Protecting Privacy Policy

Purpose
The purpose of this policy is to assist in the efforts of the Agency to be compliant with section 1347.15 of the Ohio Revised Code (ORC).

Revision Date
This policy was last revised on 23 August, 2018 (*department managers contact information only was updated.)*

Cross-Reference
- Ohio Revised Code (ORC) 1347.15
- Ohio Administrative Code (OAC) 3375-5

General Information
In order to provide library services and enable access to physical and electronic resources, the State Library of Ohio (Agency) must collect and maintain personal information about its customers. These individuals can be state employees, legislators, or members of the general public. As an employee of the State Library, it may be a job requirement to access this personal information.

It is the responsibility of all employees of the Agency to take appropriate precautions to protect the personal information and confidential personal information that the Agency maintains from unauthorized access, modification, use, or disclosure.

The State Library of Ohio is dedicated to developing and implementing information access policies and controls that enhance and ensure the privacy and security of Ohio's citizens who have information stored in the Agency's personal information systems.

§1 Definitions
Personal Information: From ORC 1347.01, personal information is 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 certain personal characteristics.

Confidential Personal Information (CPI): Personal information that is not a public record. Examples of "not a public record" are:

- Medical and health records
- Personal Benefits related information
- Social Security numbers
- Records the release of which is prohibited by state or federal law
- Library records and patron information

Protecting Privacy Policy

For more information about properly identifying Confidential Personal Information (CPI), see page 4 of Accessing Confidential Personal Information - A Guide to Section 1347.15 of the Ohio Revised Code (link provided in Section 8 of this policy).

§2 Personal Information Systems
A personal information system is a system of record that contains all of the following attributes:

- It is a group or collection of records that are kept in an organized manner in either electronic or paper formats. (See the definition of "system" in ORC 1347.01(F))
- It contains "personal information" which is a person's name or other identifier (such as SSN or driver's license number) associated with any information that describes anything about a person or indicates that a person possesses certain personal characteristics. (See the definition of "personal information" in ORC 1347.01(E))
- Personal information is retrieved from the system by name or other identifier. (See the definition of "system" in ORC 1347.01(F))
- The agency has ownership of, control over, responsibility for, or accountability for that system of record. (See the definition of "maintains" in ORC 1347.01(D))

Based on the definitions of Confidential Personal Information and Personal Information Systems, the State Library of Ohio maintains the following systems that are covered by this Protecting Privacy Policy:

- State Library ILS- library record and patron information
- SEO ILS -library record and patron information
- Ohio Digital Library - library record and patron information
- OLS: MORE - library record information
- Talking Books ILS (Library for the Blind & Physically Handicapped) -library record and patron information
- Employee Personnel and Fiscal hard files

§3 Granting Access Rights to Personal Information
Access to confidential personal information and confidential personal information systems is granted to Agency employees and contractors by State Library management or department managers. Access is only granted on condition that it is required as part of the employee's and contractor's designated job responsibilities and duties.

Protecting Privacy Policy

State Library managers and department heads who can grant access to confidential personal information and confidential personal information systems:

- Agency Director - Beverly Cain
- Data Systems Manager - Eric Maynard
- Fiscal and Business Services - Jamie Pardee
- Employee Services – Stephanie Herriott
- Research and Catalog Services - Nicole Merriman
- Circulation and Special Services - Tracy Grimm
- Associate State Librarian, Library Services- Ann Watson
- Director SEO - Dianna Clark
- Information Technology Supervisor SEO- John Stewart

§4 Logging

Any Agency manager or supervisor identified in Section 3 of this policy, who accesses or directs another employee of the State Library to access Confidential Personal Information (CPI) from a personal information system shall maintain a log which will record that specific access whenever it is directed toward a specifically-named individual or a group of specifically named individuals' Confidential Personal Information (CPI).

The logs will contain the following information:

- Name of manager /supervisor accessing or directing access of CPI
- Name of Confidential Personal Information System
- Date and time of access
- Identification of person whose CPI was accessed

Access logs are to be maintained electronically in the personal drive of each manager/supervisor. At any time, the logs must be made available for inspection by the Agency Director or their appointed representative. A template for recording the logs is included as an attachment to this document and will be provided to each manager or department head as listed in Section 3 of this policy.

Access logs shall be retained by the Agency pursuant to General Retention Schedule No. IT- OP-07 for "System Users Access Records" until they are no longer of administrative value, and then destroyed.

Protecting Privacy Policy

§5 Notification of Improper Access
If Agency employees, managers or department heads discover that CPI has been accessed improperly, the Agency Director will be notified immediately.

The Agency Director will designate the appropriate Agency staff member(s) to collect the affected individual(s) contact information and notify the affected individuals about the incident as soon as is reasonably possible. The Agency will collect as much information about the improper access prior to contacting the affected individual(s) so as to determine the scope of the incident and to properly identify the specific risks to the individuals CPI.

§6 New Equipment Purchases and Upgrades
Any significant upgrades to existing Agency computer systems, or purchasing of a new computer system that stores, manages, or contains confidential personal information must include a mechanism for recording specific access by employees of the Agency to confidential personal information.

§7 Training & Awareness
The Agency will establish a "Protecting Privacy" training program for all employees of the Agency. The training will provide information about the applicable rules and policies governing Agency access to Confidential Personal Information.

The training will include:

- Review of this Protecting Privacy Policy and related Agency rules
- Acknowledgement from all employees of attendance to training
- Distribution of Policy and related documentation on Agency Intranet
- Employee awareness of policies via electronic distribution and poster placements

The access or disclosure of CPI may be in violation of state and federal laws and may result in prosecution, fines, claims, civil liability or other discipline up to and including termination, as specified in applicable laws, policies, and work rules.

§8 Additional Documentation
- ORC 1347: Personal Information Systems
- ORC 149.432 Releasing library record or patron information
- State of Ohio- Privacy and Security Information Center http:/ /privacy.ohio.gov

- Accessing Confidential Personal Information -A Guide to Section 1347.15 of the Ohio Revised Code http://privacy.ohio.gov/resources/GuidanceOnORC1347-15.pdf
- State Library Website Privacy Policy https://library.ohio.gov/about/policiesandstatements/#Statements

§9 Data Privacy Point of Contact

The State Library of Ohio has designated a Data Privacy Point of Contact to work with the State of Ohio's Chief Privacy Office within the Office of Information Technology. Questions about the specific applications and definitions of this Agency Protection Privacy policy can be directed to:

Eric Maynard
Data Systems Manager
Data Privacy Point of Contact
State Library of Ohio
emaynard@library.ohio.gov
phone: 614-644-6849

§10 Ohio Public Library Information Network (OPLIN)

OPLIN does not maintain any confidential personal information on any systems they maintain. Questions regarding the systems and information maintained by OPLIN can be sent to the OPLIN Executive Director:

Don Yarmin
Executive Director
Ohio Public Library Information Network
hedgesst@oplin.org
phone: 614-728-5250

Protecting Privacy Policy

State Library of Ohio

Confidential Personal Information (CPI) Manual Logging Form for Paper and Electronic Systems

Log Beginning Date (MMDDYYYY) _____ Log Ending Date (MMDDYYYY) _____

Name of Personal Information System	Date Accessed (MM-DD-YYYY)	Time Accessed (HH:MM)	Name of Person Accessing	Identification of the person whose CPI was accessed	Reason for Accessing Information