

Asheville Police Department Policy Manual

Chapter: 17 - Intelligence and 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 Operations
1703.2 Cameras and Video Feeds
1703.3 Security
1703.4 Accountability

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 strengthens situational awareness, optimizes emergency response, and provides critical support for 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 communicate 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 responses to those incidents; and reporting findings to responding and/or investigating personnel to provide an informed response.
 2. Assisting in planning for public events, large crowds, and special operations to provide support, information gathering, and enhance public safety.
- 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 will 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 criminal intelligence data; see [Policy 1701 - Criminal Intelligence](#) and [SOP 3009 - Criminal Intelligence Records](#).
- F. RTIC personnel will follow the procedures listed in [Policy 505 - Automated License Plate Recognition](#) for the use of such systems.

- G. RTIC personnel will not use tools or platforms that use facial recognition technology.

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 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 or arrange for 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.
 - 2. Use of the live-streaming feature may be considered during an ongoing critical or emergency situation, when necessary. This may include, but is not limited to, active assailants, barricaded subjects, vehicle pursuits, an officer's failure to respond to communications, active emergency scenes while the officer's vehicle is at the scene or while stationed on the perimeter of the incident, or any other event as determined necessary by the Operations Bureau Commander.
 - 3. 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.

1703.3 Security

- A. Key-card access to the RTIC areas will be restricted to only authorized personnel as determined by the chief of police. Other individuals needing access to the RTIC areas will be granted access only with the approval of an RTIC supervisor, and must be accompanied by authorized personnel at all times.

- B. Recordkeeping, dissemination, management, and retention of any intelligence records generated by the RTIC will be carried out in accordance with the procedures set forth in [SOP 3009 - Criminal Intelligence Records](#).
- C. 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 its confidentiality.

1703.4 Accountability

- A. The department will remain accountable and transparent in its actions to the extent permitted by law, with respect to the use of RTIC systems, the data collected, and the sharing of information with third parties.
- B. Access to any public-facing camera or license plate reading system will be documented for subsequent audit and oversight purposes.
- C. The Intelligence Section commander is responsible for administrative duties related to ensuring compliance with applicable rules, regulations, policies, and procedures.
- D. At least quarterly, the Professional Standards Section will randomly review user access logs within the Axon Fusus system and audit trails related to live streaming of body-worn or in-car cameras. Documentation of the review will be submitted to the chief of police or designee.
- E. Audits of ALPR records will be conducted as required by [Policy 505 - Automated License Plate Recognition](#).
- F. Unauthorized access or use of RTIC systems will be investigated and could result in revocation of system access and administrative, disciplinary, or criminal action.