Policy Title:	**INTERNAL DRONE DATA USE AND RETENTION POLICY**
Date Created/Revised:	**October 24, 2024**
Created By:	**Marcus Beltramo, Code Enforcement Manager**
Approved By:	**Shannon Walker-Smith, Deputy Community Development Administrator**

Purpose and Scope:

County of Lake seeks to ensure that it retains and utilizes only data necessary to effectively conduct its Drone Policy.

Data retention periods vary depending on the type of data and the purpose for which it is collected. Procedures for retention of drone data shall be consistent with other retention procedures for the County.

This internal policy covers all data collected by the Community Development Department (CDD) through its drone operations including storage, retrieval, and dissemination of images and data captured by the drone during CDD drone operations.

Privacy Concerns:

The Fourth Amendment protects individuals from unreasonable searches and seizures, which generally means a search or seizure without consent, an emergency, or a warrant. An inspection by the County, its personnel or agents acting on behalf of, or at the direction of, the County, constitutes a search. Specifically, a search occurs when there is a reasonable expectation of privacy; a reasonable expectation of privacy is an objective belief that a particular place or area is not open to the public to view without consent from the owner, or person in possession or control of the place or area, if not the owner. Generally, there is a reasonable expectation of privacy when a violation exists on a privately owned property.

As such, all County personnel engaging in drone operations must protect private individuals' constitutional rights and reasonable expectations of privacy when conducting surveillance or collecting evidence for code enforcement use, including but not limited to, inspections and abatements. Operating personnel will be held accountable for ensuring that drone operations intrude to the minimal extent.

As privacy concerns relate to the collection of data in drone operations, all personnel shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions include deactivating or turning imaging devices away from such areas or persons during drone operations.

Classification of Drone Data:

It shall be the responsibility of the CDD Director (Drone Coordinator) to ensure that all media recorded by the drone is properly classified for retention when merged into the storage system.

The Drone Coordinator shall classify all drone footage into one of the following categories:

A. **Investigatory.** Drone footage that is part of an investigatory file.
B. **Footage Without a Corresponding Investigatory File.** When a drone is used to investigate whether a violation of law was occurring or had occurred but did not create a corresponding investigatory file.
C. **Factual Inquiry.** When a drone is used to make a factual inquiry to determine what kind of assistance is required, but not to investigate a suspected violation of law.
D. **Test.** Drone footage that is created as part of testing the working condition of the drone or recorded during training.

When categorizing drone footage, the Drone Coordinator may either review the entire video footage or may determine the category by reviewing call logs, flight requests, or any other related information to ascertain which category the drone footage belongs to.

Use of Drone Data – Storage, Retention and Integrity:

Any images and video (media) from the drone system shall not be copied, exported, or recorded in any way for any purpose other than for circumstances authorized in this policy. Unauthorized use, duplication, and/or distribution of drone files is prohibited.

Personnel shall not make copies of any drone file for their personal use and are prohibited from using a recording device such as a cellphone camera or secondary video camera to record drone files.

To prevent damage to or altering of the original recorded media, it shall not be copied, viewed or otherwise inserted into any device not approved by the Drone Coordinator. When reasonably possible, a copy of the original media shall be used for viewing (unless otherwise directed by the courts) to preserve the original media.

Drone systems should be assembled and equipped based on the manufacturer’s recommendations.

Drone operators and personnel shall not alter, reuse, modify or tamper with drone recordings. In the event a redaction is necessary by an authorized personnel to protect private information including but not limited to addresses, license plates, images of minors or other protected information, a copy of the unredacted recording must be retained equal to the time the redacted recording is retained.

Drone operators and County personnel shall not erase or otherwise destroy drone recordings unless approved by the Board of Supervisors in accordance with County Policy and California Government Code Sections 26202 and 26205. Notwithstanding the foregoing, all recordings shall be retained for a minimum of two (2) years as required under 14 CFR 107.165.

Recordings which become part of a citizen complaint or administrative/internal investigation will follow the retention time identified for the complaint/investigation pursuant to existing County data retention policies and applicable law.

Inadvertent and accidental recordings may be deleted as soon as practicable upon the approval from the Drone Coordinator.

Once submitted for storage, all recording media must be labeled and stored in a designated secure area in accordance with existing County procedures.

The CDD Director may increase the retention time for recordings when it is believed that retaining said recordings for a longer period of time would be in the best interest of CDD or the County.

Release of Data:

The CDD will make access to data captured by its drone and drone operators according to the following provisions:

All recording media and recorded images are the property of the County.

Dissemination outside of the County is strictly prohibited, except to the extent required by law.

If the CDD receives a request to release drone data via a subpoena, a Court Order, a civil discovery request, a criminal discovery request, or a California Public Records Act request, staff must consult with the County Counsel's Office regarding the legal issues surrounding the request. Although, generally, drone data related to an active investigation are considered part of the investigative record and are not available to the public under the California Public Records Act or Freedom of Information Act.

To the extent that release of drone data is legally required, all media shall be reviewed by the technical support personnel in the Information Technology Department (IT) prior to release.

Anything of a personal or confidential nature included in the media should be evaluated by the appropriate personnel, and redacted if deemed appropriate and

if permitted by law. All redactions shall be logged by CDD. An original copy of the media shall be retained by the CDD.