

Standard Operating Procedure

Control Room Officer Duties & Daily Activities • Counter Crime Partnership

Document Date:	14/08/2026
Classification:	Website / Resources / Officers

1. Role Purpose & Core Principles

The Control Room Officer serves as the vital communications hub, intelligence filter, and operational anchor for the Counter Crime Partnership. Operating multiple localised radio channels (Town-Links) across retail parks, town centres, and evening economy venues, the primary focus is to facilitate real-time threat-warning between member businesses, manage the local Exclusion Zone system, and transform raw incident data into actionable intelligence for both Members and Police.

OPERATIONAL GUIDANCE NOTE: SUPPORT VS. DIRECTION

Whilst we use the call sign “Control” so that people visualise a Control Room and immediately understand the professional environment Control Room Officers work in, we are there to support and not direct.

For example, a CCP Member might be a store like Poundland, and the person using the radio might be a member of their retail team. As Control Room Officers, we have no authority to direct their actions, order staff movements, or command security interventions.

Our role is strictly to facilitate accurate communication, log intelligence, coordinate assistance, and empower local staff to make informed decisions.

2. Key Requirements

- **Integrity:** Control Room Officers must maintain strict personal integrity, as the role requires direct access to restricted operational intelligence and sensitive personal data.
- **Standards:** Must operate strictly within the legal frameworks of the Data Protection Act / GDPR, the Information Commissioner’s Office (ICO) registration (ZA509484), the BCRP National Standards and CCP’s own Constitution and Protocols.
- **Technical Aptitude:** Competence in operating digital fleet radio infrastructure and crime management software.

3. Standard Operating Procedures & Duties

3.1 Location, Dispatcher Console & SIA Operational Boundaries

- **Desk-Based Primary Presence:** Control Room Officers must spend the majority of their shift at their workstation. This stationary presence is vital because the core purpose of the role is to support members in an administrative and intelligence capacity—such as capturing critical information and

logging notes that a member actively dealing with a live situation cannot. This level of support is reduced if the Control Room Officer is out of the office.

- **Dispatcher Console Capability:** Operating from the primary workstation provides full, comprehensive and large screen access to all relevant system tools and some management features that are unavailable on handheld radio units.
- **Site Visits & Face-to-Face Support:** Occasionally, Control Room Officers may need to visit member premises to check equipment or provide direct face-to-face support.
- **Strict SIA Licensing Boundaries & SentrySIS Incident Protocol:** During Site Visits or while away from the desk, Control Room Officers cannot persistently act in any capacity that would be considered 'licensable' by the Security Industry Authority (SIA). In the event that an officer does become involved in a situation, the SentrySIS Incident must be logged and managed entirely by another Control Room Officer.

OPERATIONAL GUIDANCE NOTE: CALL SIGN

Control Room Officers will be allocated unique Call Signs, for example Charlie-Romeo-One-Five for use when operating remotely.

3.2 Live Radio Fleet Monitoring & Emergency Contact Protocols

- **Simultaneous Monitoring:** Continuously monitor all designated live Town-Link radio channels across active geographical zones to ensure immediate oversight of emerging incidents.
- **Radio Broadcast Clarification Protocol:** When members use the CCP Radio network to advise others of an incident, transmission clarity varies. Control Room Officers must intervene to clarify and read back key details, ensuring the reporting member feels entirely supported and never embarrassed or 'silly' for omitting details. Officers must maintain a calm, thankful, and encouraging tone at all times. Standard broadcasts must systematically establish the following (ideally in this order):
 1. **Transmitting Location:** Which business/shop is transmitting or experiencing the incident.
 2. **Nature of Incident:** What specific event has occurred or is unfolding.
 3. **Individuals Involved:** How many subjects are involved.
 4. **Subject Identification:** Whether the individuals are known or unknown.
 5. **Physical Descriptions:** Brief, key physical and clothing descriptions.
 6. **Direction of Travel:** Which way they went after leaving members premises.
- **Encouraging Direct Member-to-Member Warnings & Busy Control Protocol:** Control Room Officers must actively encourage members to broadcast incidents and sightings directly to neighbouring stores rather than waiting solely to report them to Control. Members sometimes delay warning nearby businesses because they are waiting to speak directly with the Control Room. If a Control Room Officer is occupied on another channel, telephone line, or dealing with an active priority incident. Rather than asked a member to "standby unless urgent," (which is what members say if they

are busy), the officer should immediately prompt the member to broadcast their warning to local businesses directly over the radio (e.g., “Control engaged, if advisory please broadcast directly to all stores...”). This prevents critical delays—such as a member holding on a shoplifting warning for 5 minutes while an offender moves freely—and ensures surrounding stores receive instant situational awareness.

- **Emergency Services Contact Protocol (999 Directives):** Under operational agreements with Essex Police and the East of England Ambulance Service, member businesses must dial 999 directly from site during an incident. Emergency call handlers are specialized to assess live situations in real-time and, particularly during medical emergencies, must convey immediate, life-saving instructions directly to personnel on scene.
 - **State Zero Exception:** The sole operational exception where a Control Room Officer may dial 999 on behalf of a member is a 'State Zero' situation—defined as a critical incident where on-site personnel are actively using their hands to defend themselves against physical violence. In all other scenarios, members must make direct 999 contact, with Control Room Officers facilitating channel merging or relay support as required (further detailed in the CCP General User Guide).
- **Call Requests:** Respond promptly to "Call Requests" initiated by members via their advanced touch-screen radio units.
- **Misuse Channel Management:** In the event of improper radio use by a user, Control Room Officers can use their Dispatcher Console to 'drag and drop' the transmitting radio unit onto an unused channel, away from the primary network. Then explain the action privately to the member using a Secure Channel (also known as a point to point call). Any un-resolved improper radio use must be reported to the Lead Control Room Officer.
- **Interference Channel Management:** Control Room Officers should also 'drag and drop' radios to an unused channel in the event of a prolonged accidental press of the PPT button, to clear the active network. Be mindful to return the member to their original channel at the earliest opportunity because some radios have their channel change knob disabled.

3.3 SentrySIS Intelligence Management & Prioritisation

- **SentrySIS Incident Recording & Officer Discretion:** While members hold primary responsibility for logging their own SentrySIS Incidents, Control Room Officers should selectively record high-value or network-critical radio incidents directly into SentrySIS. Direct logging by an officer is appropriate when a member is unable or unlikely to submit a report, provided the officer possesses complete SentrySIS Incident details and has securely received the required imagery.
- **SentrySIS Data Entry & Tab Navigation Workflow:** When validating a SentrySIS Incident record, Control Room Officers must take responsibility for this record by pressing 'Manage Incident' and then systematically complete and verify data across all relevant entry tabs:
 - **Details Tab:** Check that the Member is correct – Sometimes Security Guards work in different premises, for example FRINTON TESCO and WALTON TESCO. As a SentrySIS user they will be linked to their primary premises so you may need to 'change' to the correct premises. Then, verify other Incident parameters, double-checking exact dates, times, and that there is a clear, objective summary of the event. Control Room Officers may edit the summary strictly to correct

spelling, grammar or remove inappropriate or superfluous text, but must not add new factual claims or make unverified assumptions. Any additional context or secondary intelligence – such as from personal memory of the incident or details gained through playing back radio incident audio – must be logged as separate entry in the Comments section of the SentrySIS Incident.

- **Location Tab:** Check that the Location of the SentrySIS Incident matches the details. A common error is for someone to add an Incident after they have finished work from home, so that location is logged.
- **Persons Tab:** Search for and link existing Profiles or create a new Profile for each person connected to the SentrySIS Incident, if this has not already been done by the Member. Ensure that the primary profile image is the best available frontal facial shot, cropped to head and shoulders.
 - **Member Profile Matching & Disagreement Protocol:** If a Member has linked the incident to an existing Profile and the Control Room Officer disagrees with the match, the CRO must add an objective comment to the Incident noting this observation. Officers must strictly adhere to the 'support, not direct' core principle, recognising that the Member may have seen the individual face-to-face and/or possesses deeper familiarity with their own CCTV system (accounting for camera distortion that can alter physical appearance).
 - **Facial Recognition Capabilities & Image Quality:** Control Room Officers may run Facial Recognition, but should note that its effectiveness relies heavily on having a clear, front-facing primary image on the existing SentrySIS Profile as well as a good-quality image on the new submission.
 - **Profile Merge Requests & Two-Party Verification:** Where multiple comments or observations accumulate suggesting that a newly created Profile matches an existing subject, the CRO should initiate a 'Merge Request' to combine the profiles. Merge requests must be formally logged with two-party verification (e.g., a Merge Request initiated by Mark SMITH, Security Guard at ICELAND, seconded by Scott PEPPER, Counter Crime Manager at CCP).
- **Media & Attachments Tab:** Verify that all securely transmitted imagery, CCTV clips, and supporting documentation are correctly attached.
- **Vehicles Tab:** Check that any associated vehicle mention in the SentrySIS Incident Description and/or Media tab is linked here.
- **Goods Tab:** Check that any Goods mentioned in the SentrySIS Incident Description and/or Media tab are logged here. Estimated values are acceptable, but check that they are ball park. If no goods are recorded as being involved, you may need to change Incident Type. A common issue is that Suspicious Circumstances are logged in error as an Attempted Theft.
- **Groups Tab:** Selecting the correct geographical groups is important because it ensures Members will see information relevant to them first. If Members then want to look at SentrySIS Incidents from further afield, they can. If the Incident happened in WALTON, the correct groups are 'FRINTON & WALTON' (where it happened), 'ESSEX' (WALTON is in ESSEX) and CCP (WALTON is in our BCRP territory).

- **Assessment Tab:** Control Room Officers must objectively assess the Source (Member & User), the Information and Handling Sensitivity. Guidance is given in SentrySIS for each aspect.
- **MG11 Tab:** This tab does NOT have to be addressed for the purposes of Control Room Officers assessing and authorising (making visible) a SentrySIS Incident. Specialist training is also required.
- **External Source & Social Media Data Policy:** SentrySIS Incidents and SentrySIS Notifications may occasionally be logged if published by verified sources (e.g., local Police or local newspapers). However, adding incidents or images directly from social media is strictly prohibited. The only exception to this rule is if a CCP member or Control Room Officer can independently verify the information and explicit permission has been obtained from the victim.
- **Prioritised Live Activation:** Review and transition logged SentrySIS Incidents based on strict operational timelines:

Priority Level	Target SLA & Operational Action
High Priority	Immediate to 5 Mins: High-value theft or attempted theft by an unknown offender unfamiliar to the reporting member. Turn live instantly to warn the network.
Normal Priority	Within 15 Mins: Lower-value theft or attempted theft by an unknown offender unfamiliar to the reporting member.
Low Priority	Within Shift: Processing and logging administrative data, including Warning Notices and Banning/Exclusion Notices.

- **SentrySIS Incident Lifecycle & State Management:** Manage Incident logs through four distinct status states within SentrySIS:
 - **Pending:** Newly logged SentrySIS Incidents that have not yet been processed or evaluated by the Control Room team.
 - **Open:** Active SentrySIS Incidents currently being investigated, monitored, or processed in real-time.
 - **Closed Solved:** Represents a positive outcome for CCP— Specifically where a crime was successfully prevented and/or the offender was positively identified.
 - **Closed Unsolved:** SentrySIS Incidents where the offender remains unidentified or immediate action could not be taken at the time of the event.
- **Ongoing Value of Closed SentrySIS Incidents ("Closed ≠ No Further Action"):** Closing a SentrySIS Incident does not mean 'No Further Action.' For 'Closed Solved' cases, the documented evidence may continue to be acted upon by Police, and the written record is actively used by CCP Members to legally justify denying entry to known offenders. For 'Closed Unsolved' cases, the Control

Room team will systematically compare Profile pictures against incoming imagery and intelligence as new information arrives.

- **Profile Management & Data Retention:** Maintain up-to-date Profiles, documenting new information about physical descriptions, such as Tattoos and ensuring that the highest quality front facing images are set as the primary Profile image.
- **Data Retention:** Periodically check the Upcoming Profile Scrubs Report of expiring Profiles, which are set to automatically delete 2 years after their most recent activity. Occasionally, we will have heard on the Radio that a person is active again, but no one has cancelled the automated deletion by adding a SentrySIS Incident. If this is the case manually over-ride the deletion; which will require a written explanation.

3.4 SentrySIS Account Administration & User Allocation

- **Premises Account Creation:** Ensure that every active CCP member premises has a dedicated SentrySIS account set up and maintained.
- **User Allocation & Authorisation:** Each premises account includes a standard allowance of up to 5 individual user profiles. It is strictly the Store Manager's decision to determine which staff members are assigned user access for their premises. While additional user slots beyond this baseline normally incur an added cost, SentrySIS permits administrators to carry over and balance user allocations across multiple premises belonging to the same member business.
- **Allocation Balancing Protocol:** When a Store Manager of a multi-site member requests an additional user for a site that has reached its 5-user cap (e.g., Aldi Walton), Control Room Officers can approve and create the new user without incurring additional fees, provided another store under the same commercial entity (e.g., Aldi Clacton only using 4 users) has unused capacity to offset the allowance.

3.5 Exclusion Zone Enforcement & Administration

- **Exclusion Tracking:** Support member businesses in managing and upholding the community-led Exclusion Zone, ensuring that barred individuals are correctly flagged within the network.
- **Notice Delivery:** Coordinate and assist in the administration process of serving official Warning or Exclusion Notices.
- **Member Assistance:** Provide swift verification for members who query unknown names or descriptions heard over the radio by checking live digital records to confirm if an individual is subject to an active exclusion.

3.6 New Member Engagement & Recruitment Dynamics

- **Promoting Partnership Benefits:** All CCP officers are actively encouraged to promote the benefits of joining the Counter Crime Partnership to potential new member businesses. While direct sales and recruitment are not the primary operational remit of Control Room Officers, understanding member decision-making dynamics is essential when communicating with prospective sites.

- **Retail Prospect Classification & Decision-Maker Engagement:** When discussing membership with retail businesses, officers should categorize prospective sites into three distinct operational structures to identify the appropriate key contact:
 - **Local Independent Retailers:** Generally, the business owner is on site and serves as the primary, direct decision-maker.
 - **National Chains:** Before engaging with national chain stores, officers must consult the CCP Counter Crime Manager to verify whether an existing organisational relationship already exists with that chain. If a partnership is already established, onboarding may simply require the local store manager to reach out to a designated contact within their corporate head office.
 - **Franchises:** These are locally owned businesses operating under a larger High Street brand (e.g., McDonald's). For franchise operations, the decision-maker is usually the individual franchisee, not usually working on-site, so officers should focus on establishing who holds that franchise ownership.

3.7 Member & Stakeholder Relations

- **Real-Time Support:** Act as a calm, authoritative, and helpful partner for Retail Staff, Security Guards, and SIA-licensed Door Supervisors, encouraging (not directing) collaborative "safety in numbers" communication.
- **Assistance to Non-CCP Members & CCTV Restrictions:** Control Room Officers must fully support CCP members if they choose to assist non-CCP member businesses during an incident. Any incident involving assistance to a non-member must be logged in SentrySIS strictly from the perspective/standpoint of the assisting CCP member. Furthermore, it is strictly prohibited to add or upload any CCTV footage or images originating from non-member premises without their explicit permission, which must be logged in the incident write up.
- **Multi-Agency Liaison:** Serve as the direct operational bridge between private business security teams, humanitarian/street agencies, and local neighborhood policing teams to foster swift, collaborative crime reduction.