

## Information Privacy Policy

<b>1.1 – General Policy of Nondisclosure</b>	1
<b>1.2 – Confidentiality of Library Records</b>	1
<b>1.3 – What Information May Be Collected</b>	1
<b>1.4 – Staff Access to Personally Identifiable Information</b>	2
<b>1.5 – 3rd Party Access to Personally Identifiable Information</b>	2
<b>1.6 – Library User Access to Personally Identifiable Information</b>	2
<b>1.7 – Reading History Services</b>	3
<b>1.8 – Removal of Retained User Information</b>	3
<b>1.9 – Credit Card Transactions</b>	3
<b>1.10 – Website Access</b>	3
<b>1.11 – Computer and Internet Access</b>	4
<b>1.12 – Disclaimer</b>	4

### 1.1 – General Policy of Nondisclosure

Jefferson County Library Cooperative (JCLC) will not sell, lease or otherwise distribute or disclose personally identifiable information about library users, their use of library resources or their borrowing history, except as required for the efficient operation of the library or as required by applicable federal and/or state law.

### 1.2 – Confidentiality of Library Records

All library records and other information relating to an individual's use of the library and its resources are considered confidential. These records include, but are not limited to, name, address and other registration information, circulation records, charges owed and payments made, class or program enrollment records, reference or informational queries, interlibrary loan transactions, computer usage and catalog searches. Personally identifiable information is not retained except as required for library operational purposes.

Confidentiality of library records is established in Alabama law (see Code of Alabama 1975, 41-8-9 and 41-8-10; Acts 1983, No. 83-565, p. 866, §1-2).

### 1.3 – What Information May Be Collected

JCLC may collect user information in several ways: directly from the user, typically during library registration; from automatically-collected network logs; and through cookies. JCLC only retains personally identifiable information required for the reasonable operation of the library.

#### **1.4 – Staff Access to Personally Identifiable Information**

Personally identifiable information of library users may be accessed by and used by a staff member of JCLC or of a member library when the staff member is acting within the scope of his or her duties in the administration of the library.

JCLC assumes no liability for disclosure of library user personally identifiable information by any library staff acting within or outside the scope of his or her duties.

#### **1.5 – 3rd Party Access to Personally Identifiable Information**

In order to provide digital library services, such as reference databases and downloadable books and audiobooks, JCLC may be required to provide personally identifiable information to companies that provide those services to authenticate and verify a library user's right to access that material. Before interacting with any such service, users should read the privacy policy of the company that is providing the service in question.

JCLC or a member library may be required to provide a user's personally identifiable information to a local, state or federal governmental entity pursuant to compulsory legal process such as through a court order, subpoena or search warrant.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) became law on October 26, 2001. Under provisions of the act, the Federal Bureau of Investigation (FBI) and law enforcement officials may seek court orders for library records for investigations relevant to national security or terrorism. Libraries or librarians served with these search warrants may not disclose, under penalty of law, the existence of the warrants or the fact that records were produced as a result of the warrants. Key provisions of the Patriot Act were renewed for four years in the PATRIOT Sunsets Extension Act of 2011, and June 2, 2015.

Some library users may choose to utilize the electronic communication services from the library for hold and overdue notices and program and class announcements. These notices are generally sent via e-mail, telephone, SMS or through other means. The library has limited ability to protect the confidentiality of this information once it is outside the library's control.

JCLC and member libraries may also offer a wireless network that allows users to connect to the Internet. Data accessed and sent over a library's wireless network is not secured. While every reasonable effort is made to provide a safe wireless network, JCLC assumes no liability for any loss or damage that may occur through use of the wireless network.

#### **1.6 – Library User Access to Personally Identifiable Information**

Individuals who use library services that require the collection of personally identifiable information are entitled to view and/or update their information, either in person or online. To maintain confidentiality, library users may be asked to provide verification of identity through a PIN or personal identification number or authorized identification card.

Any parent of a minor child shall have the right to inspect the registration and circulation records of any school or public library that pertain to his or her child (Code of Alabama 1975, 41-8-10; Acts 1983, No. 83-565, p. 866, §2). Parents may be asked to provide verification of identity through a PIN or personal identification number or authorized identification card.

### **1.7 – Reading History Services**

Users may choose to utilize an optional service through the library catalog to save reading history i.e. circulation transaction records. The user can opt-in or opt-out of the service at any time through the My Account feature on the web site. The user should be aware that saved transactional records can be discovered through compulsory legal action such as subpoena or warrant.

User opt-in to 3<sup>rd</sup> party services not controlled or administered by JCLC is a contract between the user and the 3<sup>rd</sup> party service.

### **1.8 – Removal of Retained User Information**

Personally identifiable information that is retained during user registration is typically purged from the library system after three (3) years of inactivity, unless said user account has outstanding fines or fees or other unfulfilled obligation to the library. Library users have the right to request with authorized identification that registration information be purged from the library system at any time, unless said user account has outstanding fines or fees or other unfulfilled obligation.

### **1.9 – Credit Card Transactions**

JCLC and member libraries may accept credit card payments for fines and fees accrued by library users. Payments may be made either online, at a circulation desk or at a self-checkout station at a member library. JCLC uses a secure, PCI compliant (Payment Card Industry Data Security Standard) payment connection through a third-party vendor. Credit card information is not retained by JCLC.

### **1.10 – Website Access**

No personally identifiable information is retained for visitors to the JCLC websites.

In the course of providing services through the JCLC websites, certain information may be automatically collected and used in aggregate to maintain, enhance or add functionality. This information may include:

- the IP address of the request
- pages on the JCLC website that were visited
- the URL of the web page that linked to the JCLC websites
- the Internet browser and configuration used to access the JCLC websites

The JCLC websites may contain links to other sites. JCLC does not control or monitor access to material which may be accessible from other Internet sites. JCLC is not responsible for the confidentiality of any information users provide to outside sites.

### **1.11 – Computer and Internet Access**

The JCLC member libraries may offer computers for public access. Every effort is made to remove user information from the computer in accordance with the policies of the member libraries. However, public workstations are neither private nor secure and users must practice discretion when using a library computer. JCLC assumes no liability for any violation of privacy of an individual or for any commercial or financial loss to users who use library computers.

### **1.12 – Disclaimer**

JCLC assumes no liability for any damage to user data or loss of user privacy sustained while using member library computers or other library resources. Individual JCLC libraries may have additional policies and procedures in effect.

JCLC makes every reasonable effort to maintain the confidentiality and security of all personally identifiable information that is collected. Appropriate physical, electronic, and managerial procedures are in place to safeguard and secure the information to prevent unauthorized access, alteration or disclosure of data. Despite the precautions JCLC takes to prevent unauthorized access to personally identifiable information, no system is immune from unlawful intrusion through hacking, which violates both federal and state laws; therefore, JCLC cannot guarantee that information we collect can never be accessed by unauthorized users.

Each member library is responsible for informing its users of acceptable and prohibited uses of internet and networking technologies and reporting any violations of this policy to the member library director, and/or JCLC executive director. If the member library believes criminal activity has occurred, the local authorities should also be notified. In the event that any of the prohibited activities occur, the member library or JCLC may suspend or terminate Internet access to that user or library until such time that the library implements procedures to stop this activity. Whenever practical, JCLC will provide the user and/or library advance notice and an opportunity to address the problem.