

Privacy Policy

This policy outlines the app privacy practices of Boone County Public Library (BCPL). Please read this privacy policy carefully.

Confidentiality and Privacy.

Library Records: Per Kentucky OAG 82-149, KRS 61.931-934, and KRS 61.870-884, confidentiality of Library Records containing personally identifiable information relating to an individual's use of the library including, but not limited to, registration information, checkouts, and reading history, is protected. Except pursuant to a court order, no person shall publish or make any information contained in such records available to the public. This restriction shall include the press and any agency of State, Federal or local government. The release of statistical information is permitted provided no individual is identified in the information released.

Individuals requesting their own account and/or registration information must present their library card or photo identification. Library staff may request additional identification before releasing confidential account information to any individual.

Parents or legal guardians of children 17 years of age and younger may receive account information on their children's card.

Email: The Library collects email addresses from customers with their permission. The Library uses this information only for the conduct of library business, such as sending account notices, confirming program registrations, and sharing library news. Customers may opt in to receive emails promoting specific library services, collections and programs. The Library does not sell, exchange, or lend email lists to outside companies, organizations, or individuals.

Photography: Customers can take photos/videos/recordings in the Library because it is a public building. Photos must not intrude upon or invade the privacy of the people using the Library. Photo, video and recording of library users without the individuals express consent is not permitted. If customers want to set-up a formal photo session, or if a local news organization wants to take pictures, they need to talk to the Branch Manager or the Public Relations Director first.

Data Security: The Library takes reasonable steps to ensure data security, such as: electronically purging outdated patron records two times a year, investing in appropriate technology to protect the security of personally identifiable information while it is in the library's custody, and removing cookies, search histories, cached files and temp directories after each public computer session.

Third Party Vendors: The Library enters into agreements with reputable third-party vendors to provide certain online content and services to Library customers, such as program registrations, study room reservations, mobile applications, digital collections and text notifications. Customer information may be accessible to third party vendors in

order to provide these services. Customers are encouraged to read and become familiar with the privacy policies of these third-party vendors posted on the Library's website.

Procedure for Request of Confidential Information: On receipt of any legal process, order or subpoena for confidential library records, the Library staff member in charge will immediately notify the Library Executive Director, Public Service Director, IT Director, or Board President. The Library Executive Director or his/her designee will consult with the Library Attorney to consider appropriate action. Until the legality of such process, order or subpoena has been affirmatively shown to the satisfaction of the Library attorney, the Library will resist its issuance or enforcement until any such defect has been cured.

Staff is instructed to cooperate with law enforcement officials executing a search warrant. If a search warrant is executed immediately, staff will notify a library official as previously noted.

If a sworn law enforcement officer requesting the information represents that it is impractical to secure a court order as a result of an emergency where the law enforcement officer has probable cause to believe that there is imminent danger of physical harm, the information requested must be limited to identifying a suspect, witness, or victim of a crime. The information requested without a court order may not include the disclosure of registration or circulation records that would indicate materials borrowed, resources reviewed, or services used at the Library. If requested to do so by the Library, the requesting law enforcement officer must sign a form acknowledging the receipt of the information. (KRS 61.870-884)

In the event of a demand pursuant to the Patriot Act, the Library Executive Director and/or the Library Attorney will be consulted.

The Executive Director and designated staff members shall use their best discretion under the circumstances known to them at the time.

Created 06/2022

Approved