Manchester Community Library
Privacy Policy

Statement of Values

The Manchester Community Library believes that the right to privacy is essential to free inquiry, thought, speech, and association, and that all Library users should be free to select, explore, and consider information for themselves without fear of censure, judgment, or punishment. The Library seeks to uphold the Library Bill of Rights, a publication of the American Library Association, and the ALA Code of Ethics.

The Manchester Community Library does not sell any library user data, and does not share user data with other organizations except in cases where the Library is partnered with said organizations to provide services (e.g., sharing RSVPs to an off-site event with event hosts).

Library Privacy Regulations

The ethics of the field of library science and the laws of the state of Vermont (22 V.S.A. § 172) provide for the confidentiality of library members' registration and borrowing records. As such, Library staff keep confidential records of who maintains membership at the Manchester Community Library, and the borrowing activities tied to each account. Member registrations and borrowing records are available only to staff and agents of the Library to the extent necessary to administer Library services.

Library members may make corrections and updates to the Library's records of their contact information and other personal details by logging into the catalog and visiting the Dashboard page. Because membership information is kept confidential, updating personal details in the catalog does not carry over to other Library systems such as the newsletter or donor database. Please contact the Library directly for assistance updating these other systems.

Household memberships and privacy of records

For information about the kinds of memberships available at the Library, please see the Membership page. Multiple people living together may set up a household Library membership, in which each has their own library card, but the membership is billed (in the case of non-resident members) and renewed as a single unit. In this case, membership and borrowing records, with the exception of messages related to membership renewal, are kept separately to each card as if they were single memberships, and each member's records are not available to other members within the household (except for children under 16, as specified under Records of Members Under Age 16, see below).

A household membership can also be arranged such that one adult is the primary borrower named on the account and this individual specifies the other adults/children residing with them who are authorized borrowers on their card/account. In this case, the non-primary borrowers will be able to check out materials from the Library on the card, but only the primary borrower will be allowed access to account records. The primary borrower will be able to see what materials other authorized borrowers on that card have used the account to access.

In the case where a member over the age of 16 cannot come to the Library on their own, they may authorize someone else in writing to borrow items on their membership for them by filling out a Library Card Access Permission Form. This authorization will be in effect until canceled. All items borrowed during this time are the responsibility of the member. If a member over the age of 16 is without capacity to complete a written authorization, and requires assistance

to manage their Library membership, their custodial parent or legal guardian may present paperwork—usually court documents—demonstrating the custodial arrangement in order to be authorized on the account.

As of September 2021, the Library will only create and renew household memberships according to the structure described in the first paragraph of this section. Library members who have household memberships structured according to the second paragraph may visit the Help Desk to request that their accounts be changed to give each household member their own card during any of the Library's open hours, and will be asked to do so at the time of the next renewal of their membership if they have not done so by that time.

Records of members under age 16

22 V.S.A. § 172 provides for the disclosure of library users' membership and borrowing records to custodial parents or guardians for library users under the age of 16. Custodial parents and guardians of Library members who are under the age of 16 may reference their children's Library records, and borrow and return materials on their children's behalf.The Library has the right to take reasonable steps to verify that the person attempting to access the membership is in fact a custodial parent or guardian of the child they are inquiring about before providing the records, including by asking for photo identification.

Library members between the ages of 12 and 16 will be notified by Library staff when a custodial parent or guardian accesses their records. Once a Library member turns 16, custodial parents and guardians will no longer be granted permission to view that member's records, including records from before the member turned 16.

In the case of an authorized judicial order or warrant directing disclosure, the Library may be required to share your information with the relevant authorities. No confidential information on Library members will be revealed to law enforcement without presentation of an authorized judicial order or warrant directing disclosure.

Deletion of member records

Library memberships which have expired and been inactive for two years are purged from Library records, unless there is an outstanding fine related to overdue materials. Library members who wish for their Library membership records to be purged before the account has expired and two years have passed may request that the records be deleted by submitting a Request for Data Deletion. The Library has the right to take reasonable steps to verify that the person submitting the request is in fact the owner of the membership before deleting the records, including by asking for photo identification. Members requesting deletion will be required to settle outstanding fines owed to the Library before the records are deleted.

Recording

Photography

Library staff and volunteers take photos and videos to document Library events and proceedings and share them with the community. Users of the Library may also record images, audio, and video in Library spaces where there is no reasonable expectation of privacy (e.g., common areas of the Library including, but not limited to: entrances, near book and media collections, public seating, delivery areas, and parking lots. Recording is not permitted in areas where staff and public have a reasonable expectation of privacy (e.g., restrooms and study rooms), and it is not permitted to record in such a way as to intentionally identify a person's reading, viewing, or listening activities in the Library.

Recordings and photographs taken by Library staff may be uploaded to the Library's online channels, e.g. the Library website, YouTube channel, social media channels, and to GNAT-TV. Library staff will take reasonable steps to avoid

posting recordings or photographs that identify a person's reading, viewing, or listening activities. Library users may opt out of themselves and/or their minor children being photographed/recorded by Library staff by approaching the photographer and requesting to be excluded from recording for that event or day. Library users requesting this exemption will be asked to fill out a Recording Exemption Form.

If you would like a photograph or recording of you to be removed from our website or social media accounts, please let us know via the Request for Data Deletion. Library staff will respond to requests for deletion within five business days. Where possible, please provide a link to where the media is displayed.

If you have a great photo of Library goings-on, or footage of you or someone you know enjoying one of our events, we would love to take a look. Send it in, and we might feature it online.

Tip: If you upload or otherwise transmit your own images to the Manchester Community Library, and grant us permission to post them on the website, you should avoid uploading images with embedded location data (EXIF GPS) included. Visitors to the website can download and extract any location data from images on the website.

Security cameras

The Manchester Community Library operates security cameras on the exterior and interior of the building to increase the safety of Library users, staff, and property; to discourage violations of Library rules of conduct; and, where necessary, to assist Library staff or law enforcement in following up on violations of Library policy or the law, respectively. This policy should be interpreted with the understanding that the image of a person on library property is not protected, but anything that would identify the content of a library user's account is protected and held private.

Cameras may be installed in locations where staff and patrons would not have an expectation of privacy. Examples include common areas of the Library such as entrances, near book and media collections, public seating, delivery areas and parking lots. Cameras will not be installed in areas where staff and users have a reasonable expectation of privacy, such as restrooms and study rooms, nor are they positioned to intentionally identify a person's reading, viewing, or listening activities in the library. Cameras will not be installed for the purpose of monitoring staff performance.

Public notification is given of the use of security cameras in the form of clear signage. The purpose of this is to give Library users reasonable and adequate warning that security cameras are in operation before entering any area under video surveillance. Signage is posted at the Library's entrances at all times, disclosing this activity.

Staff may have access to real-time monitors. Images will be viewed on monitors placed in secure areas to ensure privacy. Designated staff may additionally access stored footage in pursuit of documented incidents of criminal activity or violation of the Library's rules of conduct. Staff designated to access stored footage are: the Executive and Associate Directors, Facilities Manager, and Information Technology and Instructional Librarian, and other individuals designated by the Executive Director.

Library user access to video footage is not allowed without a valid court order. For investigations initiated by law enforcement agencies, recorded data will be made available to law enforcement upon presentation of a valid court order or subpoena establishing probable cause to review the data. However, in emergency situations that present imminent danger of physical harm, law enforcement may gain access without a court order. In such imminent danger emergencies where law enforcement calls for a waiver of the court order, the requesting officer is required to provide their name, agency, badge number, the nature of the emergency, and the extent of data requested.

Production of video copies for distribution is limited to designated staff as specified above and may only be carried out with permission from the executive or associate director.

Images will be stored for a length of time based on available storage, but no longer than 30 days, except when retention is specifically requested by someone with authority to access recordings as specified in this policy, or for images used in ban-and-bar documentation. As new images are recorded, the oldest images will be automatically deleted. The length of storage time varies depending on the camera's memory and recording length.

In situations involving banned-and-barred users, stored still images may be shared with staff system-wide. Shared images may remain posted in restricted staff areas for the duration of the banning period. After the banning period ends, these images are archived in the administrative offices for five years.

Because security cameras are not constantly monitored, staff and Library users should take appropriate precautions for their safety and security of personal property. The Manchester Community Library is not responsible for loss of property or personal injury.

Public Computers and Wi-Fi

The Library does not monitor the online behavior of individual users, whether on public computers or personal devices connected to our public Wi-Fi. Custodial parents and guardians of children under the age of 16 are responsible for monitoring the use of Library technology by their children. Users should be aware that in some cases, third parties can gain access to information transmitted over a public wireless network, and users accept this risk by using the Library's free wireless internet service.

Public computers are set up to delete browsing history and cached data daily, but users always have the option to delete their own browsing data at the end of a computer session to ensure subsequent users that day will not see it. It is the user's responsibility to delete their own browsing data at the end of a computer session if so desired. If you are not sure how to do this, you can request help from Library staff at the Help Desk.

Library Website

Contact forms and event registrations

Information submitted via web forms is never sold or shared with other organizations except as necessary to provide the service the form is requesting, (e.g. registering you for an event or joint/co-sponsored event, or answering a request for technical support). Most fields on these forms are optional, and users are not required to submit personally identifying information except to such an extent as it will help staff contact them to follow up on their inquiries. Form submission data is not used for the Library's own advertising or solicitation purposes unless the user grants that permission, usually by ticking a checkbox that indicates their willingness to share their data for this purpose.

Form submission data is stored on the Library's web server for up to 90 days before being deleted. Emails about form submissions, such as the email receipts you might receive to confirm you have submitted a form, may be stored longer than that by their recipients (i.e., you), Library staff, and/or email service providers.

Embedded content from other websites

Pages on the Library website may include embedded content (e.g. videos, images, and articles). Embedded content from other websites behaves in the exact same way as if the user has visited the other website. These websites may collect data about you, use cookies, embed additional third-party tracking, and monitor your interaction with that embedded

content, including tracking your interaction with the embedded content if you have an account and are logged in to that website.

Aggregate Data

The Library collects aggregate data about how library users interact with our services, including but not limited to:

- the number of people who visit our premises each day, and the number of people who use particular services like the public computers and wi-fi,
- the number of people who attend events at the library,
- the number of people who visit our website, and who visit particular pages on it,
- the number of people who view and like our social media posts, and watch our online videos, and
- the number of people who subscribe to and open our digital newsletters.

The Library uses these numbers as statistics to help measure the success of our services, but does not report library users' names or other identifying data in these records. All paper records of who used a service, such as sign-in sheets for public computers, are destroyed at the end of each business week after their entries are counted.

Data Breach Procedures

The Manchester Community Library takes user privacy seriously, and takes multiple measures to ensure that no one gains unauthorized access to user data. In the event that such a breach is discovered, the Library will immediately work to establish what data was affected, when, and how; will take steps to remove all unauthorized access from Library systems; will notify all library users whose personal data was affected by the breach; and will post a public notice of the breach. After all of these steps are completed, Library staff will complete a postmortem study of the breach event to decide what measures can be taken to prevent a recurrence of the event in the future, and will implement an action plan based on the postmortem's findings.

Last updated October 12, 2021