

	ANCHORAGE POLICE DEPARTMENT POLICY AND PROCEDURE	Distribution ALL PERSONNEL	Policy Number 7.07
		Previous Issue Date MM/DD/YY	Reissue/Effective Date MM/DD/YY
Order Title: Real Time Crime Center (RTCC)		Accreditation Standard:	Section 7
		Rescinds:	
Section Title: Special Operations		Sean Case, Chief of Police	

This Policy is for departmental use only and does not apply in any criminal or civil proceeding. This Policy should not be construed as creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims. Violations of this Policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.

I. PURPOSE

To establish guidelines for the operation of the Real Time Crime Center (RTCC), which supports Anchorage Police Department (APD) personnel by providing real-time data, video access, and analytical intelligence to enhance public safety, officer efficiency, and crime prevention.

II. POLICY

The RTCC exists to deliver timely, actionable intelligence to law enforcement personnel, enabling rapid response to incidents, proactive crime deterrence, and improved situational awareness across Anchorage. The RTCC supports patrol and investigative units by utilizing available technology and information systems to provide timely information to officers working in the field, during initial response to calls for service, continued investigations, and significant events. The information may be used to inform shift commanders and other personnel of criminal activity in real-time, allowing for greater effectiveness and efficiency in the department's response to crime. The information may also be valuable in department training initiatives and strategic planning of future operations.

APD is committed to the protection of individual rights as governed by the United States Constitution, the Alaska State Constitution, both Federal and State law, and Municipal Code. The collection of public and private video streams is strictly intended for legitimate law enforcement purposes and never for the arbitrary collection of video surveillance. Access to public and private video streams will be limited to those assigned to the real-time crime center and case officers if it is determined that the video is evidence. Video evidence, along with data and information from authorized technologies embedded within the camera system will be used to conduct criminal investigations against a person, enhance responses to critical incidents and public threats, safeguard the lives of community members by using this technology to locate at-risk missing persons, and protect assets and resources of the Municipality of Anchorage. This policy applies to all sworn and professional staff assigned to or interacting with the RTCC.

III. DEFINITIONS

Automated License Plate Reader (ALPR): Specialized camera system that automatically captures and processes images of vehicle license plates using optical character recognition (OCR). These systems can identify plate numbers in real time or from recorded footage, and cross-reference them against databases to assist with law enforcement, traffic management, and security operations.

Digital Multimedia Evidence (DME): Digital recording of images, sounds, and associated data.

Drone as First Responder Program (DFR): A public safety initiative in which unmanned aerial vehicles (UASs) are autonomously or remotely deployed in response to emergency calls or incidents, often arriving at the scene before ground personnel. These programs are designed to enhance situational awareness, reduce response times, and improve officer and community safety.

FAA: An agency of the United States Department of Transportation responsible for regulating and overseeing all aspects of civil aviation. Established in 1958 and incorporated into the DOT in 1967, the FAA ensures the safety, efficiency, and environmental sustainability of air travel through the development and enforcement of aviation standards, certification of pilots and aircraft, management of U.S. airspace, and regulation of commercial space transportation.

Optical Character Recognition (OCR): Technology that converts images of printed, typed, or handwritten text into machine-readable digital text. It uses pattern recognition and artificial intelligence to identify characters in scanned documents, photographs, or video frames, enabling the text to be edited, searched, and stored electronically.

Predictive Analytics: A branch of advanced data analysis that uses historical data, statistical algorithms, and machine learning techniques to forecast future outcomes. By identifying patterns and trends in existing datasets, predictive analytics estimates the likelihood of future events, enabling organizations to make proactive, data-driven decisions.

Real Time Crime Center (RTCC): A centralized law enforcement element that integrates live camera feeds, public safety data, and analytical technologies to provide immediate operational intelligence. It functions to support rapid response to crimes in progress, enhance situational awareness, and facilitate public safety.

Unmanned Aircraft System (UAS): A system that includes the necessary equipment, network, and personnel to control an unmanned aircraft.

IV. PROCEDURE

A. Overview

1. Real-Time Crime Center (RTCC) involves a centralized unit within APD that uses technology to collect, analyze, and distribute data to aid police operations.
2. RTCC allows the following video feeds to be viewed by RTCC personnel:

- a. Residents or Businesses can voluntarily join a registry allowing officers to know where cameras are located. Officers can request video from the known location through an Axon interface or,
- b. Residents or Businesses can provide APD with access to their cameras. All access and retention are controlled by the owner of the cameras. APD only controls the retention if a video is collected and stored as evidence.

B. Operational Objectives

1. Monitor and analyze live feeds from public and private cameras, license plate readers, and drones when available.
2. Analyze incoming data to identify victims, suspects, crime scenes, and public safety threats.
3. Support Officers in the field with real-time information during active incidents or investigations.
4. Coordinate with additional emergency services during large-scale events or disasters.

C. Authorized Use

1. All technology use must comply with APD policies, state law, and federal regulations regarding privacy, data retention, and civil liberties. The RTCC may utilize:
 - a. City-owned cameras
 - b. Privately owned cameras (when authorized in writing)
 - c. Traffic camera systems
 - d. Automated License plate readers (ALPR)
 - e. Body-worn camera feeds (when authorized and available)
 - f. Public safety databases and dispatch systems
 - g. UAS systems and associated DME

D. Prohibited Use

1. Predictive analytics are not to be used in the RTCC. All activities must be observed and verified before police action can take place.
2. RTCC will not conduct operations solely on individual characteristic (e.g. race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of law.

E. Staffing and Training

1. The RTCC shall be staffed with sworn or professional staff.
2. The RTCC will be a part of the crime suppression division and report to a RTCC Commander.

3. Cross-training with field units and dispatch is encouraged to ensure seamless communication.
4. Officers shall successfully complete the APD academy and FTO process before being eligible for RTCC duties.
5. Professional staff are required to complete a training cycle not to exceed six weeks comprised of basic dispatch functions, criminal data base research and familiarization, and camera use.
6. DFR pilots shall complete FAA part 107 (remote pilot certificate) prior to engaging in any drone operations.

F. DME Collection and Retention

1. DME collected shall be used strictly for law enforcement and public safety purposes.
2. APD does not retain as public record any data from camera feeds unless there is a law enforcement purpose associated with a criminal investigation or public safety threat.
3. APD Owned Cameras: All camera feeds are stored for 14 days and then are deleted unless the videos are captured and stored as evidence in a case.
4. DME shall be handled in accordance with all applicable laws and existing Department policy on data and record retention. (APD's policies: Digital Evidence Collection 3.10.025 and CJIS Disposal of Media 2.02.015).

G. DME Protection

1. All data retained will be stored in a secure government digital evidence management system that include:
 - a. FedRAMP Certification
 - b. Encrypted Storage
 - c. Robust Audit Trails
 - d. Third-Party Validation
 - e. Agency Controlled Access.
2. All DME downloaded from a video management solution to a mobile workstation or to digital evidence storage like Axon evidence shall be accessible only through a login/password protected system capable of documenting all access of information by name, date and time.
3. All data will be closely safeguarded and protected by both procedural and technological means.

H. DME Access & Sharing

1. Citizens requests for digital evidence must be submitted in writing through APD's Public Records Request Portal located on APD website.

2. Each request will be reviewed by Records Division for release eligibility and redaction requirements. Digital evidence will not be released if:
 - a. It relates to an ongoing criminal investigation or prosecution
 - b. It violates a court order.
 - c. It contrains protected information.
3. Access is restricted to authorized personnel with a legitimate law enforcement purpose.
4. To the extent required by law, videos obtained from APD camera systems shall be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, which includes enhancing criminal investigation and prosecution as allowed by law. These request shall be approved by the Chief of Police.

I. Access to the RTCC

1. Only employees assigned to the RTCC will have access to the RTCC and the systems used in the RTCC. All information accessed in the RTCC shall be logged for audit purposes.
2. Personnel authorized to use APD camera equipment or access videos collected using such equipment shall be specifically trained in such technology and authorized by the Chief of Police or his designee.
3. External agency access requires written authorization from the Chief of Police and must comply with APD standards.

J. Privacy

1. RTCC shall not engage in observations of constitutionally protected activities (e.g., protests) unless there is a specific and credible threat to public safety or observation is requested by event organizers.
2. RTCC shall conduct all operations in accordance with federal, state, and local laws.
3. No information obtained by the RTCC shall be used for law enforcement purposes unless (a) it is collected from areas where there is no reasonable expectation of privacy, (b) a court approved search warrant is obtained, or (c) use of the information is necessary and legally appropriate because of an immediate threat to life or safety..

K. Quarterly Review

On a quarterly basis, the Chief of Police shall assess RTCC operations and determine if the benefits the RTCC provides to law enforcement and public safety outweigh the potential legal liability and risks to citizen privacy.

L. Audit Report

APD shall publish an annual report summarizing RTCC activities to include the following:

1. Number of feeds monitored
2. External agency sharing

3. Warrants obtained
4. Misdemeanor and Felony arrests
5. Number of First Amendment events where video recordings were obtained

DRAFT