Watch Commander

Contents

Policy Statement

Summary West Yorkshire Police uses in car CCTV as an **overt** evidence gathering tool to promote public reassurance, capture best evidence, modify behaviour, prevent harm and deter people from committing crime and anti-social behaviour.

The chosen system to record video in Police vehicles is called '**Watchguard**'

An additional feature of Watchguard is **Watch Commander**, which allows live streaming of footage over a secure 4G network from any of the 3 installed cameras in compatible vehicles to the force network.

The purpose of this policy is to ensure that officers and staff comply with legislation and force requirements, and are aware of their responsibilities in relation viewing live streamed footage from compatible Operational Support vehicles.

Scope This Policy applies to all Police officers, Supervisors and Police support staff who use Watch Commander.

Principles

General
- The use of live streaming from Watch Commander can:
  - Assist in real time risk assessments during authorised pursuits by trained TPAC TAC advisors & force communications supervisors;
  - Facilitate enhanced tactical assessment for firearms related incidents;
  - Allow real time viewing from vehicle cameras in the Special Operations Room (SOR) for special deployments, for example, category A type escorts;
  - Assist supervisors when it is believed that there is a serious risk of harm or injury to any officer within or around their vehicle; and
  - Support transparency, trust and confidence in the police.
- Only **authorised staff** will be able to access Watch Commander.
- Access will be granted on a case by case basis by system administrators with the expectation that it will mainly be used by:
  - TPAC Tactical advisors;
  - Firearms Tactical advisors;
  - Force command supervisors;
  - Force duty officers (FSUP);
  - Road Policing supervisors;
  - Firearms supervisors;
  - Special Operations Room (SOR) commanders / operators;
  - IT administrators for testing and diagnostic;

- ○ Vehicle preparation unit technicians for testing and installation; and
- ○ System single point of contact for system for testing, training and diagnostics.
- Watch Commander has two levels of access:
  - ○ **Admin:** Force IT Administrators who can access the system, live stream from vehicles and add/remove users. They also able to audit log files.
  - ○ **Users:** All other authorised users including vehicle preparation unit technicians for installation and testing purposes.
- Most users of the system will fall under the USER level access.
- Due to the very simple web based interface, there is no specific requirement for training prior to using Watch Commander.
  However it is expected that all users familiarise themselves with this policy prior to use.
- Officers and staff have a positive duty to collect the best available evidence and could face disciplinary action if they fail to do so.
- Officers should **never** disconnect, sabotage, circumnavigate or in any way attempt to reconfigure the 4RE system, 4G routers or any associated cabling or network equipment.
- Users have an obligation under the legislation detailed in this policy to comply with and respect privacy. Disciplinary action may be taken should a user intentionally breach this policy.

Technical Information

Principles

- The equipment installed in the vehicle is referred to as Watchguard 4RE.
- There are 3 fixed cameras in the vehicle, referred to as Front; Cabin & Rear.
- A 4G Speedroute router installed in the vehicle, connected by ethernet cable from the Watchguard smart hub.
- An O2 sim card routed through West Yorkshire Police's APN network facilitates connectivity to the Police network
- Footage is streamed directly to the Watch Commander server which is installed at Dudley Hill data centre.
- Users view the streamed footage via the 'Watch Commander' website on the WYP intranet, which is only accessible by authorised persons.
- Watch Commander is hosted locally by West Yorkshire Police.
  Due to security requirements, there is no external access.

Right to Record/View

Principles
- Officers and staff must consider article 8 of the Human Rights Act 1998 - the right to private and family life, officers **must not** connect to a vehicle and view live footage unless it is necessary for:
  - Allowing for real time risk assessments during authorised pursuits by trained TPAC tac advisors and appropriate supervisors;
  - Allowing enhanced tactical assessment for firearms related incidents;
  - Allowing real time surveillance in the SOR for category A type escorts;
  - Allowing access to communications supervisors when it is believed that there is a serious risk of harm or injury to the officer within or around their vehicle;
  - Testing and diagnosis of the system; or
  - Limited use for training and necessary demonstration.

Privacy

Principles
- Due to the intrusive nature of live video streaming access to the system is strictly limited to the roles detailed, and this policy sets out its usage reasons and rules.
- **Breach of this policy would undermine officer confidence in the Watchguard system, as well as potentially breach data protection, and human rights legislation.**
- When a Watch Commander user makes a remote connection to a vehicle they are able to view live video from any of the 3 cameras installed in the vehicle.
- Under certain conditions, users have the ability to hear audio through the installed microphone from within the vehicle.
- Live audio only possible when the Watchguard system is in an 'Event Record' state (for example, responding, pursuing or dealing with a member of the public at the roadside).
- The officer in the vehicle can also manually activate the microphone.
- When the microphone is activated, the 4RE control panel in the vehicle will display an orange illuminated '3'.
- When a remote connection to the vehicle is established, the vehicle user is informed by an audible beep, and an eyeball icon displayed at the top of the Watchguard 4RE screen.
- Taking into consideration article 8 of the Human Rights Act 1998 - the right to private and family life, users should make every effort to inform the vehicle occupants that they are about to commence a live stream connection. This includes connections for the purpose of testing and diagnostics.
- Where it is not practicable to contact the vehicle users prior to connection, Force communications supervisors should announce on the relevant radio channel that live streaming is in use.
- For pre-planned operations, the potential use of live video streaming should be included in the briefing.

- Users should only connect to a vehicles live stream for genuine policing purposes and in the interest of supporting a live incident, offering tactical advice or to gain necessary situational awareness.
- To respect privacy and professionalism live streaming **must** be used with the knowledge of those officers present and not for speculative viewing of their shift

Responsibilities

Watch Commander Users

Responsibilities Officers and staff who are Watch Commander are responsible for:
- Only using Watch Commander in relation to live ongoing incidents and operations as detailed above where the need exists;
- Only viewing video from vehicles directly involved in the associated incident;
- Making it known that live streaming is in use to those involved in the particular incident; and
- Announcing on the respective radio channel that live streaming is being conducted if the vehicle user cannot be contacted or it is not practical to do so.

Professional Standards Department

Responsibilities The Professional Standards Department are responsible for:
- Ensuring use is for Policing purposes only and that policy and legislation is complied with; and
- Investigating complaints in relation to misuse of the system.

Additional Information

Compliance This policy complies with the following legislation, policy and guidance:
- Protection of Freedoms Act 2012
- Freedom of Information Act 2000
- APP Information management
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- Human Rights Act 1998
- Criminal Procedures and Investigations Act 1996
- Police and Criminal Evidence Act 1984

- College of Policing Code of Ethics 2014
- Surveillance Camera Code of Practice June 2013
- NPIA Practice Advice on Police use of Digital Images 2007
- Information Commissioners Data Protection
- Information Commissioners Code of Practice – conducting Privacy Impact Assessments

Further Information	Further guidance in relation to this policy can be sought from: • The Watchguard iLearn