Patron Privacy Policy

1. Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. At the Las Vegas-Clark County Library District (the District), the right to privacy means the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.

The courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states provide guarantees of privacy in their constitutions and statute law. Numerous decisions in case law have defined and extended rights to privacy. This library's privacy and confidentiality policies are in compliance with applicable federal, state, and local laws.

Patron rights, and the District's responsibilities outlined here, are based in part on what are known in the United States as the five "Fair Information Practice Principles." These five principles outline the rights of Notice, Choice, Access, Security, and Enforcement.

The District's commitment to patron privacy and confidentiality has deep roots not only in law but also in the ethics and practices of librarianship. In accordance with the American Library Association's Code of Ethics:

> The District protects each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired, or transmitted.

Adopted by the Las Vegas-Clark County Library District Board of Trustees on November 13, 2003; revised and adopted on April 16, 2009; revised and adopted on April 10, 2014.

2. Las Vegas-Clark County Library District's Commitment to Patrons' Rights of Privacy and Confidentiality

This privacy policy explains library patrons' privacy and confidentiality rights, the steps the District takes to respect and protect patron privacy when using library resources, and how the District deals with personally identifiable information that it may collect from patrons.

The Board delegates to the Executive Director the authority to set administrative practices regarding the requirements of library patrons to present identification including a verifiable address of residency as a condition of borrowing District library materials and use of various library services.

Administrative practices and identification requirements are intended to protect District resources from abuse, theft and damage by enabling District staff to recover unreturned library materials and other resources or fees associated with their abuses, loss and damage.

The administration should only require such personal information as necessary to enable recovery of said resources and expenses associated with their recovery and hold all such information as private and confidential subject only to limitations set forth by federal and state statutes.

1. Notice & Openness

The District affirms that its patrons have the right of "notice" — to be informed about the policies governing the amount and retention of personally identifiable information, and about why that information is necessary for the provision of library services.

In all cases the District avoids creating unnecessary records. The District avoids retaining records not needed for the fulfillment of the mission of the library and does not engage in practices that might place information on public view.

The Nevada Revised Statutes Chapter 239 limits the District's authority to establish policy regarding the disposition of certain public records. Federal law, including the U.S. Patriot Act (October, 2001), may further limit the State of Nevada's and the District's ability to protect the confidentiality of patron records.

NRS Chapter 239.013 provides:

> Any records of a public library or other library which contain the identity of a user and the books, documents, films, recordings or other property of the library which he used are confidential and not public books or records within the meaning of NRS 239.010. Such records may be disclosed only in response to an order issued by a court upon a finding that the disclosure of such records is necessary to protect the public safety or to prosecute a crime.

In accordance with NRS 239, the District will not retain any records pertaining to a patron's use of library resources longer than necessary to provide appropriate stewardship of those resources. This policy applies to library circulation records, tape back ups, financial records pertaining to payment for lost or damaged materials, computer use records and all other records linking a patron's personally identifiable information to the library resource used.

Example: District records that link a patron's identity to the use of library materials will be expunged upon the return in good standing of loaned materials to the District.

2. Choice & Consent

The District will not collect or retain private and personally identifiable patron information without the patron's consent. Further, if a patron consents to provide personally identifiable information, the District will keep it confidential and will not sell, license or disclose personal information to any third party without patron consent, unless compelled to do so under the law or to comply with a court or other enforceable order presented by a law enforcement agency. Such orders are to be presented to the Executive Director or his or her designee and will be reviewed by counsel to assure compliance with applicable law prior to release of patron information.

In order to provide borrowing privileges, the District must obtain certain information about its patrons. When visiting the District's web site and using the District's electronic services, a patron may choose to provide his or her name, e-mail address, library card barcode, phone number or home address.

A patron has the option of providing an e-mail address for the purpose of notification about their library account and may request that the District remove the e-mail address from his or her record at any time.

The District never uses or shares the personally identifiable information provided to it on-line in ways unrelated to the ones described above without also providing its patrons an opportunity to prohibit such unrelated uses, unless the District is compelled to do so under the law or to comply with a court or other enforceable order as outlined above.

3. Access by Users

Individuals who use library services that require the function and process of personally identifiable information are entitled to view and/or update their information. To protect patron privacy, patrons may only update personal information in person (except e-mail address and PIN [personal identification number] on-line, and patrons may be asked to provide verification of identity through a PIN or authorized identification card.

The purpose of accessing and updating personally identifiable information is to ensure that library operations can function properly. Such functions may include notification of overdue items, recalls, reminders, etc. District staff will explain the process of accessing or updating information so that all personally identifiable information is accurate and up to date.

4. Children's Information

In accordance with the Children's Online Privacy Protection Act (COPPA), the District's website does not collect or store any personal information, even in aggregate, about children under the age of 13. We will never disclose a child's personal information as full name, address, etc. ("information that would facilitate or enable the physical or online locating and contacting of a specific individual") without written approval from a parent or legal guardian.

Information gathered online or in person by the District for the summer Club Read program is maintained from the first of June through the end of September. This stand-alone platform/ software package is not a part of the District's website. Any information collected online in this system is for the sole, one-time purpose of registering for random prize drawings related to Club Read. Any contact made to award a prize is made through the parent, via the email address or phone number provided by the parent at time of registration. In September of the same year that the data is collected, all data related to Club Read is purged.

5. Data Integrity & Security

Data Integrity: The data collected and maintained at the District's libraries must be accurate and secure. The District takes reasonable steps to assure data integrity, including: using only reputable sources of data; providing the District's users access to their own personally identifiable data; updating data whenever possible; utilizing middleware authentication systems that authorize use without requiring personally identifiable information; destroying untimely data or converting it to anonymous form.

Data Retention: The District protects personally identifiable information from unauthorized disclosure once it is no longer needed to manage library services. Information that should be regularly purged or shredded includes personally identifiable information on library resource use, material circulation history, and security/surveillance tapes and logs.

Tracking Users: The District removes links between patron records and materials borrowed when items are returned or when a patron's use of services has been completed, and deletes records as soon as the original purpose for data collection has been satisfied. The District permits in-house access to information in all formats without creating a data trail. The District has invested in appropriate technology to protect the security of any personally identifiable information while it is in the library's custody, and ensures that aggregate, summary data is stripped of personally identifiable information. The District does not ask library visitors or web site users to identify themselves or reveal any personal information unless they are borrowing materials, requesting special

services, registering for selected services, programs or classes, or making remote use from outside the library of those portions of the library's web site restricted to registered borrowers under license agreements or other special arrangements. The District discourages users from choosing passwords or PINs that could reveal their identity, including social security numbers. The District regularly removes cookies, web history, cached files, or other computer and Internet use records and other software code that is placed on the District's computers or networks.

Third Party Security: The District ensures through periodic audits that its contracts, licenses, and offsite computer service arrangements reflect the District's policies and legal obligations concerning user privacy and confidentiality. Should a third party require access to patrons' personally identifiable information, the District's agreements address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that personally identifiable information may be disclosed, the District will warn the patron. When connecting to licensed databases outside the library, the District releases only information that authenticates patrons as "members of the District's community." Nevertheless, the District advises patrons of the limits to library privacy protection when accessing remote sites.

Cookies: Users of networked computers will need to enable cookies in order to access a number of resources available through the library. A cookie is a small file sent to the browser by a web site each time that site is visited. Cookies are stored on the user's computer and can potentially transmit personal information. Cookies are often used to remember information about preferences and pages visited. A patron can refuse to accept cookies, can disable cookies, and remove cookies from his or her hard drive. The District's library servers use cookies solely to verify that a person is an authorized user in order to allow access to licensed library resources and to customize web pages to that user's specification. Cookies sent by the District's library servers will disappear when the user's computer browser is closed. The District will not share cookies information with external third parties.

Security Measures: The District's security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. The District's managerial measures include internal organizational procedures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. The District's technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and storage of data on secure servers or computers that are inaccessible from a modem or network connection.

Staff Access to Personal Data: The District permits only authorized library staff with assigned confidential passwords to access personal data stored in the

District's computer system for the purpose of performing library work. The District will not disclose any personal data the District collects about its patrons to any other party except where required by law or to fulfill an individual patron's service request. The library does not sell or lease patrons' personal information to companies, universities, or individuals.

Security Cameras: Security cameras are installed at various branch libraries to assist security personnel and staff in monitoring and quickly responding to situations affecting the health and safety of library visitors and staff. Recordings from security cameras are stored no longer than 10 days, unless an incident occurs that requires holding the entire recording or a portion of the recording longer. Security camera recordings are only made available to law enforcement through a legal subpoena or lawful court order. Library security cameras are limited to locations and uses that do not violate the reasonable expectation of privacy. Public use areas include, but are not limited to: the grounds, parking lots, entrances and interior hallways.

6. Enforcement & Redress

The District will not share data on individuals with third parties unless required by law as previously noted this policy. The District conducts periodic privacy audits in order to ensure that all library programs and services are enforcing the District's privacy policy. Library users who have questions, concerns, or complaints about the District's handling of their privacy and confidentiality rights should file written comments with the Executive Director of the Library District. The District will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures.

The District authorizes only the Executive Director or her/his designee to receive or comply with requests from law enforcement officers, who will confer with the District's legal counsel before determining the proper response. The District will not make library records available to any agency of state, federal, or local government unless a subpoena, warrant, court or other enforceable order is issued and is in proper form. The District has trained all library staff and volunteers to refer any law enforcement inquiries to library administrators.