McCLOUD COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: VIDEO/PHOTO RECORDING
POLICY NUMBER: 1160
ADOPTED: May 25, 2015
REVIEWED: May 12, 2015; October 8, 2019; March 11, 2020; 8/10/23
REVISED: June 8, 2015; November 12, 2019; March 23, 2020

1160.10 Purpose: The additional protection provided by visual surveillance devices is helpful and safe to use, while affording additional protection of District property. Proper visual surveillance, where deemed necessary, can be a very effective means of helping to keep District facilities and properties operating in a safe, secure and effective manner. This policy provides direction concerning the context, procedures and protocols, within which the District installs and operates surveillance cameras.

1160.20 Notice of Use of Video/Photo Surveillance: In compliance with state law, the District shall post signs, visible to employees and members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds that video surveillance may be in use.

1160.21 The District may choose to monitor public and work areas with security cameras or other recording devices, in doing so, the District will comply with all state and federal laws. The public and employees should not expect privacy from visual recording by others in public areas; employees should not expect video privacy in work-related areas except restrooms and locker rooms.

1160.22 Given the open and public nature of the District facilities and service, filming and/ or recording may be done at any time in a 24-hour period because individuals may be present at all hours of the day and night.

1160.23 The ability of authorized and unauthorized personnel to adjust cameras or other devices shall be restricted so they cannot adjust or manipulate cameras/devises to overlook spaces that are not intended to be covered by the video/photo surveillance program.

1160.24 Recording equipment must be located in a strictly controlled access area. Only authorized personnel shall have access to the controlled access area and the recording equipment. The General Manager or his/her designee shall determine authorized personnel.

1160.30 Unauthorized Access and/or Disclosure (Privacy Breach):

1160.31 Any District employee who becomes aware of any unauthorized disclosure of a video recording or photo violation of this policy, and/or a potential privacy breach has a responsibility to ensure that the General Manager and their staff is immediately informed of the breach.

1160.32 District staff shall work to mitigate the extent of the privacy breach, and to review the adequacy of privacy protection with the existing Policy. The staff shall inform the General Manager of events that led up to the privacy breach.

1160.33 The General Manager in consultation with the staff, in which the breach of policy occurred, shall investigate the cause of the disclosure with the goal of eliminating future occurrences.

1160.34 A breach of this Policy may result in disciplinary action up to and including dismissal. A breach of this Policy by service provider (contractors) to the District may result in termination of their contract.

1160.40 Visual Equipment/Records:

1160.41 District Facilities using video/photo recorders will retain these records for a minimum of one (1) year A record of an incident will only be stored longer than one (1) year where it may be required as part of a criminal, safety, or security investigation, evidentiary purposes, or management purposes.

1160.42 Access to the video/photo surveillance equipment and records shall be restricted to District personal authorized by the General Manager and only in order to comply with their roles and responsibilities as outlined in the Video/Photo Surveillance Policy and/or individual job descriptions.

1160.43 The General Manager may approve access to a video/photo from surveillance record if required for the purpose of law enforcement or by court order. The General Manager shall consult legal counsel before releasing any information.

1160.44 Formal requests for video/photo surveillance records from the public shall be made to the General Manager, who shall make a determination on releasing any information or recordings.

1160.45 All recordings or other storage devices that are not in use must be stored in a locked receptacle located in District office.

1160.50 Custody, Control, Retention, and Disposal of Recordings:

1160.51 The District retains custody and control of all original visual records not provided to law enforcement. With the exception of records retained for criminal, safety, or security investigation or evidentiary purposes, the District will not maintain a copy of recordings for longer one (1) year. The District will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal. Old recordings and storage devices must be disposed of in accordance with the District records retention policy and/or an applicable technology asset disposal process. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.