

**Pickerington Public Library**

**Information Security Policy**

**Board Policy Date Approved: 10/21/19**

 **Effective Date: 10/21/19**

 **Replacing Policy Effective: 4/11/11**

As a state funded and locally tax supported government agency, the Pickerington Public Library (PPL) is entrusted with the duty of collecting sensitive and personal information about library staff and customers. The Library will protect information contained within its systems and services from unauthorized disclosure, modification or destruction, whether accidental or intentional. The Library will comply with Ohio Revised Code regarding the duties of state and local agencies maintaining personal information systems (ORC 1347). In addition, because credit cards are accepted for the payment of fees, PPL will comply with the Payment Card Industry Data Security Standard (PCI-DSS).

As a member of the Central Library Consortium (CLC), whose libraries constitute an interconnected or combined system in order to enable collaboration, the Library supports and abides by the Central Library Consortium Security Policy. The Library’s Information Security Policy is to be used concurrently with the CLC Security Policy.

**Administrative Procedure Date Approved: 10/21/19**

 **Effective Date: 10/21/19**

 **Replacing Procedure Effective: New**

This policy applies to all employees, full-time and part-time, temporary and permanent, and contractors and consultants who are on site. Volunteers will not be given access to customer or staff personal information.

All handling of customer records and card processing activities and related technologies will comply with this policy. Additionally, customer records are defined as “personally identifiable information about an individual who has used any library service or borrowed any library materials” according to ORC 149.432 (A)(3).

The Library Director and Information Technology (IT) Specialist are designated to oversee the Library’s Information Security Policy. They will address potential internal and external security risks to the security, confidentiality, and integrity of personal information that could result in a compromise as follows.

**Internal Risks**

1. Personal information deliberately or inadvertently given to someone via Library staff

Risk is addressed through employee training and Library management. Library managers, under the direction of the Library Director and IT Specialist, are responsible for ensuring that this policy and the responsibilities of their direct reports are communicated to Library staff and that the Library staff comply with this policy in the course of their staff duties.

Upon employment with the Pickerington Public Library, the appropriate manager will train all newly hired employees on information security policies and procedures with refresher training offered periodically during staff development sessions.

Customer records, and paper versions of adult library card applications and juvenile library card applications, will be stored securely and destroyed in accordance with the Library’s Records Retention Policy.

Cardholder records require the cardholder’s legal name, current address, and a current phone number and/or email address to communicate account information to the customer. Library cardholders are assigned a unique four-digit Personal Information Number to access their cardholder account online.

In accordance with the Library’s Cardholder Policy, cardholders are responsible for ensuring that their account information is accurate and up to date.

The laws of Ohio require a Library to provide information about a minor child to her/his parent, guardian or custodian.

All candidates for employment with the Pickerington Public Library are hired contingent on a successful background check. Volunteers ages 18 and older are also subject to background checks.

Applications for employment and background check information are securely stored and subsequently destroyed in accordance with the Records Retention Policy and its schedule.

While not considered customer or cardholder records, applications for employment for those who are not hired by the Library are also stored and destroyed according to the same policy.

Disciplinary action up to and including termination may be applied when a breach of confidentiality in regard to personal information is discovered.

1. Access to personal information via a staff computer

Risk is addressed with staff training and management. Only authorized users of Library equipment will have access to workstations and software where confidential information is stored. Authorized users include Library staff members and contract employees.

The Library requires unique logins for staff members on staff terminals and password protection on staff terminals.

Customers will not be permitted access to staff terminals under any circumstances.

Volunteers will be provided access to terminals only when those terminals do not contain, or provide access to, customer confidential information.

Authorized users must notify their direct supervisor and the IT Specialist immediately if secure information, including passwords and confidential information is lost, stolen, or shared (inadvertently or otherwise) or suspected of being lost, stolen, or shared.

Authorized users will lock all computers, laptops, and mobile devices with passwords when not in use or when devices are located at unattended terminals. Users will keep secure all mobile devices in locked staff areas when not in use.

Before any equipment that stores confidential information is discarded, sold or returned, the IT Specialist will make certain that hard drives are secured or completely erased.

**External Risks**

1. Access to personal/customer information via an outside computer or other outside source

Risk is addressed via the Central Library Consortium (CLC) firewall applications which are configured to protect cardholder data. The Library will also maintain a local firewall to protect against external intrusion.

Complex passwords will be required for access to customer information. Cardholder data across open, public networks is encrypted.

The IT Specialist will ensure that antivirus software is maintained and regularly updated, and that regular security system checks are run.

The Library will contract only with outside service providers who are capable of maintaining appropriate safeguards to customer information. Vendor-supplied defaults for system passwords and other security parameters will not used.

All third-party providers and vendors are required to uphold the Library’s Information Security Policy.

When customers pay Library fees online via Comprise SmartPay, the last four (4) digits of their credit card are encrypted and retained by comprise for audit purposes only.

**Breach of Security**

**While the Library has** put into place physical, electronic, and managerial procedures in an effort to safeguard and secure the information collected to prevent unauthorized access; to maintain data security; and to ensure the correct use of information, it cannot guarantee that information collected would never be accessed by unauthorized users.

Any security breach or suspected security breach of confidential information must be reported immediately to the Library Director and IT Specialist. The IT Specialist will investigate and respond to any suspected intrusion or firewall failure, and will notify CLC staff of the situation.

The Library Director will take disciplinary action where appropriate, when and if error on the part of specific Library staff members are involved in the breach.

The Library Director will communicate with any impacted customers and/or members of their staff. This will include notification of the breach and what steps, if any, the library will take to remedy the situation for the customer or staff member.

**Privacy Statement**

***Editor’s note: the Privacy Statement included here has been edited and adapted from the policy on the Library’s website:*** [***https://pickeringtonlibrary.org/ppl-privacy-statement/***](https://pickeringtonlibrary.org/ppl-privacy-statement/)***.***

***Any edits made to the Privacy Statement in the Information Security Policy must be updated on the website.***

The Library will not make any information about cardholders or cardholders’ use of library services or materials available to anyone or any group except to law enforcement personnel if presented with a court order, search warrant, or subpoena. If a court order, search warrant or subpoena is issued, the Library will consult legal counsel to assure the document is in proper form before complying.

In the event of special circumstances, such as emergencies involving public health or safety, that require an immediate decision, the Director or his/her designee will be contacted, and legal counsel consulted when possible.

The Library provides its customers with the opportunity to share additional personal information, beyond cardholder information, in order to personalize their Library experience: these opportunities include event registration forms and online mailing lists. The Library will use this information only to communicate information to customers and to provide the services as requested by the customer.

The Library works with third party vendors to help provide services to its customers. The Library may share information with these vendors in order to use the providers product/software. Any data shared with third party vendors must comply with Ohio law and the rules of the Information Security Policy. The Library does not sell information we collect about customers to any third party vendor.

The Library’s website includes links to third party sites. Those sites, and any others that customers choose to visit, may have different privacy statements and the Library’s Information Security Policy and Privacy Statement do not apply. The Library is not responsible for protecting personal information gathered by third party web sites.  This statement of privacy does not apply to e-mail and other electronic communications that customers send and receive outside of the Library via the Internet or through wireless communication. On the Internet, there is no reasonable expectation of privacy. For more information, please see the Library’s Computer Use and Internet Access Policy.

**Pickerington Public Library**

**Information Security Acknowledgement**

I, **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** understand that Federal and State Laws prohibit the unauthorized use of or access to personal information as defined in the Information Security Policy.

It is understood that the Pickerington Public Library is a locally tax supported government agency entrusted with the duty of collecting sensitive and personal information about library staff and customers. When obtaining personal information for the business of the Pickerington Public Library, the library employee has responsibility for safeguarding that data from unauthorized use.

“Personal information” means any information that describes anything about a person, or that indicates actions done by or to a person, or that indicates that a person possesses a certain personal characteristic, which can be retrieved from a system by a name, identifying numbers, symbol or other identifier assigned to a person.

As an employee of the Pickerington Public Library, I acknowledge that the unauthorized use of customer/staff account information is strictly prohibited and will result in disciplinary action up to and may include termination on the first offense.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_**

Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor Signature Date