CUSTOMER POLICIES

CONFIDENTIALITY OF CUSTOMER LIBRARY RECORDS

Board Policy:

DATE REVIEWED: 01/26/2023
DATE APPROVED: 01/26/2023
EFFECTIVE DATE: 03/01/2023
REPLACING POLICY EFFECTIVE: 12/01/2009

Columbus Metropolitan Library (CML) maintains confidentiality of library records, customer information and library use by customers to the extent state and federal laws allow. CML employees are required to keep customer requests and records confidential.

Customer information and library records related to customer library usage, including materials circulated, reference questions asked and computer programs and/or sites used, are confidential to the extent provided by law. Confidentiality of library records is meant to provide customers privacy regarding information they seek in order to promote the most complete access to information.

Customers who choose to provide information about themselves or their interests through CML's optional social networking/personalization or other third-party services agree that the information they choose to share via such services is not a confidential library record and may be publicly available consistent with the features and functions and terms and conditions of the applicable service.

CML is a member of the Central Library Consortium (CLC), a partnership between public libraries in Central Ohio. Through this partnership, employees of other CLC libraries have access to CML customer information and records through a shared database that allows each library system to serve customers from other systems as their own. All CLC libraries and their employees must adhere to the CLC Security Policy and its related documents or have an alternative policy that offers the same or better protection of data as a condition of participating in the consortium.

Administrative Procedure:

DATE REVIEWED: 01/26/2023
DATE APPROVED: 01/26/2023
EFFECTIVE DATE: 03/01/2023
REPLACING POLICY EFFECTIVE: 08/24/2021

A. **Customer Access to Library Records**
Information regarding a customer's library account or informational or computer use of the library will be released upon the request, or with the consent, of the customer. Anyone in possession of the customer's library card, or with knowledge of the customer's library card number, will be assumed to be an authorized user of the card and may, accordingly, have the ability to access the customer's library records. It is

the customer's responsibility to maintain the security and confidentiality of their library card and account information. Customers must report lost or stolen cards immediately to prevent unauthorized use.

B. **Non-Cardholder Access to Library Records**
CML will not to disclose a customer's library records to a contractor, vendor or other third party, except as required or permitted by applicable law.

Third party requests for disclosure of library records are subject to the review and approval of CML's executive leadership team and legal counsel, as appropriate, except in the case of exigent circumstances.

Third party requests for library records should be directed to the Chief Customer Experience Officer, Chief Financial Officer or the Chief Executive Officer.

C. **Requests from Law Enforcement**
Requests for library records from a law enforcement agent or officer should be directed to the Chief Customer Experience Officer, Chief Financial Officer or the Chief Executive Officer.

1. If the agent or officer does not have a court order compelling the production of records, the Chief Customer Experience Officer, and/or the Chief Financial Officer, and/or the Chief Executive Officer will inform the agent or officer that records are not available, except when a proper court order in good form has been presented.

2. If the court order is presented in the form of a search warrant, the Chief Customer Experience Officer, and/or the Chief Financial Officer, and/or the Chief Executive Officer, will instruct staff to cooperate with the search.

3. If the court order is a subpoena, the Chief Customer Experience Officer, and/or the Chief Financial Officer, and/or the Chief Executive Officer will review the information that may be produced before releasing the information to ensure that the subpoena is followed strictly and no information not specifically requested is released.

4. When the subpoena is processed and completed, all information pertaining to the subpoena including the original document, email correspondence relating to the subpoena, and any other data will be packaged and forwarded to the Chief Financial Officer. The Chief Financial Officer will retain copies of the information in both paper and electronic files.

5. Under exigent circumstances, records may be released to a law enforcement agent or officer without a search warrant or court order. Exigent circumstance is defined as an emergency situation requiring swift action to prevent imminent danger to the life or safety of a person or serious damage to property, or to forestall the imminent escape of a suspect, or destruction of evidence. Staff should make a good faith determination of whether an exigent circumstance exists based on the information available at the time of the request. If time permits, staff may contact the Chief Customer Experience Officer, the Chief Financial Officer, and/or the Chief Executive Officer to aid in making such determination. In making any such determination, the key factor is whether the facts as presented by the requesting agent or officer indicate that disclosure of the information is urgently required in order to help avoid, prevent or mitigate an event that will have a negative public safety impact.

Related Policies/Forms:

- Cardholder Registration and Account Access
- Computer Security and Internet Access
- Video Surveillance for Safety and Security Purposes