Cobb County Police Department

Policy 6.12

Real Time Crime Center

Effective Date: February 6, 2025	**Issued By:** Chief E.S. VanHoozer
Rescinds: N/A	**Page 1 of 5**
The words "he, his, him," which may appear in this policy, are used generically for clarity and ease of reading. These terms are not meant to imply gender and relate to all employees of the Department.	

The purpose of this policy is to establish the mission, use, and guidelines associated with the Real Time Crime Center (RTCC). This policy shall function in alignment with other established County and Police Department policies, including but not limited to:

- CCPD Policy 3.08 – In-Car/Body-Worn Cameras
- CCPD Policy 3.09 – Automatic License Plate Recognition (LPR) Devices
- CCPD Policy 3.11 – Property/Evidence Collection and Packaging
- Cobb County DPS Policy – Law Enforcement Communications
- Cobb County Policy – (ITS) Information Technology Policy
- Cobb County Policy – (ITS) Multi-Factor Authentication Standards
- Cobb County Policy – (ITS) Network Security Standards
- Cobb County Policy – (ITS) Technology User Account Standards

I. Mission

The RTCC uses technology to capture and share real-time information with law enforcement and other public safety personnel, facilitating resolution of public safety incidents. The RTCC also enhances officer and public safety by identifying and disseminating immediate and actionable information during real-time incidents and supporting post-incident investigations.

II. Definitions

A. FOReCAST

The Field Operations Response, Crime Analysis, and Strategic Technologies (FOReCAST) unit is responsible for operational control of the RTCC, the Crime Analysis Unit, and research and development of certain public-safety technology. This unit is commanded by a Police Lieutenant.

B. RTCC Platform

A web-based technology platform and all associated hardware, software, and services, with which the Department contracts, purchases, or otherwise uses to serve as the foundation of the RTCC. Access to this platform will comply with ITS and CJIS credential standards. Access that predates the effective date of this policy

shall be brought into compliance with this policy within six months of this policy's effective date.

C. Government-Owned Video Systems:

Any camera, network infrastructure, video recording device, or other hardware/software owned and maintained by a government entity.

D. Privately-Owned Video Systems:

Any camera, network infrastructure, video recording device, or other hardware/software owned and maintained by a private entity.

E. Public Safety Analyst:

A non-sworn position with the primary responsibility of supporting the operations of the RTCC.

F. Investigative Window:

The time period during which video and other data is available for analysis. Its duration is determined by factors such as storage capacity, data rates of integrated cameras, and other factors.

III. Organizational Structure and Staffing

The RTCC falls under the Special Investigations and Response chain of command (Deputy Chief) and is overseen by the Special Response & Technologies Commander (Captain). The following is the FOReCAST / RTCC hierarchy associated with its operation.

A. Commander:

The RTCC is commanded by a police lieutenant assigned to the FOReCAST Commander position who reports to the Special Response & Technologies Commander.

B. RTCC Manager:

The RTCC Manager is responsible for overseeing the RTCC and the Crime Analysis Unit. This position reports directly to the FOReCAST Commander.

C. Supervision:

The RTCC and the Crime Analysis Unit are supervised by RTCC Supervisors, with one supervisor assigned to each of the RTCC’s operational shifts.

D. Staff:

The RTCC is staffed by non-sworn Public Safety Analysts. Sworn personnel may be relied upon during specific events or for temporary assignment as directed.

IV. Data Usage, Retention, Auditing, and Policy Review

Each user is responsible for safeguarding their account from unauthorized access. All personnel shall exclusively access RTCC-integrated video through County-issued electronic devices. Any access beyond the scope of County-issued devices requires written approval from the FOReCAST Commander. Both the applying employee and the RTCC Commander must maintain a copy of the employee's written authorization approval for the duration of such access. Access that predates the effective date of this policy shall be brought into compliance with this policy within six months of this policy's effective date.

The use of RTCC technology or software is restricted to legal and policy-compliant activities while personnel are working in an on-duty capacity and location. Each authorized user must log into RTCC technology and software with their own credentials. Authorized users are prohibited from allowing unauthorized persons to access RTCC technology and software.

Nothing in this section is intended to limit the authority of the Department in conducting law enforcement investigations and other related activities.

A. RTCC Video and Data Usage

1. All recordings and information accessed, viewed, and disseminated through the RTCC shall only be used for legitimate law enforcement purposes, in compliance with federal and state laws, rules, and regulations. Information shall not be sought, gathered, or retained through any unlawful means or in violation of Department policy, county, state, or federal laws.

2. Except as required by law, subpoena, or court process, such data will not be otherwise disclosed by the departmental personnel without the approval of the Chief of Police or designee.

3. Department or external agency public safety employees requiring assistance with any footage or data derived from the RTCC platform should submit a request for assistance to RTCC personnel.

4. The RTCC integrates several existing technologies governed by specific established policies. Nothing in this policy shall override or supersede existing policies for those technologies.

5. No unauthorized recording, viewing, reproduction, retention, or distribution of RTCC video feeds or other data is allowed. Any data and imagery are only to be used for law enforcement, public safety purposes, or other reason approved by the Chief of Police or designee.

Under no circumstances shall an employee make a copy of a video for personal use.

6. Video cameras and other devices are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include but are not limited to: in response to an incident, special events, and specific investigations authorized by the Chief of Police or designee.

7. Pursuant to Policy 3.19 Facial Recognition, the Department shall not connect any facial recognition system to any interface that performs live video surveillance.

B. Video Data Retention

1. The RTCC Platform can be setup with both government-owned and privately-owned video systems. It is utilized to bring video in to the RTCC from disparate video systems during an investigative window.

2. Any data, video and imagery with evidentiary value will be stored by the investigating personnel in a department-approved evidence retention system in compliance with Policy 3.12 Property / Evidence Documentation and Storage.

3. Data retention associated with technologies having their own individual policies or applicable county, state, or federal laws shall adhere to the established data retention schedules.

C. Auditing

The FOReCAST Commander or their designee shall conduct random audits of the RTCC platform to ensure that access to integrated video systems complies with this policy. These audits will assess security measures, including user account management, proper credentialing, and camera access to ensure compliance with the RTCC only being utilized for legitimate public safety purposes. At a minimum, one sample audit shall be conducted annually. A memorandum summarizing the audit findings will be submitted to the Chief of Police by December 31 each year.

D. Policy Review

An annual review of this policy should be completed prior to December 31 of each calendar year to ensure it is accurate and complies with applicable law, rules, and regulations. The completion of this review shall be included in the annual audit memorandum to the Chief of Police by December 31 each year.

E. Camera Integrations

Businesses, other organizations, and private citizens can enhance the safety of their

community by consensually allowing the Department direct access to their video system in the event of a public safety concern on the property or area. This is carried out with the RTCC Platform serving as an intermediary between the privately-owned / government owned video system and the RTCC.

1. Each entity is required to authorize the RTCC Platform to allow departmental review of video applicable to the collection of real-time intelligence for public safety purposes.

2. It is understood the entity reserves the right to withhold any recordings made by their systems, necessitating Department personnel to obtain recordings through warrant or subpoena. The entity also solely controls how the video is shared with the Department.

3. The RTCC is not a camera monitoring service for the private entity and will only access cameras for public safety purposes.

4. Only public safety personnel or individuals authorized by the Chief of Police or his designee, will have access to live video from integrated video systems.

F. Georgia Open Records Act

1. The Department will accept Georgia Open Records Act requests for RTCC-related video through the Records Management unit. The Records Management unit may contact the FOReCAST Commander, the RTCC Manager, or RTCC Supervisors for direction on the response and accessing requested material/video data.

2. Georgia Open Records Act requests related to traffic management system cameras will be accepted and processed by the Department. Requests for video data shall not be directed to the Department of Transportation, as there are no recording functions in their video management system.

V. COMPLIANCE, ENFORCEMENT, REVIEW

Failure to comply with this policy may result in disciplinary action, up to and including suspension or revocation of RTCC operating privileges and termination. The Department will regularly review the RTCC's operations to ensure compliance with this policy, adjusting as needed to enhance operations and respond to new legal guidance.