# Asheville Police Department Policy Manual

**Chapter:** 17 - Intelligence and Analysis **Original Issue:** 12/1/1992

**Policy:** 1701 - Criminal Intelligence **Last Revision:** 10/1/2026

**Previously:** 1140 - Criminal Intelligence, 1703 - Gang Intelligence

**Contents**

Introduction
Policy Statement
Definitions
Rules and Procedures
1701.1 Responsibilities
1701.2 Intelligence Collection
1701.3 Intelligence Dissemination
1701.4 Gang Intelligence
1701.5 Security and Retention

**Associated Directives**

Policy 1002 - Confidential Informants
Policy 1703 - Real Time Intelligence Center
SOP 3009 - Criminal Intelligence Records

**Introduction**

This policy provides department members with guidelines and principles for collecting, analyzing, and distributing intelligence information.

**Policy Statement**

It is the policy of the Asheville Police Department (APD) to properly utilize criminal intelligence to enhance public safety and crime prevention. The department is committed to gathering data from all legal sources while maintaining strict adherence to constitutional rights and individual liberties. Intelligence will be used to identify criminal trends, anticipate emerging threats, and provide decision-makers with the information necessary to safeguard the community.

**Definitions**

Criminal Intelligence: information compiled, analyzed, and/or disseminated to anticipate, prevent, or monitor criminal activity.

Criminal Intelligence Records: all records or information that pertains to criminal intelligence investigations, including information derived from witnesses, laboratory

tests, surveillance, investigators, confidential informants, photographs, and measurements.

Reasonable Suspicion: sufficient facts to give a trained law enforcement officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. This suspicion must be supported by a criminal nexus, meaning a direct and logical connection between the observed facts and a specific violation of law.

**Rules and Procedures**

**1701.1 Responsibilities** [40.2.3 a]

A. The Technology and Intelligence Division commander is responsible for oversight of the department's criminal intelligence processes.

B. The Technology and Intelligence Division is primarily responsible for directing intelligence operations, coordinating personnel, and collecting criminal intelligence information for the department.

C. The department's Real-Time Intelligence Center is primarily responsible for evaluating, collating, analyzing, and disseminating criminal intelligence information to field personnel in support of active or ongoing events. It may also facilitate data collection through specialized technological tools; see Policy 1703 - Real-Time Intelligence Center.

D. Although the primary responsibility for criminal intelligence may be assigned to specific department personnel, all department members are responsible for reporting and properly handling intelligence information. All department members will adhere to the guidelines established in department directives regarding criminal intelligence.

E. The Criminal Investigations Division will handle confidential informants; see Policy 1002 - Confidential Informants.

F. The Technology and Intelligence Division Commander, or designee, in collaboration with the Criminal Intelligence Division, is responsible for conducting an annual review of criminal intelligence procedures and processes. [40.2.3 e]

**1701.2 Intelligence Collection**

A. The collection of criminal intelligence will be for the purpose of suppressing criminal activity or for a legitimate law enforcement need.

B. Information collected from all sources must be evaluated and designated according to its reliability, content validity, and relevance. Complete guidelines are outlined in SOP 3009 - Criminal Intelligence Records.

C. Information will not be collected on any individual or organization based solely on any of the following: ethnic background or race, religious or political affiliation, support of unpopular causes, or personal habits or lifestyles unless such information directly relates to possible violations of the law and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

D. Intelligence and information gathering, including by use of ALPRs, will be conducted in a manner that respects the constitutional rights of all individuals, groups, and organizations. Use of intelligence gathering tools and technology in connection with protests or public demonstrations will be limited to that which is necessary to support law enforcement's role in facilitating individuals' First Amendment right to express themselves while protecting participants and ensuring public safety.

E. Information gathering, including the use of confidential informants and electronic devices, will be conducted in a legally acceptable manner and in accordance with department directives.

F. Information readily found on the internet, in newspapers, publications, television, and radio broadcasts, or distributed for public consumption by any means, is open-source information that can be gathered, analyzed, and used to create open-source intelligence.

G. Criminal intelligence information developed or received by department members will be forwarded to the Intelligence Section commander or designee for review to ensure the information meets the criteria outlined in this policy. [40.2.1]

    1. Information from criminal justice sources, particularly other law enforcement agencies or investigators, may be forwarded directly via email or directed to contact the department's Intelligence Section

    2. Information from non-criminal justice sources, such as information gathered from citizens or confidential informants, should be submitted in writing to the department's Intelligence Section) whenever possible.

    3. All submitted criminal intelligence should include as much relevant and identifying information as possible to assist in evaluating the source's reliability and content validity.

### 1701.3 Intelligence Dissemination [40.2.3 c]

A. The department may disseminate information gathered and maintained for intelligence purposes only to authorized personnel for legitimate law enforcement purposes, in accordance with applicable laws and department directives.

B. Department members must not disseminate confidential criminal intelligence information or records of criminal investigations to individuals or criminal justice agencies except as outlined in department directives or when directed by a court.

C. External requests for criminal intelligence information from within the department will be directed to the Intelligence Section.

D. Criminal intelligence information collected by APD is not public record; however, criminal intelligence that is part of a criminal investigative file may be discoverable. The N.C. General Statutes will govern the disclosure of criminal intelligence information provided to a prosecuting attorney.

E. Procedures for labeling and outside dissemination are available in SOP 3009 - Criminal Intelligence Records.

F. Intelligence products will be compiled and provided to authorized recipients as soon as possible, where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or individuals emerge. [40.2.2 b]

### 1701.4 Gang Intelligence

A. Criminal gangs will be identified based on specific, documented, and reliable information.

B. An individual may be considered an active member of a criminal gang if they meet the criteria outlined in N.C. Gen. Stat. § 14-50.16A, as determined by the officer's experience and knowledge of criminal street gangs.

C. It is the responsibility of the department's Intelligence Section commander or designee to ensure that gang members are properly validated. Probable cause to establish an individual's membership in a criminal street gang must be corroborated by documented information. [40.2.3 a]

D. Criminal gang intelligence gathered by the department may be cataloged in specialized regional, state, and/or federal gang databases. [40.2.3 c]

### 1701.5 Security and Retention

A. All sensitive, restricted, and confidential files, both physical and electronic, must be secured. Access to intelligence records will be controlled and recorded in accordance with procedures established by the Intelligence Section commander and SOP 3009 - Criminal Intelligence Records. These procedures will include administrative, technical, and physical safeguards to prevent unauthorized access or damage. [40.2.3 b]

B. Criminal intelligence information will be retained only if it meets legal retention requirements. Information that is out-of-date or incorrect will be purged in accordance with applicable records retention schedules and SOP 3009 - Criminal Intelligence Records. [40.2.3 d]

By order of:



Jackie Stepp
Chief of Police