

Asheville Police Department Policy Manual

Chapter: 17 - Intelligence & Analysis

Original Issue:

Policy: 1703 - Real Time Intelligence Center

Last Revision: N/A

Previously: N/A



Contents

Introduction
Policy Statement
Definitions
Rules and Procedures
1703.1 Duties and Responsibilities
1703.2 Operations
1703.3 Cameras and Video Feeds

Associated Directives

[Policy 505 - Automated License Plate Recognition](#)

[Policy 1701 - Criminal Intelligence](#)

[SOP 3009 - Criminal Intelligence Records](#)

Introduction

The purpose of this policy is to establish operational standards, deployment criteria, and governance principles for the department's Real-Time Intelligence Center (RTIC). This directive provides department members with clear guidelines to ensure the utilization of real-time situational awareness and investigative technologies balances public safety needs with strict accountability, data security, and the preservation of constitutional rights.

Policy Statement

It is the policy of the Asheville Police Department (APD) to use the Real-Time Intelligence Center to enhance public safety by collecting, analyzing, and disseminating data related to active criminal activity in accordance with the law.

Definitions

Real-Time Intelligence Center (RTIC): a centralized technology hub within the APD tasked with the legal collection, analysis, and immediate dissemination of data to enhance situational awareness during active criminal threats and critical incidents.

Rules and Procedures

1703.1 Duties and Responsibilities

- A. The Technology Manager will provide overall leadership and supervision of the RTIC.
- B. The Intelligence Section commander is responsible for administrative duties related to ensuring compliance with applicable rules, regulations, policies, and procedures.
- C. The RTIC will conduct information gathering in a manner that respects the constitutional rights of individuals, groups, or organizations involved. As such, the RTIC's activities should be limited to those necessary to achieve legitimate law enforcement objectives.
- D. In conducting intelligence gathering, RTIC personnel must adhere to the legal principles and public policies governing the collection, storage, retention, and dissemination of domestic and criminal intelligence data, see [Policy 1701 - Criminal Intelligence](#) and [SOP 3009 - Criminal Intelligence Records](#).

1703.2 Operations

- A. The primary function of the RTIC is to collect, process, analyze, and share information about potential criminal activity to prepare for, mitigate, and/or respond to such activity or a critical incident. Duties and responsibilities of members of the RTIC include:
 - 1. Planning, collection, processing, analysis, and sharing of criminal information.
 - 2. Threat assessment and monitoring.
 - 3. Development and implementation of special projects, strategies, and initiatives.
 - 4. Supporting criminal investigations and critical incident response.
- B. In response to public events and large crowds, such as street festivals, sporting events, or other outdoor activities, the RTIC may utilize available technological resources near relevant events to look for suspicious activity leading up to and during the event and report any activity as soon as possible and/or practicable to appropriate employees.

- C. The RTIC will support special operations, including joint operations across multiple agencies, such as the pre-planned execution of arrest and/or search warrants.
- D. The RTIC will use all databases in accordance with the department's guidelines and federal, state, and local laws and regulations; see [Policy 505 - Automated License Plate Recognition](#).
- E. Access to the RTIC areas will be restricted to authorized personnel only.

1703.3 Cameras and Video Feeds

- A. A legitimate law enforcement purpose is required to use and/or review video recordings that are accessible to, and/or are the responsibility of, the RTIC.
- B. Based on crime trends or active crime scenes, the RTIC personnel may monitor relevant cameras for suspicious or related activity.
- C. Department members must report any identified equipment issues to the Technology Unit. RTIC personnel will periodically inspect camera positioning, perform necessary camera maintenance, and address any required repairs.
- D. Video surveillance in public areas will be conducted in a manner that is both legally and ethically sound, while respecting and protecting constitutional privacy standards.
- E. Live streaming of body-worn or in-car cameras will be used in emergencies or exigent circumstances, and only with the permission of the Operations Bureau Commander.
 - 1. Livestreams will only be used to gain crucial information, such as officer location and current situation, to relay to responding units for situational and tactical awareness, or to expedite assistance as necessary. Use of the live-streaming feature may be considered, when necessary, during an ongoing critical or emergency situation, such as, but not limited to:
 - a. An active assailant
 - b. Barricaded subjects
 - c. Vehicle pursuits
 - d. An officer's failure to respond to communications

- e. Active emergency scenes while the officer's vehicle is at the scene or while stationed on the perimeter of the incident
 - f. Any other event as determined necessary by the Operations Bureau Commander.
2. Livestreaming of an officer's body-worn camera can only occur if the body-worn camera is already recording. Officers will receive an audio (beeping) and visual (camera light) notification if this feature is activated.
 3. Anyone activating the live streaming feature must complete a Live Feed Audit form. Quarterly audits of live streaming activity will be conducted by the Intelligence Section commander.

By order of:

Chief of Police