11 – Privacy Policy

11-1 Introduction

The Palatine Public Library District (the Library) is strongly committed to protecting the privacy of our users. We believe that privacy is essential to the exercise of free speech, free thought, and free association, and we have created this Privacy Policy so that users can understand what the Library does with information that is collected. By using the Library's services, including our website, users agree to be bound by the terms of this Privacy Policy.

At the Library, the right to privacy includes 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.

Courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution. Many states, including Illinois, provide mandates of privacy in their constitutions and statutory law. Numerous decisions in case law have defined and extended rights to privacy. Under Illinois state law, the Library is subject to the provisions of The Library Records Confidentiality Act (75 ILCS 70/1 et seq.). The Library's privacy and confidentiality policies intend to be in compliance with applicable federal, state, and local laws.

The Library's commitment to privacy and confidentiality has deep roots not only in law but also in the ethics and practices of librarianship. In accordance with the spirit of the American Library Association's Code of Ethics, the Library protects each user's right to privacy and confidentiality with respect to services sought or received and resources consulted, borrowed, acquired, utilized, or transmitted. (Revised 8-10-11, Effective 8-10-11; Reapproved 3-13-13; Revised 3-11-15, Effective 4-1-15; Reapproved 4-12-17)

11-2 Notice of Information Gathered

The Library affirms that users have the right of "notice" – to be informed about the policies governing the gathering, retention and removal of personally identifiable information and about why that information is necessary for the provision of library service.

Information the Library may gather about users includes the following:

a. Library card registration information such as full name, full address, telephone number, and a photographic image. Additional registration information gathered for those under 14 years of age includes the user's birth date and the full name and address of the parent or legal guardian. Such information is provided voluntarily by users to qualify for borrowing privileges and access to other library services;

b. Circulation information such as a record of materials currently checked out, lost or damaged and fines and fees incurred;

c. An e-mail address provided voluntarily by users. This allows for a convenient means to receive circulation notices and updates on library resources and programs;

d. A borrower's card number, required to access most services;

e. Information relating to registration for library programs including library-wide reading programs;

f. Information relating to meeting room booking, such as the name of requesting organization, resident cardholder making application, purpose of meetings, and status as a profit or not-for-profit organization; and

g. Other information reasonably required in the orderly provision of library services.

The Library avoids creating unnecessary records. The Library intends to remove records no longer needed for the provision of library services. The Library intends to avoid practices that might place personally identifiable information on public view. (Revised 8-10-11, Effective 8-10-11; Reapproved 3-13-13, Revised 3-11-15, Effective 4-1-15; Reapproved 4-12-17)

11-3 Disclosure

The Library strives to keep confidential any and all personally identifiable information under its control. The Library will not sell, license, or disclose information to any third party without the user's consent, unless compelled to do so under the law or to comply with a court order. With the user's prior consent, the Library may disclose personally identifiable information to other institutions to facilitate access to library services such as reciprocal borrowing or interlibrary loan. The Library may disclose

information to institutions such as a collection agency in order to protect library resources from loss or damage and to collect fees owed to the Library.

The Library will grant access to library-controlled information about children who have not reached 14 years of age to their custodial parents, legal guardians, or legal foster parents. (See Policy 2**:** Library Cards and Accounts section on Youth)

The Library provides a mechanism by which a patron may grant access to their own personally identifiable information to others to aid in obtaining library services. (See Policy 2: Library Cards and Accounts section on Linking Records) (Revised 8-10-11, Effective 8-10-11; Reapproved 3-13-13; Revised 3-11-15, Effective 4-1-15; Reapproved 4-12-17)

11-4 Access by Users

Users are entitled to view and/or request updates to their personally identifiable information. Users must be able to verify their identity when accessing such information.

The Library may offer users the opportunity to create their own lists relating to reading, viewing and listening preferences. Such lists would be voluntarily created and modified by users. Users might elect to receive notification from the library of new materials acquired based on such lists. Such information will be protected under this privacy policy. (Reapproved 3-13-13; Reapproved 3-11-15; Reapproved 4-12-17)

11-5 Data Integrity & Security

Data Integrity: The data the Library collects and maintains should be accurate and secure. The Library takes reasonable steps to assure data integrity, including using only reputable sources of data; providing users access to their own personally identifiable data; updating data whenever possible; and destroying data no longer needed.

Data Retention: The Library protects personally identifiable information from unauthorized disclosure. Information is purged or shredded when it is no longer needed. Information that is regularly purged or shredded includes personally identifiable information on library resource use, material circulation history, and security/surveillance data.

Tracking Use: The Library removes links between patron records and materials borrowed. The Library deletes records as soon as the original purpose for data collection has been fulfilled. To protect against loss or damage to the collection, the Library may maintain a link between an item

and the most recent prior checkout of that item. As explained in the Homebound Services Policy, the Library maintains a record of all items checked out by a homebound patron for purposes of selecting materials for that person. (See Policy 3: Library Operations section on Homebound Services)

The Library permits in-house access to information in all formats without creating a data trail. The Library does not request or reveal any personal identification information unless users are borrowing materials, requesting special services, registering for programs or classes, reserving or utilizing computer stations, or making remote use of those portions of the Library's website restricted to registered borrowers under license agreements or other special arrangements. The Library regularly removes cookies, history, cached files, or other computer and Internet use records that are temporarily retained on its computers or networks.

Third Party Security: The Library strives to ensure that contracts, licenses, and offsite computer service arrangements reflect Library policies and legal obligations concerning patron privacy and confidentiality. Should a third party require access to a user's personally identifiable information, agreements specify appropriate restrictions on the use, aggregation, dissemination, and sale of that information. When users are remotely connecting to licensed databases, the Library will release only information that authenticates users as valid cardholders.

Security Measures: The Library's security measures involve both managerial and technical policies and procedures to protect against loss and the unauthorized access, destruction, use, or disclosure of data. The Library has internal organizational procedures which limit access to data and which include safeguards so that individuals with access do not utilize the data for unauthorized purposes.

The Library will take all measures reasonably necessary to protect the security, confidentiality, and integrity of "personal information" as defined in the Personal Information Protection Act, 815 ILCS 530/1, et seq.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records. Any suspected breach or compromise of the security of data which contains personal information will be investigated promptly by the Library Director or designee. Using personal information for a purpose unrelated to the business of the Library, and making personal information available in order to further disclosures that are unauthorized, also constitute breaches or compromises of the security of the data. The provisions of this paragraph are as defined or stated in 815 ILCS 530/5.

The Director may consult with local law enforcement officials and/or the Library's attorney before making a determination as to notifying the affected individuals that there has been a breach of data which contains personal information.

If notice to the affected individuals is appropriate, notice will be given in accordance with the Personal Information Protection Act. "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

A. Social Security number,
B. Driver's license number or state identification card number
C. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's account

Only the Library Director or designee will contact any individual about a suspected breach or compromise of the security of data which contains personal information. Every such security-related incident must be reported immediately to the Library Director or designee. (Revised 8-10-11, Effective 8-10-11; Revised 3-13-13, Effective 3-13-13; Revised 3-11-15, Effective 4-1-15; Revised 4-12-17; Effective 5-1-17)

11-6 Library Website Security

The Palatine Public Library District is strongly committed to protecting the privacy of its online users. The Library is supported in protecting the privacy of its users by national and state-level laws, as well as the Library's Privacy Policy.

Type of Information Collected: Where it is necessary for the Library to identify users, the Library collects only the minimum information necessary and retains that information for only as long as it is needed to fulfill its purpose. This information may include IP address, browser type, domain names, access times, and referring website addresses. Additionally, personally identifiable information may be transmitted in connection with other activities, services, or resources made available on our site.

How the Information Is Used: The information is used by the Library for the operation of a service, to maintain quality of a service, and to provide general statistics regarding use of websites. Any personally identifiable information provided is maintained by and accessible only to the Library unless the Library explicitly states otherwise. The Palatine Public Library

District does not sell, rent, lease, or otherwise provide its cardholder lists to third parties.

While remaining committed to user privacy, the Library may be forced to disclose information to the government or third parties where necessary to comply with law. In addition, in the unlikely event that the Library needs to investigate or resolve problems or inquiries associated with the operation of the library, it may be necessary to disclose information to parties outside of the library, such as law enforcement or other government officials.

Third-Party Websites: The Library website contains links to websites and resources owned and operated by third parties, including databases and electronic journals, which the Library has licensed for its users. While every attempt is made to include user information protections in license agreements with these third parties, use of these websites and resources is not governed by the Library's Privacy Policy. Such websites are governed by their own privacy policies.

Security: The Library has taken reasonable measures to safeguard the integrity of its data and prevent unauthorized access to information maintained. Steps include, but are not limited to, authentication, monitoring, and auditing. Security measures have been integrated into the design, implementation and day-to-day practices of the entire operating environment. These measures are intended to prevent corruption of data, block unknown or unauthorized access to library systems and information, and to provide reasonable protection of private information held by the Library. For example, information required when making online credit card payments for Library fines or fees, is encrypted and transmitted via secure connection to the Library's payment service. No security measures, however, can guarantee complete security from unauthorized "hackers."

Cookies: A "cookie" is information that a website may place on a computer's hard drive to collect information about a user. A cookie records an individual's preferences in using a certain website. The Palatine Public Library District does not use any persistent cookies to collect permanent information. The Library may use non-persistent cookies in applications that keep track of a user's session. Non-persistent cookies are only necessary to maintain session information and are temporary. They are invalidated once a user's session is completed.

Acceptance of Terms: Using the Library's website signifies acceptance of the Library's Privacy Policy. (Adopted 8-10-11, Effective 8-10-11; Reapproved 3-13-13; Revised 3-11-15, Effective 4-1-15; Reapproved 4-12-17)

11-7 Identity Protection

The purpose of this policy is to protect social security numbers from unauthorized disclosure. The Library does not collect the social security numbers of patrons. Regarding the use of social security numbers, the Palatine Public Library District intends to comply with the provisions of the Identity Protection Act (5 ILCS 179/1 et seq.).

Requirements

1. All employees who have access to social security numbers in the course of performing their duties must be trained to protect the confidentiality of social security numbers. Training will include instructions on the proper handling of information that contains social security numbers from the time of collection through the destruction of the information.

2. Only employees who are required to use or handle information or documents that contain social security numbers will have access to such information or documents.

3. Social security numbers requested from an individual will be provided in a manner that makes the social security number easily redacted if required to be released as part of a public records request.

4. When collecting a social security number, or upon request by the individual, a statement of the purpose or purposes for which the social security number is being collected and used must be provided.

Prohibited Activities

No employee may do any of the following:

1. Publicly post or publicly display in any manner an individual’s social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the general public.

2. Print an individual’s social security number on any card required for the individual to access products or services.

3. Encode or embed an individual’s social security number in or on any cards or documents, including, but not limited to, using a barcode, chip, magnetic strip, RFID technology, or other technology.

4. Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

5. Print an individual's social security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless state or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

6. Collect, use, or disclose a social security number from an individual, unless:

    a. Required to do so under state or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities;

    b. The need and purpose for the social security number is documented before collection of the social security number; and

    c. The social security number collected is relevant to the documented need and purpose.

7. Require an individual to use his or her social security number to access an Internet website.

8. Use the social security number for any purpose other than the purpose for which it was collected.

The prohibitions listed immediately above do not apply in the following circumstances:

1. The disclosure of social security numbers pursuant to a court order, warrant, or subpoena.

2. The collection, use, or disclosure of social security numbers in order to ensure the safety of other employees.

3. The collection, use, or disclosure of social security numbers for internal verification or administrative purposes.

4. The collection or use of social security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

Public Inspection and Copying of Documents

Notwithstanding any other provision of this policy to the contrary, all employees must comply with the provisions of any other state law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's social security number. This includes requests for information or documents under the Illinois Freedom of Information Act. Employees must redact social security numbers before allowing the public inspection or copying of the information or documents.

Applicability

This policy does not apply to the collection, use, or disclosure of a social security number as required by state or federal law, rule, or regulation. (Approved 4-13-11, Effective 4-13-11; Reapproved 3-13-13; Reapproved 3-11-15; Reapproved 4-12-17)

11-8 Enforcement & Redress

The Library conducts regular privacy audits in order to ensure that all library programs and services are in compliance with this privacy policy. Library users who have questions, concerns, or complaints about the library’s handling of their privacy and confidentiality rights should file written comments with the Library Director. The Library will respond in a timely manner and may conduct a privacy investigation or review of policy and procedures. (Reapproved 3-13-13; Revised 3-11-15, Effective 4-1-15; Reapproved 4-12-17)

11-9 Release of Information from the Patron Record to Courts or Sworn Officers

The Library authorizes only the Library Director and designated Person In Charge to receive or comply with requests from law enforcement officers. The Library confers with its legal counsel before determining the proper response. The Library will only make library records available to any agency of federal, state, or local government if a subpoena, warrant, court order, or other investigatory document is issued by the Federal Government or by a court of competent jurisdiction that shows good cause and is in proper form, or if a sworn law enforcement officer states there is probable cause to believe there is imminent danger that someone will be physically harmed and that it is impractical to secure a court order as a result of an emergency. The sworn officer making such a claim must complete and sign a form (Appendix 11A) acknowledging declaration of said emergency and acknowledging receipt of the information requested from the Library.

The information released under signature of a sworn law enforcement officer will be limited to identifying a suspect, witness, or victim of a crime and will not include disclosure of registration or circulation records that indicate materials borrowed, resources reviewed, or services used at the library.

(Policy 11-9 Adopted January 9, 2008, Effective January 1, 2008; Revised 8-10-11, Effective 8-10-11, Reapproved 3-13-13; Revised 3-11-15, Effective 4-1-15; Reapproved 4-12-17)