VIDEO SURVEILLANCE POLICY & PROCEDURES

Originally issued:	9/23/2019
Approved:	9/24/2026
Scheduled review date:	9/20/2027
Primary contact:	President of the Board, CEO

Policy

The Boys & Girls Clubs of Chaves and Lincoln Counties makes limited use of video surveillance systems in its Club locations. Video surveillance systems may be used to record access at building entrances and in program areas within the interior of the facilities. Video surveillance cameras may also be used to provide surveillance of the exterior of the building and surrounding streets.

Video surveillance cameras are never used in areas where employees or members would have an expectation of privacy, such as restrooms or locker rooms.

CAMERA LOCATIONS, PROHIBITED AREAS, AND NOTICE

Surveillance cameras may be installed in entrances, exits, hallways, classrooms, program areas, gyms, common areas, parking areas, building exteriors, vehicles, and other locations where monitoring supports safety, security, supervision, or incident review.

Cameras shall not be installed in restrooms, changing areas, shower areas, or any location where children, employees, volunteers, or visitors have a reasonable expectation of personal privacy. Cameras must not be positioned in a manner that intentionally captures activity inside a restroom or designated changing area.

When a shared area is temporarily used for changing clothes, camera coverage must be blocked, disabled, repositioned, or otherwise prevented from recording the changing activity. Staff shall continue to follow all supervision and restroom procedures during these periods.

Audio recording shall not be used unless it has been specifically approved by the Chief Executive Officer or designee and determined to comply with applicable law.
BGCCLC shall provide reasonable notice that video surveillance is in use through posted signs, handbook language, enrollment materials, employee policies, or another appropriate method. The location of every camera does not have to be individually identified when general notice has been provided.

Procedure

All video surveillance cameras may be capable of being recorded continuously by a digital video recording system.

SYSTEM MANAGEMENT AND AUTHORIZED ACCESS

Access to live video and recorded footage is limited to the Chief Executive Officer or designee and specifically authorized employees whose duties require access. Access shall be limited to the minimum footage necessary for the authorized purpose.

If a licensed facility has cameras with recording capability, BGCCLC will provide the ECECD licensing authority access to requested footage as required by 8.9.4.17(G) NMAC. A subpoena or court order is not required for a licensing request. The CEO or designee will coordinate and document the access without

obstructing or unnecessarily delaying the licensing review.

Video footage may be provided to law enforcement, emergency responders, state licensing personnel, child protective services, or another legally authorized agency when necessary to respond to an active emergency or immediate safety threat; locate or protect a missing or endangered child; investigate suspected abuse, neglect, criminal conduct, or a serious incident; preserve evidence; or comply with a subpoena, court order, or other legal requirement.

Access during an emergency does not have to wait for a subpoena or court order when immediate review or disclosure is reasonably necessary to protect a child or another person.

INDEPENDENT AND UNAFFECTED REVIEW

Any person who has a personal, familial, employment, or other direct connection to a child, parent, employee, volunteer, or other individual involved in the incident shall not view, retrieve, review, copy, release, or participate in decisions regarding the applicable footage.

This restriction applies even when the person would normally have authority to access footage because of their employment, leadership position, law-enforcement role, licensing role, or other official position. The footage must be reviewed by an authorized individual or agency representative who is not personally or professionally affected by the incident or its outcome.

If an authority requesting footage has a personal or familial connection to anyone involved, the request must be transferred to another unaffected representative of that agency. BGCCLC will document the request, the reason access was granted, the person who reviewed or received the footage, and confirmation that the reviewer had no identified conflict of interest.

A parent, guardian, family member, employee, or other personally affected person may not use an official position or professional authority to personally view footage involving their child, relative, household member, or another person with whom they have a personal connection. When a requesting law-enforcement, licensing, child-protective-services, or other authorized representative has such a conflict, BGCCLC will immediately request review by an unaffected representative or supervisor from the same agency. This safeguard will be implemented without concealing evidence, obstructing an investigation, or refusing access that the agency is legally entitled to receive.

FAMILY ACCESS

Parents, guardians, family members, and other members of the public will not be permitted to directly view surveillance footage. This restriction applies even when the individual's own child or family member appears in the recording.

BGCCLC may review relevant footage internally and provide the family with appropriate information about the incident. Footage may be preserved or released to an unaffected law-enforcement officer, licensing representative, child protective services representative, court, or other legally authorized party when appropriate or legally required.

No family member may obtain access by using an employment position, official title, law-enforcement authority, licensing authority, or other professional relationship when the footage involves or may affect their child, relative, household member, or another person with whom they have a personal connection.

LIVE MONITORING, SYSTEM ADMINISTRATION, CREDENTIALS, AND ACCESS LOGS

The Chief Executive Officer or designee shall determine who is authorized to administer the surveillance system, view live camera feeds, review recordings, export footage, or provide footage to an authorized third party. Access shall be based on job responsibilities and limited to the minimum level necessary.

Live camera feeds may be viewed only for legitimate safety, supervision, security, operational, emergency-response, or incident-review purposes. Cameras shall not be used to inappropriately monitor, target, embarrass, harass, or retaliate against a child, employee, volunteer, family member, or visitor.

Each authorized user shall use an individually assigned account whenever the system supports individual accounts. Usernames, passwords, access codes, and authentication devices shall not be shared. Multi-factor authentication shall be used when available. Access from a personal or mobile device is permitted only when specifically authorized and when the device is reasonably protected against unauthorized access.

Access shall be promptly removed or changed when an employee's duties no longer require it, employment or service ends, credentials may have been compromised, or the Chief Executive Officer or designee withdraws authorization.

BGCCLC shall maintain an electronic system log or written access log identifying, when reasonably available: the person accessing the system or footage; the date and time of access; the camera, location, and approximate recording period reviewed; the reason for access; whether footage was viewed, preserved, copied, or released; the recipient of any released footage; and the person authorizing the access or release.

Emergency access by law enforcement, emergency responders, licensing authorities, child protective services, or another legally authorized agency shall be limited to the footage reasonably necessary for the emergency or official purpose. The accessing representative must be unaffected by and have no personal or familial connection to the incident, as required by this policy.

When immediate emergency access prevents advance documentation, the access and reason shall be documented as soon as reasonably possible afterward.

A technology provider, security contractor, or system vendor may access the surveillance system only when necessary to install, maintain, repair, secure, or troubleshoot the system. Vendor access must be authorized, limited in scope and duration, and documented. Vendors may not use, retain, or disclose footage for their own purposes.

REQUESTS, INVESTIGATIONS, CONFIDENTIALITY, AND VIOLATIONS

All requests to view, obtain, preserve, or release surveillance footage must be directed to the Chief Executive Officer or designee. Employees, volunteers, board members, contractors, parents, guardians, visitors, and other individuals shall not independently provide access to or release footage.

BGCCLC may review and use footage for safety, security, supervision, training, policy enforcement, internal investigations, licensing compliance, insurance matters, legal proceedings, or other legitimate organizational purposes. Footage shall not be used for entertainment, personal purposes, or unauthorized public disclosure.

Parents and guardians may report an incident and request that relevant footage be preserved. Submitting a preservation request does not give the requesting person the right to view or receive the footage. BGCCLC may provide an appropriate summary of its findings when doing so does not violate another person's privacy, interfere with an investigation, or conflict with legal or licensing requirements.

Footage involving children, families, employees, volunteers, or visitors is confidential. BGCCLC will limit disclosure to information reasonably necessary for the authorized purpose and will take reasonable steps to protect the identities and privacy of individuals who are not relevant to the matter.

BGCCLC shall cooperate with law enforcement, child protective services, state licensing authorities, emergency responders, courts, insurers, legal counsel, and other legally authorized parties when access or

disclosure is appropriate or required. Access must comply with the independent and unaffected-review requirements of this policy.

When practical, an authorized BGCCLC representative shall remain present while an outside authority reviews footage. If a copy is released, the release must be documented in the electronic Surveillance Footage Access and Release Log.

No person may alter, conceal, selectively edit, destroy, disable, obstruct, or tamper with a camera, recording, access log, or surveillance-system component. No person may direct another individual to improperly access, alter, conceal, copy, release, or destroy footage.

Suspected unauthorized access, disclosure, copying, alteration, destruction, system tampering, credential sharing, or other violation must be reported immediately to the Chief Executive Officer or designee. Violations may result in disciplinary action, termination, removal from service, loss of access privileges, reporting to licensing authorities, or referral to law enforcement or another appropriate authority.

BGCCLC prohibits retaliation against a person who, in good faith, reports a surveillance concern, requests preservation of relevant footage, participates in an investigation, or reports a suspected violation of this policy.

If someone from the media or other organization approaches you and asks you for a comment you should direct them to the CEO per the Communications Policy.

ROUTINE RECORDING RETENTION

Video surveillance recordings will ordinarily be retained for at least 30 calendar days from the date of recording. After the retention period expires, recordings may be automatically overwritten or securely deleted unless they have been identified for preservation because of an incident, complaint, investigation, insurance matter, legal request, licensing review, or other authorized purpose.

The availability of footage is not guaranteed when equipment fails, a camera is obstructed, storage capacity is exceeded, or another technical problem occurs. Any known equipment or recording failure shall be reported to the Chief Executive Officer or designee.

PRESERVATION OF INCIDENT-RELATED FOOTAGE

When BGCCLC becomes aware that surveillance footage may relate to an accident, injury, missing child, suspected abuse or neglect, behavioral incident, complaint, licensing matter, insurance claim, law-enforcement investigation, anticipated legal action, or other significant event, the relevant footage shall be identified and preserved as soon as reasonably possible.

Preservation should include a reasonable period before and after the event so that the circumstances surrounding the incident are documented. When the precise time is uncertain, BGCCLC shall preserve a broader period reasonably likely to include the event.
Incident-related footage shall be preserved for at least three years or until the matter is fully resolved, whichever is later.

The Chief Executive Officer or designee shall document the reason the footage was preserved, the dates and approximate times included, where it is stored, everyone granted access, and the date and authorization for its eventual deletion.

SECURE DELETION AND AUTHORIZED COPIES

Video recordings that have reached the end of the applicable retention period and are not subject to a preservation requirement may be automatically overwritten or securely deleted.

Surveillance footage shall not be downloaded, photographed, screen-recorded, copied, emailed, texted, posted to social media, stored on a personal device, or transferred to unauthorized storage.

Authorized copies may be created only when necessary for an incident review, licensing matter, insurance claim, law-enforcement investigation, legal proceeding, or another purpose approved by the Chief Executive Officer or designee. Each authorized copy shall be protected against unauthorized access and maintained according to the same confidentiality and retention requirements as the original recording.

Any person who receives an authorized copy shall be documented. The record shall identify the footage provided, the recipient, the purpose, the date of release, and the person who authorized the release.

When an authorized copy is no longer required, it shall be securely deleted or destroyed in a manner that prevents recovery. No employee, volunteer, board member, contractor, parent, guardian, or other person may retain a personal copy of surveillance footage.

Any unauthorized access, copying, disclosure, alteration, deletion, or distribution of surveillance footage must be reported immediately to the Chief Executive Officer or designee and may result in disciplinary action, termination, removal from service, loss of access, or referral to the appropriate authorities.

Limitations of Video Surveillance Systems

A security officer is not watching cameras most of the time and there should not be an expectation that they are under continuous surveillance when they are in the range of a camera. For example, employees walking to their car at night who may feel concerned should request an escort rather than assume that they are already being watched by a security officer using a camera.

The video surveillance system has cameras that cover only a small fraction of the total Club area, and even when camera coverage exists, it may not provide the level of detail necessary to spot suspicious activity or identify criminals.

ACTIVE SUPERVISION AND SYSTEM LIMITATIONS

Surveillance cameras are an additional safety and security measure. They do not replace active supervision, required staff-to-child ratios, head counts, direct visual supervision, required facility checks, or any other employee responsibility. Employees may not rely on a camera or video monitor as their primary method of supervising children.

The absence of a camera, incomplete camera coverage, equipment failure, an obstructed view, poor image quality, or the unavailability of a recording does not reduce an employee's responsibility to follow all supervision and safety requirements.