Pleasanton Public Library Privacy Policy

The Pleasanton Public Library's mission is "To build community through exceptional services and inclusive programming. Discover, Connect, Belong." To fulfill this mission, the library provides free and equal access to services while prioritizing the privacy of users' personal information. The Library Privacy Policy affirms this commitment by outlining how the library collects, uses, and safeguards user information while helping community members understand their privacy rights when using library services.

Table of Contents

Library Privacy Principles

Library users have the right to privacy and confidentiality. The Pleasanton Public Library upholds the principles of the American Library Association as outlined in Article VII in the Library Bill of Rights, which emphasizes that "All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use." Additionally, the library affirms its ethical duty to “advocate for, educate about, and protect people’s privacy, safeguarding all library use data, including personally identifiable information.”

The library is dedicated to safeguarding privacy by:

- Taking reasonable measures to protect the confidentiality of all library users
- Collecting only the minimum personal data necessary to provide library services
- Ensuring transparency of third-party services that collect, use, or share data
- Limiting the disclosure of library records to circumstances defined by state law.

To safeguard library user records, the library:

- Securely stores physical data
- Uses encryption for storing and transmitting electronic data
- Restricts data use to its intended purpose
- Deletes data securely once it is no longer needed
- Provides staff with ongoing privacy training.

Libraries and California State Law

Library Records and Legal Protections

California Government Code § 7927.100 - § 7927.105, titled *"Library Records and Similar Matters,"* protects library records from public disclosure, with limited exceptions. These records include any written or electronic documentation identifying a library member, such as borrowing history, name, address, telephone number, or email address.

Library records may be accessed by City staff only as necessary to perform their official duties, in accordance with California Government Code § 7927.305.

The library may only disclose records to law enforcement if presented with a valid subpoena, warrant, or court order, as required by California Government Code § 7927.505. Requests for library records by law enforcement or other entities must be accompanied by a valid subpoena, warrant, or court order. The privacy protections described in California Government Code § 7927.505 do not distinguish between adult

records and minor records. The City Attorney will review requests to ensure compliance with state and federal privacy protections.

Public Record Requests

California Government Code § 7927.105 explicitly exempts library records from public disclosure under the California Public Records Act (CPRA). This provision ensures that personal information and borrowing histories remain confidential, with disclosure only allowed under specific legal circumstances.

In alignment with these laws, the library will not release records in response to public records requests.

Library Services and Personal Data

Data Collected from Library Users

The library may collect personal data directly from users of library services, such as signing up for a library card, attending classes and events, and reserving meeting rooms. The library aims to collect the least amount of data and only what is essential for providing library services. Personal data collected by the library may include:

- Name
- Physical address
- Email address
- Telephone number
- Birth year
- Student ID number (for PUSD Student Success Library Cards)
- Grade level (for PUSD Student Success Library Cards)
- School name (for PUSD Student Success Library Cards)
- Teacher or intervention specialist (for PUSD students referred to Paws to Read or students participating in School Field Trips).

The library may also collect data about a user's library activities, such as:

- Materials checked out to a member, including items that are overdue or billed
- Class and event attendance through registration and survey forms
- Inquiries sent to the library through email, web form, phone, mail or in person
- ADA accommodation requests for library program participants
- Computer/network information: The City collects certain information about devices connected to its wired and wireless network, including Media Access Control (MAC) addresses, device types, and connection timestamps

- Borrowing history: Members can save their history in their online library account. This feature must be manually activated and can be disabled at any time.

Student Success Library Program

The Library may also collect data from other sources, such as the Pleasanton Unified School District (PUSD) for the Student Success Library Card Program. As outlined in Section D of the Memorandum of Understanding between the City of Pleasanton and PUSD related to Library Cards:

> *"To the extent that Library staff have access to any personally identifiable information from student records: (1) it will not use such information for any purpose, including targeted advertising, except for the legitimate educational purpose of providing services pursuant to this MOU; and (2) it shall not disclose this information to any other party for any reason, except as required by law (§ 49073.1(b)(3) and (9))."*

Library Member Services

Account Access and Notifications

When new members sign up for a library card, they complete an online or paper application that asks for their name, physical address, email address, telephone number, birth year, and four-digit PIN.

After registering for a card, members can access several options for managing their library account and checkouts:

- Set up an online account through the library's catalog software to access their accounts online, view checked out items and renew and request materials
- Use library card number and PIN to check out physical materials. A physical card can be used for checkout, or a digital card can be stored in the Pleasanton Library App
- Designate another user to check out materials on their account. The member and the authorized user must visit the library together to set this up. This designation allows the authorized user limited access to the library member's account, including the physical address, email address, and phone number on file
- Contact library staff at any time to request to review or update the personal data in their accounts
- For security, when a library member requests account information or updates personal information, staff will ask for their library card number or photo identification to verify their identity.

The Library also provides various notification methods to help members track the due dates of their materials. Library members may be notified that an item is due through

email or text message through the online catalog, depending on the preferences they provide for their account. These preferences can be changed at any time by notifying library staff.

Library Reserves

Library materials on hold for pickup are shelved in a public area, except for LINK+ items on loan from other libraries. Each item on hold contains a slip with the name of the member who reserved the item. Members may contact the Library if they prefer to have items placed on hold in a staff area at Member Services for privacy reasons.

Collection Agency Accounts

When a library account with past-due items remains unresolved for over 60 days, it may be referred to a collection agency that manages lost or damaged material fees on behalf of the City.

The City provides the collection agency with only the minimum personal data required to seek payment. This includes the library member's name, address, phone number, email address, and the replacement cost for lost or damaged materials.

Youth Account Permissions

If a library member is younger than 14, a parent or legal guardian is the account owner and has access to their account and library record.

When a member turns 14, the youth member becomes the account owner. At that point, the parent or legal guardian has limited access to account information, such as information required for billing purposes, unless their child provides permission to share the full library account information with their parent or legal guardian.

Library Member Accounts and Retention

Library staff annually reviews expired or inactive member accounts and eCards to determine eligibility for deletion:

- Paper library card applications are shredded once the information is inputted by staff into the Integrated Library System (ILS) software system
- Library members are asked to renew their accounts every four years
- Library accounts are deleted annually at the end of the calendar year if they have expired for over four years, provided no outstanding balances or unreturned materials exist
- eCards, valid for 30 days, are deleted after one year if they remain inactive
- The checkout history of each library item in the collection, which is connected to library member accounts in the ILS, is retained for one year before being automatically removed
- Library accounts retain payment histories with the titles of the items billed and paid indefinitely.

Library Program Participation Data

Program Registration and Surveys

Pleasanton Public Library collects data related to its programs to improve services and track participation:

- Program registration information, which includes names and email addresses, is stored in the Library's online event system and is only accessible to library staff
- Participants submit program surveys through the City's survey provider. City staff access and use survey data for program planning and vendor privacy policies, available on the Library's website.

Pleasanton Reads Literacy Program Data Collection

The Library's Pleasanton Reads Literacy Program collects personal data to match students with tutors. Some personal data is collected because the State of California grant agency, California Library Literacy Services (CLLS), requires collecting this data for funding and reporting purposes.

Data collected for the Pleasanton Reads Literacy Program may include:

- Telephone
- Address
- Phone number
- Email
- Birth year
- Gender
- Race
- Ethnicity
- Education
- Home country
- Primary language
- Written goals for literacy learners.

Program Participation and Retention

Program registration information is archived in the Library's events platform and retained for two years, consistent with the Library's general record retention schedule (Section 1406-2 of the City Records Retention Schedule, 2008).

For the Pleasanton Reads Literacy Program, the Library retains records related to grant programs for five years after it submits its final expenditure report for the funding cycle

under which the program was awarded, as required by the State of California. Grant program records without personally identifying information, such as program statistics and financial reports, are retained longer for planning purposes.

Third-Party Library Services

Data Practices and Third-Party Services

Pleasanton Public Library partners with third-party vendors to offer services such as e-books, streaming media, research databases, the online catalog, and the library app. These vendors may collect and use data about library members' interactions with their services, including:

- Information provided by library members (e.g., when creating an account)
- Shared data such as name and email address
- Browser, operating system, and device details
- Web page addresses visited, along with timestamps
- Library members' IP address and location
- Social media account information and content and inferred data.

Each third-party service has its own privacy policy and data practices, which determine how it collects, uses, and shares information. California law requires third parties acting on behalf of the Library to protect the privacy and confidentiality of data.

The City of Pleasanton regularly reviews vendor agreements on their renewal cycle to ensure privacy compliance. City IT staff review all software agreements to verify compliance with security and privacy requirements. The City will not enter into agreements with vendors that do not meet these standards.

Vendor Privacy Policies and information about their data practices are updated regularly on the Library's Vendor Privacy Policy webpage.

Library Website Privacy

Data Collection and Tracking Tools

The City of Pleasanton maintains the library web pages and uses analytics tools to collect data such as:

- Browser, operating system, and other information about the device used to visit the website
- Addresses of the web pages visited
- The time and date the website was visited

- The visitor's internet address (i.e., IP address).

Cookies and Web Browser Settings

The City website uses cookies, which are small files sent to a web browser to store and send data. Website users can set their browsers to reject these cookies. To learn more, website users may review the City of Pleasanton Privacy Policy.

Library Public Computers and Internet Access

Pleasanton Public Library provides access to public computers, printers, and wireless Internet, and City IT maintains this access.

Privacy Considerations for Public Computer Use

The Library's Public Access to the Internet Policy addresses privacy regarding public computers and network access

Library users of public computers are advised of this policy on the screen each time they log in to use a computer at the Library

Parents and legal guardians are responsible for the safety and security of their children while using public library computers.

Internet Filters

Technology protection measures (or "internet filters") block or filter the Internet, other forms of electronic communications, and access to inappropriate information.

As required by the Children's Internet Protection Act (CIPA), filters are applied in the children's area of the Library to visual depictions of material deemed obscene or child pornography or to any material deemed harmful to minors. Individuals requesting access to the Internet without these filters are directed to use the computers in the adult computer area.

Security Measures

The City of Pleasanton makes every effort to ensure public computers have basic security measures. Library members should exercise caution and follow online security best practices when using public computers:

- Users should sign out of all accounts and delete any personal files saved on the computer at the end of the session. Public computers do not automatically delete personal data when users end their session
- Public computers are in a public area where individuals can see the content on others' computer screens
- Users may connect to the wireless network using their own device or one of the Library's Take-Home Laptops and move to another building area for more privacy.

Public Computer Data and Retention

The City of Pleasanton does not track computer or network use, such as reading or sending emails, website visits, or working on files.

The City collects certain information about devices connected to its wired and wireless networks, including:

- MAC Addresses: The unique identifier assigned to a device's network interface
- Device Types: Information about the type of device being used (e.g., smartphone, tablet, laptop)
- Connection Timestamps: The time and date a device connects to and disconnects from our network
- Bandwidth Usage: The amount of data transferred to and from a device while connected to the City network.

This data is collected to manage network performance, troubleshoot connectivity issues, ensure fair usage of the network resources, enhance overall service quality, and maintain cybersecurity. Additionally, the data may be used for investigative purposes if there are incidents or concerns regarding network security or misuse.

Usage logs are retained for one year to facilitate the analysis and resolution of technical issues, optimize network management, enhance cybersecurity, and support investigative efforts if necessary. After this period, they are securely deleted to protect user privacy.

Library Take-Home Laptops and Mobile Hotspots

Pleasanton Public Library offers take-home laptops and mobile hotspots for adult library members ages 18 and older. Devices can be checked out for three weeks. Laptop borrowers must complete the Take-Home Laptop Loan Agreement each time they check out a device and confirm it is in working order before leaving the Library.

Mobile Hotspots

- The Library provides hotspots to check out
- Hotspots do not track or log user data usage. However, the service provider may collect data in accordance with their privacy policy.

Laptop User Responsibilities

The City of Pleasanton makes every effort to ensure that Take-Home Laptops have basic security measures at checkout, including secure browser settings and up-to-date software patches. Laptop users sign an agreement to borrow a device that provides information on online security and data protection measures.

Once a laptop is in the borrower's possession, library users should exercise caution and follow online security best as outlined in the Take-Home Laptop Loan Agreement.

Laptop Security and Monitoring

All data handling follows established privacy laws designed to protect user information. When library users sign in to a Take-Home Laptop, they may see a notification stating that the device is managed by cityofpleasantonca.gov. City IT manages the laptops available through the Library's Take-Home Laptop service to ensure they are up-to-date, secure, and function optimally.

As part of the City's commitment to maintaining the security and integrity of the Take-Home Laptops, the following information may be monitored:

- User Access Logs: Records of who has used the device and when. This is used solely for operational and security purposes
- Networking Information: IP addresses, interface configurations, and connection quality. This helps troubleshoot connectivity issues and improve network services.

Laptop Usage Logs and Data Handling

As part of the City's commitment to ensuring the best possible user experience and maintaining the integrity of library devices, the following information may be monitored:

- User Access Logs: Records of device usage, including timestamps. These logs are used solely for operational and security purposes and do not track personal activity
- Networking Information: IP addresses, interface configurations, and connection quality to troubleshoot connectivity issues and improve network services.

Data is collected strictly for administrative and security purposes, not for personal surveillance or profit.

While the City of Pleasanton does not monitor personal activities on Take-Home Laptops and Chromebooks, City IT maintains device usage logs for security and troubleshooting. These logs record access times and network diagnostics but do not capture or store personal browsing history or content.

Library users are responsible for safeguarding the device during the loan period, including applying for updates and avoiding potentially harmful websites.

Laptop Data Protection Measures

- The City of Pleasanton takes privacy and data security seriously. The City does not access or use personal data beyond the minimum required for device management and operational purposes. All data handling follows established privacy laws and City policies designed to protect library user information.

- Device Reset and Data Purge: Laptops are reset and data purged upon return, but users are encouraged to sign out of all programs before returning.

Library Privacy Policy Commitment

Pleasanton Public Library is committed to protecting member privacy and continuously improving its Privacy Policy. This commitment includes:

- Reviewing and updating privacy practices whenever new services and resources are introduced or modified
- Regularly updating the Privacy Policy to reflect changes in library services, technology, and data practices, with updates communicated through the Pleasanton Public Library website
- Maintaining a comprehensive, publicly accessible list of Vendor Privacy Practices on the library website
- Providing staff with ongoing training to assist members with privacy-related questions regarding library services and digital resources.

Emerging Technologies and Artificial Intelligence (AI)

The Pleasanton Public Library acknowledges the increasing role of artificial intelligence (AI) in digital tools and services, including potential impacts on user privacy. The Library is committed to ensuring transparency and security regarding AI technologies, adhering to ethical AI use and data minimization principles. The following guidelines apply:

- Transparency: Library users will be informed when AI technologies are incorporated into library-provided services, applications or resources
- Consent and Awareness: The Library will communicate the scope of data collection, processing, and analysis by any AI system integrated into Library services, ensuring informed consent wherever feasible
- Data Minimization and Purpose Limitation: AI systems used by the Library will collect and process only the minimum data necessary for their intended functions and clearly defined purposes. Library staff will not input or upload patron personally identifiable information (PII) into any AI tools, including generative AI or third-party AI-powered platforms, unless the city has formally reviewed and approved those tools for privacy, security and appropriate use
- Bias and Fairness: The Library strives to utilize AI systems that are transparent, equitable and unbiased, ensuring they do not disproportionately impact or disadvantage any group or individual
- Regular Review and Compliance: The Library will regularly review AI technologies and their usage for privacy impacts, compliance with relevant

privacy laws, and alignment with the City's forthcoming overarching AI and administrative AI policies

- Training and Staff Awareness: Library staff will receive ongoing training on AI privacy and ethical practices to assist patrons effectively and responsibly
- Collaboration with City Policies: The Library's practices regarding AI will align with broader citywide administrative and ethical guidelines for AI usage once finalized and adopted.

Staying Connected

Library members are encouraged to review the Privacy Policy regularly to stay informed about how the library protects user privacy.

Members may contact the Library Administration for questions or concerns about their privacy rights at the library.

Glossary of Terms

- **Americans with Disabilities Act (ADA) Accommodation Requests** – Requests made by library members for accessibility accommodations to participate in library programs or services.
- **American Library Association (ALA) Bill of Rights** – A guiding document that outlines fundamental library principles, including intellectual freedom, access to information, and privacy.
- **Authorized User** – A person designated by a library member to access their account and check out materials on their behalf.
- **Borrowing History** – A record of past checkouts by a library member, which is only stored if the member manually enables this feature in their online account.
- **Browser** – A software application used to access websites and online services, including the Library's online catalog.
- **Children's Internet Protection Act (CIPA)** – A federal law requiring internet filtering on library public computers to block inappropriate content for minors.
- **City IT** – The City of Pleasanton's Information Technology department, responsible for managing and securing the City's technology infrastructure.
- **Cloud Services** – Online data storage and computing services used to store information securely, including patron data protection and backup.
- **Collection Agency** – A third-party agency that manages overdue or lost library materials and associated fees.

- **Connection Timestamps** – Records of the time and date a device connects to and disconnects from a network, used for performance monitoring.
- **Cookies** – Small data files stored on a user's device by a website to track and improve user experience. These can often be disabled in browser settings.
- **Customer Relationship Management (CLM) system** – The Library's help desk system for managing and responding to patron inquiries.
- **Cybersecurity** – Measures taken to protect digital data and network infrastructure from unauthorized access, hacking, or cyber threats.
- **Data Practices** – Policies and procedures governing how personal and library-related data is collected, stored, shared, and deleted.
- **Data Purge** – The process of securely deleting personal or sensitive data when it is no longer needed.
- **eCards** – Temporary digital library cards that provide access to online resources for a limited period before requiring full registration.
- **Encryption** – A security process that encodes electronic data to protect it from unauthorized access.
- **People Counting Software** – A system that utilizes sensors to track foot traffic in the Library.
- **Web Analytics** – Web analytics services track and report website traffic, user interactions, and other data.
- **Internet Filters** – Software tools that restrict access to certain online content, used in libraries to comply with CIPA requirements.
- **Library Member** – An individual with an active Pleasanton Public Library card who has access to borrowing materials.
- **Library Records** – Any documentation related to a library member's account, including borrowing history, personal information, and communications with the library.
- **LINK+** – A resource-sharing network that allows library users to borrow materials from participating academic and public libraries across California and Nevada.
- **Loan Records/Checkout History** – A record of materials borrowed by a library member.
- **MAC Address (Media Access Control Address)** – A unique identifier assigned to a device's network interface, used for network management and security.
- **Memorandum of Understanding (MOU)** – A formal agreement outlining responsibilities between organizations, such as the Library and the Pleasanton Unified School District.

- **Mobile Hotspots** – Portable devices that adult library members can borrow to access the Internet through a vendor's cellular network.
- **Network Diagnostics** – The process of analyzing network performance and identifying technical issues to ensure reliable and secure internet access.
- **Online Catalog** – The Library's digital system where members can search for materials, place holds, renew checkouts, and manage their accounts.
- **Operating System (OS)** – The software that manages a device's hardware and software resources (e.g., Windows, macOS, Android, iOS, ChromeOS).
- **Personally Identifiable Information (PII)** – Any data that can identify an individual, such as name, address, phone number, or email.
- **Phishing** – A type of cyberattack where scammers attempt to obtain sensitive information through emails, messages, or websites.
- **PIN (Personal Identification Number)** – A secure code set by a library member that allows access to their online account and self-service features.
- **Integrated Library System (ILS)** – A library software used by staff for item cataloging, circulation, patron records, acquisitions, and statistical reports.
- **Public Records Act (CPRA - California Public Records Act)** – A state law that allows public access to government records but exempts library user records from disclosure.
- **Retention Schedule** – A policy outlining how long the Library keeps certain records before securely deleting them.
- **Student Success Library Card Program** – A partnership between schools and public libraries in which a Student ID functions as a Library Card for easy access.
- **Take-Home Laptops** – Laptops that adult library members can borrow for a period of three weeks.
- **Third-Party/Vendor Services** – Digital platforms or vendors that provide online library services, such as e-books, databases, and event management systems. The Library's Vendor Privacy Policy webpage has a complete list of vendors and third-party services, along with links to their privacy policies.
- **VPN (Virtual Private Network)** – A security tool that encrypts internet traffic to protect user privacy and prevent tracking while online.
- **Web Analytics** – Services that track and report website traffic, user interactions, and other data.
- **Wireless Network** – A system that allows library users to connect their devices to the Internet while visiting the facility.

Related Policies and Regulations

- Library Bill of Rights – https://www.ala.org/advocacy/intfreedom/librarybill
- California Government Code – https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=GOV&division=10.&title=1.&part=5.&chapter=7.&article=
- City Website Privacy Policy – https://www.cityofpleasantonca.gov/privacy-policy/
- Pleasanton Public Library, Public Access to the Internet Policy – https://www.cityofpleasantonca.gov/assets/your-community/library/public-access-to-internet.pdf

Approval by Library Commission, April 3, 2025

Approval by City Council, July 15, 2025

Next scheduled update: July 2030