SHREWSBURY PUBLIC LIBRARY
POLICY MANUAL

Your Privacy and Confidentiality at the Shrewsbury Public Library

Confidentiality of Library Records

The Shrewsbury Public Library is committed to maintaining patron confidentiality and makes every reasonable attempt to ensure that all records pertaining to a patron's use of library materials and information resources remain confidential.

Any patron data stored (either intentionally or incidentally) on our computer network or on our consortium's servers is confidential and protected by Massachusetts law (MGLA Chapter 78, Section 7: "That part of the records of a public library which reveals the identity and pursuits of a person using such library shall not be a public record as defined by clause Twenty-sixth of section seven of chapter four.").

Confidential information includes circulation records, interlibrary loan transactions, database usage statistics, program registration information, photocopier usage data, room reservation requests, reference questions, or any other private patron information supplied to or gathered by the library.

This information shall not be made available to or disclosed to any individual, corporation, institution, or government agency without a valid warrant, subpoena, or court order. Upon presentation of such a warrant, subpoena, or court order, the library shall make every legal effort to maintain the confidentiality of all patron records.

We are committed to doing our best to protect the privacy of your personal information that you have entrusted to us. We do not sell or give information on any of our visitors to third parties. When you send us an email, sign up for our alerting service, or register for a library card, we do not share that information with any third party. We only use the information for the purposes you have authorized.

Please note that confidentiality rights on circulation records are forfeited when a patron has overdue materials, and parents or guardians of minors may request information concerning their children's current circulation records solely to assist their children in returning such items.

The following is the staff procedure for responding to law enforcement requests for patron records:

1. The front desk staff member will not disclose any information but will instead immediately contact the Library Director. If the Library Director is out of the building, every attempt should be made to contact the Director. In the event that the Director cannot be reached, the Assistant Director or other library department head will act in the Director's absence.

2. The Director (or other supervisor acting on her behalf) will request to see official law enforcement identification and will photocopy the identification.

3. If the law enforcement official presents a subpoena, the request should be directed to the Library Director. The Library Director (or other supervisor) will immediately contact legal counsel. A subpoena is not immediately executable, and legal counsel should be involved before the library responds to such a request.

4. If the law enforcement official presents a warrant, do not interfere with the search and/or seizure, but contact the Library Director immediately. The Library Director (or other supervisor) will immediately contact legal counsel for further advice on how to proceed with the response to the search warrant.

5. If the Law enforcement official presents a request for information under the provisions of the USA PATRIOT Act and or Foreign Intelligence Surveillance Act (FISA), do not interfere with the search and/or seizure, but contact the Library Director immediately. The Library Director (or other supervisor) will immediately contact legal counsel for further advice on how to proceed with the response to the USA PATRIOT Act or FISA request. The USA PATRIOT Act and FISA require that no employee or official disclose the existence of the court order or the fact that records were produced in response to such an order, including to the patron who is the subject of the court order. Disclosure of this information is punishable under the penalty of law.

6. The Library Director will notify the Town Administrator of all contacts with legal counsel regarding requests for patron information. When time and circumstance allow, she will notify the Town Administrator prior to contacting legal counsel. When this is not possible, such as when a warrant is immediately executable or disclosure is prohibited by the USA PATRIOT Act or FISA request, the Director will contact legal counsel without contacting the Town Administrator.

7. In all cases of requests for patron information, the Library will maintain a record of all materials, data, or information requested or seized.

8. In all cases of requests for patron information, the Library will maintain a record of all costs incurred by any search or seizure. The Board of Library Trustees will seek reimbursement of such costs from the appropriate agency.

Confidentiality Concerns for Public Computer Use

In the networked, electronic world we live in we are all rightfully concerned about our personal privacy and the confidentiality of our personal information. It is difficult to maintain our privacy even at home on our personal computers. It is even harder for us to help you maintain your privacy when you use our shared, public computers. Our job is to adapt what is usually a private instrument — the personal computer — to a public setting. In doing so, we have to make certain

compromises between the needs of individual users for privacy and the needs of all users to safely access a broad range of electronic information services.

As you use our computers in the library, it is best to keep in mind at all times that complete privacy is not a realistic expectation. However, we do try to protect your privacy to the maximum extent possible, given the fact that our computers are shared. The privacy implications of using our public computers are explained below.

Any patron data stored (either intentionally or incidentally) on our computer network or on our consortium's servers is confidential and protected by MA law (MGLA Chapter 78, Section 7: "That part of the records of a public library which reveals the identity and pursuits of a person using such library shall not be a public record as defined by clause Twenty-sixth of section seven of chapter four."). We maintain no permanent records of what you view or the documents you create. The history file of sites you visit is erased when the computer is reset or rebooted.

Security in a networked electronic environment cannot be guaranteed. Even the most secure networks can be susceptible to outside intervention. Therefore, all transactions, files, and communications on a public computer are vulnerable to unauthorized access and use and should be considered public. Think very carefully about what you are revealing about yourself as you type into a computer.

Library computers are located in public areas which must be shared by library users of all ages, backgrounds, values, and sensibilities. We strive to balance the rights of users to access different information resources with the rights of users to work in a public environment free from harassing sounds and visuals. We ask that all Library users remain sensitive to the fact that they are working in a public environment shared by others. If what you view or listen to causes discomfort to others, staff may intervene.

Computer users are asked to respect the privacy of other computer users. This includes but is not limited to, not using someone else's login/password, not modifying someone else's password, not trying to gain access to someone else's data or search history, not retrieving someone else's printout, and not hovering over others while waiting to use a computer.

As an added security feature, all of our computers are equipped with software that purges all new data, restoring them to a default state upon each restart, and each computer is set to restart each time a patron session ends. This should prevent any future users from gaining access to any previous user's personal data when using that same computer.

We have no control over how the sites you visit on our computers use your personal data, nor the degree of privacy they extend to you. We encourage you to review their privacy policies individually. Be especially careful when the page owner asks if you want your password to be "remembered." This works fine at home but is not a good idea with public computers. Some sites, assuming you are working on a private computer, utilize "cookies" — small bits of tracking software typically used to personalize and streamline your usage of their site — that can occasionally compromise the security of your login and other information. You may even want to avoid sites that seem to "remember" you when you don't want to be remembered. Also, be

sure to log out of any services you may have logged into when using library computers. Web-based email is notoriously vulnerable to unauthorized access and modification, and while the library makes every effort to ensure that no personal data remains on computers after patron sessions end, ultimately responsibility for not exposing said data to unauthorized use rests with you, the user.

Data loss is a fact of life in an electronic environment. Our prioritization of your privacy makes data loss more likely on our computers than on a private computer in your home. To protect your privacy, our computers have software that keeps data from being permanently stored on the hard drive. Once the computer is rebooted for any reason, any stored information from your session is deleted and the computer is reset to a default state. This protects your privacy but can lead to the loss of your data, especially in the event that a computer freezes or power is interrupted. When a computer is restarted for any reason, data purged at that time cannot be recovered. For privacy and data safety reasons, we encourage you to use a flash drive or a cloud storage system to backup any files you work on while using library computers. This will ensure that no data is lost when your session concludes. Flash drives may be purchased from the reference desk for $8.

Ultimately, we cannot guarantee absolute security and confidentiality for any action you take while using our computers. If you are concerned about any electronic financial transaction or any transfer of sensitive electronic data, we suggest you do not use library computers for such purposes. If you have any more specific questions about the security of library computers, they may be directed to the Electronic Resources Librarian or the Technology Specialist.