Published on *SWAN Library Services* (https://support.swanlibraries.net)

Library Use Policy

Approved by the SWAN Board 2/19/2021

The SWAN Library Services Platform (LSP), is a suite of SWAN-supported tools and databases which include, but are not limited to SWAN Support systems, Symphony WorkFlows, EBSCO, BLUEcloud Central (and associated tools), BLUEcloud Analytics, Enterprise, and Aspen Discovery. These tools allow library staff access to a large amount of patron data along with personally identifiable information (PII) which includes circulation activity and sensitive contact information. SWAN and its member libraries have an obligation to protect the privacy, security, and integrity of users' personally identifiable information (PII) as part of our professional ethics and to satisfy obligations under state and federal laws

This policy specifies member library's responsibilities for using any tools or databases in conjunction with the SWAN LSP. By using the SWAN LSP suite of tools, you agree your library will:

- ensure that individual library staff have access to training in their job functions and are familiar with this agreement before gaining access to any SWAN LSP logins. Procedures are followed for onboarding new staff.
- maintain staff in the L2 directory.
- protect the security of SWAN LSP accounts by using strong passwords whenever applicable that incorporate letters, numbers, and symbols.
- refrain from saving passwords in ways that they may be accessible by non-designated staff, vendors, or patrons.
- not share SWAN LSP accounts, passwords, or access with any non-designated staff, vendors, or patrons.
- not share access to or privileged information from the SWAN LSP with external vendors or 3rd parties without coordinating a SWAN Vendor Access Policy agreement with SWAN staff beforehand.
- avoid exporting or printing out unnecessary patron information and will safeguard any data that has been exported/printed. Exported data that includes patron PII must be password protected and/or encrypted if transferred by any means.
- only collect patron data using SWAN-designed or approved tools. Data collected by non-SWAN tools must be encrypted end-to-end and appropriately secured to prevent unauthorized

access.

- only use patron data for library purposes. Accessing this data for non-library use is prohibited.
- notify SWAN immediately when a staff member with SWAN LSP access is no longer employed at your library so that the account can be deactivated or removed, or shared logins updated.
- If your library suspects a breach of your SWAN LSP accounts, the accounts of others, or the SWAN LSP in general, you will notify SWAN immediately.
- not store sensitive information in patron records, including social security number, driver's license number, or credit card.

Failure to respect any aspect of this policy may result in the suspension of access to SWAN LSP services at your library.

Source URL (modified on 02/19/2021 - 11:47): https://support.swanlibraries.net/node/85218

Reminder and Related to SWAN Policy: State of Illinois Library Records Confidentiality Act

The Library Records Confidentiality Act [75 ILCS 70/1] provides that registration and circulation records of a library are to be confidential and cannot be published or made available to the public except by a court order, or the rare example of someone's personal health and safety requiring that a sworn law enforcement officer be given the information of an individual's name and address based on a sworn statement by the officer of such need. Statistical reports of circulation and registration may be published if the reports do not identify particular individuals. [75 ILCS 70/1 (b)].