, even to law enforcement officials. MCLINC will explain this Privacy Policy to the requestor and inform the requestor that MCLINC's policy is guided by law, which MCLINC must follow. MCLINC will also offer to provide a copy of the policy for review.
Subpoena	A subpoena is a call to come before a court, and may include a direction to bring specified records. A subpoena normally indicates that a response is required within a certain number of days. ***Not all subpoenas are court orders.*** In addition, even a valid subpoena may be overly broad or otherwise subject to negotiation with the issuing authority. MCLINC's counsel can determine if a particular subpoena must be complied with as is or whether it is subject to negotiations with the issuing authority or needs to be dealt with in a court proceeding such as seeking a Protective Order or filing a Motion To Quash.
Court Order/ Search Warrant	A search warrant is an order signed by a judge directing a law enforcement officer to conduct a search. All search warrants are court orders. MCLINC is required to disclose library records in response to search warrants.

Foreign Intelligence Surveillance Act (FISA) Orders	A FISA order is a search warrant under the umbrella of the Foreign Intelligence Surveillance Act. The USA Patriot Act amended FISA to allow the FBI to apply for a court order requiring "the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment . . ." If the library receives a FISA order it will be presented by an FBI agent and MCLINC is required to disclose library records in response to a FISA order. Further, it is illegal to disclose to any other person (other than those persons necessary to produce the tangible things sought in the warrant) that the FBI has sought or obtained records or other items under FISA.

If confronted with a court or FISA order, the following shall apply:

1. All transfers of physical evidence (electronic records) into the hands of law enforcement authorities shall be managed by the MCLINC System Administrator.

2. The law enforcement agent(s) will be asked to supply a receipt or inventory of any records or equipment collected from MCLINC.

3. Many times, that is all that is necessary. The law enforcement official presents the court order; copies of the records are made by MCLINC and produced to the official.

4. While unlikely, it is still possible that a court or FISA order is executed is in an abrupt/somewhat hostile manner. If that occurs:

a. Present MCLINC staff will cooperate fully and keep as complete notes as possible as to what is accessed/taken to ensure that only the records identified in the court or FISA order are produced and that no other library user's records are disclosed.

b. If the law enforcement officer wants access to, or to take, records that MCLINC does not believe are covered by the search warrant, MCLINC will still cooperate. Failure to do so could result in the MCLINC staff person being arrested. Whether or not a document taken was subject to the search warrant can be addressed by MCLINC's counsel after the search is over.

c. With respect to the form of media to be given to, or taken, by the law enforcement officials, MCLINC will offer to provide copies of the electronic records wherever possible. Copies may include backup media, screen shots or reports from the system software. Removing the original records and/or hardware will present a hardship, by preventing MCLINC from conducting library service for an extended period of time. But if the law enforcement officials demand the original records and/or hardware, MCLINC will still cooperate. Failure to do so could result in the MCLINC staff person being arrested.

Revised -December 17, 2010

Last Revised -January 14, 2013