1. PURPOSE OF SECURITY CAMERAS

The Library has security cameras to enhance the safety and security of Library users, staff, and property. Security cameras are used to discourage illegal behavior and policy violations, to enhance the opportunity to apprehend offenders, and to provide recorded data relevant to the control of library security and operations. The security camera installation consists of dedicated cameras providing real-time surveillance through a central monitoring facility. There is no audio recording associated with the cameras.

2. SIGNAGE

The library posts signs at both public entrances alerting patrons to the use of security cameras for monitoring and recording on library property, both inside and outside.

3. STAFF ACCESS TO DIGITAL IMAGES

a. Controlled access

The recorded data and recorders are considered confidential and secure.

b. Authorized staff

Specifically designated staff have access via the library's network to live surveillance or recorded data in order to monitor activity at the library when necessary. Only the following administrative staff are permitted to access or to authorize access-to the recorders and recorded archival data: Executive Director, Associate Director, Department Directors, and Managers.

Such authorized administrative staff may direct IT staff to access and isolate live or recorded data related to a specific incident or may ask other staff to view live or recorded data in order to ascertain security concerns. Authorized staff shall notify the Executive Director whenever video data is accessed.

c. Operational checks

Occasional spot checks of the recorded data are made by the Executive Director, Associate Director, or Information Technology Manager to assure proper operation of the system and to review server room access. The frequency of viewing and the amount of video viewed at one time will be limited to the minimum needed to give assurance that the system is working and to verify compliance with server room access.

4. RETENTION OF DIGITAL IMAGES

Recordings shall be kept for approximately 30 days, unless required as part of an ongoing investigation. The storage media shall be kept in a secure area.

5. ACCEPTABLE USE AND PATRON PRIVACY

a. Activity on library property

Authorized staff may use live surveillance, a still shot, or selected portions of recorded data to assess the security risk of a specific individual, to investigate a crime on library

property, to request law enforcement assistance, to validate serious or repeated policy violations, to alert staff to banned or repeatedly disruptive individuals, or to address internal security / operational concerns. In the discharge of such duties, authorized staff are permitted to connect the recorded digital image with identification data available on the library's patron databases.

b. Requests from general public

Staff specifically may not access surveillance or recorded data in response to requests from the press or general public, including victims of crime and individuals concerned with the personal safety of family, friends, or co-workers. Such individuals are directed to contact law enforcement.

c. Requests from law enforcement

Authorized staff may use live surveillance or recorded data to cooperate with law enforcement investigations of criminal activity, missing persons, or runaways. Video data is made available to law enforcement without a court order as long as the request is limited to the person's visible presence in the library or surrounding library property.

Any such video data provided to law enforcement will be with the knowledge and authorization of the Executive Director, Associate Director, a Department Director, or a Manager.

Any law enforcement request for access to library records of a person's registration, borrowing, or computer use at the library is granted only upon presentation of a valid court order issued by a judge and establishing probable cause to review the data, as specified in the library's policy on "Confidentiality of Records" (III-B-23).

However, in emergency situations that present imminent danger of physical harm, law enforcement may request access to information from library registration, circulation, or computer use records without a court order. In such imminent danger emergencies where law enforcement calls for a waiver of the court order, the requesting officer is required to provide in writing his/her name, agency, badge number, the nature of the emergency, and the extent of data requested.

d. Privacy

In all other respects, recorded data will be accorded the same level of confidentiality and protection provided to library users by Illinois State law, The Urbana Free Library policies, and the American Library Association policies on confidentiality and privacy.

Adopted July 10, 2007

Amended March 19, 2013; January 10, 2017