



Security Cameras Policy

Security cameras are installed at the Nevins Library to protect the safety and security of people, the building, and its contents, while protecting individuals' right to privacy. Only authorized Library staff may view recordings.

Placement of Cameras

Video recording cameras will be used in public spaces of the Library to discourage criminal activity and violations of the Behavior Guidelines of the Library. The recording of audio is restricted under the Electronic Communications Privacy Act and will not be used.

Cameras may be installed in outdoor and indoor places where individuals lack a reasonable expectation of privacy. Examples include public common areas of the library such as parking lots, entrances, seating areas, and areas prone to theft or misconduct. Cameras will not be installed in areas of the Library where individuals have a reasonable expectation of privacy such as restrooms or private offices. Cameras will not be positioned in areas where patrons' viewing, listening, or personal account information may be easily monitored.

Signs are posted at the Main Entrance of the library informing the public and staff that security cameras are in use.

Because security cameras are not constantly monitored, staff and public should take appropriate precautions for their safety and for the security of personal property. The Nevins Library is not responsible for loss of property or personal injury.

Storage and Access to Recorded Data

Recorded data is confidential and secured in a controlled area. Video recordings will typically be stored for no longer than 3 weeks. As new images are recorded, the oldest images will be automatically deleted.

Video surveillance records are not to be used directly or indirectly to identify the activities of individual Library patrons except as viewed in relation to a specific event or suspected criminal activity, suspected violation of Library policy, or incidents where there is reasonable basis to believe a claim may be made against the Library for liability. Authorized Library staff may use a still shot or selected portions of recorded data to request law enforcement review for assessing the security risk of a specific individual or for investigating a crime on library property.

Video data will be made available to law enforcement officials or agencies upon written request submitted to the Library Administration, and with approval of authorized Library staff. The Library shall retain a copy of the request. Recorded data will be accorded the same level of confidentiality and protection provided to library users by Massachusetts law and the Library's policies related to privacy. Access is also allowed by law enforcement when pursuant to a subpoena, court order, or when otherwise required by law.

Patrons who experience a crime such as theft of personal possessions while at the Library must submit a report to law enforcement. Members of the public will not be granted access to recorded data; this access must be requested, in writing, by law enforcement, as stated above.

In situations involving patrons who are under criminal trespass order, stored still images may be shared with staff Library-wide. Shared images may remain posted in restricted staff areas for the duration of the banning period. The general public will not have access to this information. Staff are not authorized to share these images.

Unauthorized Access and/or Disclosure

A breach of this policy may result in disciplinary action up to and including dismissal. Any library employee who becomes aware of any unauthorized disclosure of a video recording and/or a potential privacy breach has a responsibility to immediately inform the Director of the breach.

Disclaimer of Responsibility

Questions from the public may be directed to the Library Director.

The Library disclaims any liability for use of the video data in accordance with the terms of this policy, given that the library is a public facility and the security cameras shall be limited to those areas where patrons and/or staff have no reasonable expectation of privacy.