

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, compliance with state and federal laws, and the preservation of privacy and constitutional rights.

Policy Statement

It is the policy of the Asheville Police Department (APD) to operate its real-time intelligence function as a transparent, community-partnered public safety asset. The Real-Time Intelligence Center enhances situation awareness, optimizes emergency response, and supports active criminal investigations. The department is committed to complete transparency regarding system capabilities, voluntary community integrations, and accountability systems.

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 Operations

- A. The department's Technology Manager will provide overall leadership and supervision of the RTIC.
- B. The primary responsibility of the RTIC is to collect, process, analyze, and disseminate information about potential or unfolding criminal activity to prepare for, mitigate, and/or respond to such activity or a critical incident. Employees within the RTIC are responsible for:
 - 1. Monitoring incoming public safety calls for service, related call records, and radio traffic, checking resources and authorized criminal justice databases to support response to those incidents, and reporting findings to responding and/or investigating personnel.
 - 2. Assisting in planning for public events, large crowds, and special operations to provide support and intelligence gathering.
- C. RTIC personnel 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. RTIC personnel will use all databases in accordance with the department's guidelines and federal, state, and local laws and regulations.
- E. 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 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 incidents, RTIC personnel may monitor relevant cameras for suspicious or related activity. 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.

- C. RTIC personnel will periodically check camera positioning and perform any needed maintenance or repairs.
- D. 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 occur only if the 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.

1703.3 ALPR Systems

- A. RTIC personnel will follow the procedures listed in Policy 505 - Automated License Plate Readers.
- B. RTIC personnel will monitor the ALPR system and address alerts as appropriate.
- C. RTIC personnel will enter license plate numbers into the designated ALPR hotlist when requested and when they meet the required criteria.

- D. RTIC personnel will manually review vehicle data entered in the ALPR system(s) **at least once per shift** and remove any information found to no longer be relevant to an active investigation.

1703.4 Security

- A. Access to the RTIC areas will be restricted to only authorized personnel as determined by the chief of police.
- B. Remote terminal access will not be permitted.
- C. Recordkeeping, dissemination, management, and retention of any intelligence records generated by the RTIC will be safeguarded in accordance with the procedures in [SOP 3009 - Criminal Intelligence Records](#).
- D. Law enforcement information gathered through the RTIC will not be disclosed to any unauthorized person or entity, except as permitted by law or with a compelling need to share such information for legitimate law enforcement purposes, and only when appropriate safeguards are in place to protect the confidentiality of the information.

1703.5 Accountability

- A. The Intelligence Section commander is responsible for administrative duties related to ensuring compliance with applicable rules, regulations, policies, and procedures.
- B. Audits of ALPR records will be conducted as required by [Policy 505 - Automated License Plate Recognition](#).
- C. At least quarterly, the Intelligence Section commander will conduct an unannounced internal inspection of database queries and audits of live streaming from body-worn or in-car cameras for submission to the Technology and Intelligence Division Commander.
- D. Audit trails will be implemented to prevent unauthorized access. **At least quarterly, an unannounced internal inspection of database queries will be conducted...**
- E. Unauthorized access, use, or dissemination of department intelligence will be investigated and could result in revocation of system access and administrative or disciplinary action, up to and including termination; see [Policy 2301 - Administrative Investigations](#).