Security of Personal Information

Revised 9 May 2023

In accordance with KRS 61.931-934 and applicable policies adopted by the Department for Local Government, the Library will take every reasonable precaution to ensure that any personal information that is kept by the Library for any purpose is safeguarded from unauthorized access.

The Library also acts to limit the amount of personally identifiable information that it retains. Some information, however, is necessarily and understandably retained for the transaction of day-to-day business.

Point of contact

The Library Director is tasked with ensuring that appropriate security measures are in place to prevent loss or compromise of the data that the Library stores. The Library Director will also create procedures for the appropriate recovery responses in the event that a loss or compromise of the Library's network or storage systems and ensure their implementation in any breach event. These procedures are regularly reviewed and updated by the Library's staff.

Patron information

Most information related to patrons is kept for the purposes of circulating materials and ensuring that responsibility is attributed to the correct person when an item is borrowed. This information is not publicly available and, beyond interactions between the Library and the patron, will be shared only with law enforcement personnel upon valid, legal request. Information related to delinquent patrons is shared with a third party vendor for the purposes of collection. The Library will not share personally identifiable patron information for any other purpose.

When a patron record has been inactive for three years, the record is deleted from the Library's computer system and is not archived.

Personal information about patrons is generally only retained in electronic format with appropriate back-up devices in place to recover in the event of a database

failure. All back-up devices are located on the Library's property and are kept secured at all times in areas that are not accessible to the general public and with limited accessibility by staff.

Staff information

The Library retains information about its staff that is directly related to the work environment. Social security numbers, health information, and performance records are retained only as a part of standard human resources processes (such as payroll, retirement, or health insurance).

Personal information about staff members is, in some cases, subject to the Open Records Act and will be shared with anyone requesting that information as permitted by Kentucky Revised Statutes. Information that is not permitted under the Open Records Act will not be shared with any outside agency for any purpose other than for the reason it was collected (i.e. to a payroll vendor for tax purposes).

Security measures

The Library will comply with best practices established by the Department for Local Government (as required in KRS 61.932) to secure all personal information under its care.

The Library does not share any information with any outside agency for any reason other than the purposes for which it was collected. Third party vendors with whom the Library does business are expected to provide their own security measures to protect any personal information. Where possible, the Library has informed each entity in writing that appropriate security is required.

The Library provides an internal, closed network for the collection and use of most patron data. The network is not accessible to the general public and access to it is limited to third party vendors with whom the Library has contracted services.

Personal information stored on computers or back-up devices is not accessible to the general public and is protected by a computer firewall and anti-virus systems.

Security breaches

If the Library becomes aware of a breach that would allow outside access to its network or access to devices used to store personal information, action will immediately be taken to remove the device from the network or to close the network to all external traffic.

Where the Library's systems do have interaction with any outside vendor or patron (i.e. through the internet-based catalog), transactions will take place using secure transmission protocols. Such interactions will be limited to the

purpose of the transaction only and will not allow access to any more information than is required for the purpose of the transaction (i.e. a patron reviewing a list of items that are currently checked out).

Notifications

The Library will notify vendors of their responsibilities to inform the Library of any breach in their own systems which would expose or compromise the security of personal information provided by the Library. Notification of such must conform to the requirements of KRS 61.932 and will include any reports of investigations that are conducted into the breach. Contracts that are made or amended with the Library must contain provisions to account for the requirements under KRS 61.932.

If the Library's own computer network or data storage systems are breached, the Library will immediately take action to secure the network or system, to prohibit any off-site access, and to determine the extent of the data that was obtained by the unauthorized party. Where appropriate, the Library will notify any/all affected parties within the guidelines of KRS 61.933 or as directed in guidance from the Department for Local Government. Investigations which follow such a breach will be reported as required by the same statute.