Watchguard

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'.

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 to securing and preserving best evidence and safeguarding the integrity of the captured digital images, if these need to be used in criminal or complaint proceedings.

Scope

This policy applies to all police officers and police staff who use Watchguard to provide video evidence to support prosecutions.

Principles

General

- The police service has the power to use Watchguard under common law.
- If a member of the public objects to being recorded in or around the Police vehicle, the officer will continue to record and explain their reasons for doing so. These include:
  - That an incident has occurred requiring police to attend;
  - The requirement to secure best evidence of any offences that have occurred, whether this is in writing or on video, and the video evidence will be more accurate and of higher quality and, therefore, in the interests of all parties;
  - Continuing to record would safeguard all parties with true and accurate recording of any significant statement made by either party;
  - An incident having previously taken place may recur in the immediate future;
  - Continuing to record will safeguard the officer or staff against any potential allegations from either party; and/or
  - Officers and staff must consider article 8 of the Human Rights Act 1998 - the right to private and family life, officers must not record beyond what is necessary for the evidential requirements of a case.
- The use of Watchguard can:
  - Support transparency, trust and confidence in the police;
  - Enhance opportunities for evidence capture and help employees gather evidence of road traffic offences, and at incidents of crime and disorder;
  - Provide independent evidence to improve the quality of prosecution cases;

  - Increase early guilty pleas;
  - Reduce employee case preparation and court time;
  - Reduce protracted complaint investigations (providing impartial and accurate evidence);
  - Allow for real time scene assessment by tac advisors and supervisors with live streaming;
  - Provide timely resolution of Police related collisions and vehicular damage;
  - Aid driver training and assessment; and
  - Support evidence and scene assessment at firearms operations and live time incidents
- The equipment fitted within the vehicle is referred to as 4RE, along with 3 fixed cameras, referred to as 'FRONT HD' Cabin & 'Rear'.
- The website used to view, evidence and edit event recordings is referred to as Evidence Library 4 or EVIDENCE LIBRARY and is hosted locally by West Yorkshire Police.
- Live Streaming is enabled using in car 4G routers, and live footage accessed using 'Watch Commander' and only accessible by trained and authorised persons. Watch Commander is hosted locally by West Yorkshire Police.
- Video recordings uploaded to EVIDENCE LIBRARY on the force network are referred to as 'Events'.
- 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 **must not** disconnect, sabotage, circumnavigate or in any way attempt to reconfigure the 4RE system.
- Completed recordings must be retained and handled in accordance with the APP – Information Management. Any breach of the APP or this policy may render the user liable to disciplinary action and/or adverse comment in criminal proceedings.
- The master copy is retained on the EVIDENCE LIBRARY server and is the primary exhibit. Any subsequent copies are working copies and are exhibited as such.
- In court proceedings, the Defence solicitor/counsel may try to get in-car CCTV evidence excluded if its content contains compelling evidence. For this reason, this policy **must** be strictly adhered to.

Training

- There is an expectation that all trained officers and staff in relevant roles will use Watchguard in every case where a Roads Policing Unit, Driver Training or Armed Response Vehicle fitted with 4RE is used and where there is public contact for a policing purpose.
- This means where a degree of investigation or the exercise of police powers is required.
- The rationale for not using Watchguard or stopping the event recording prematurely may need to be explained at a later stage and justified to a supervisor, Professional Standard, IOPC and or during court proceedings.

- All Road Policing Unit, Firearms, Driver Training staff and their supervision will be trained in the use of the 4RE equipment and EVIDENCE LIBRARY software to ensure the equipment is used properly, proportionally and in compliance with legislation and codes of practice.
- Training can take place in person by an approved trainer, or by use of the force iLearn facilities.
- Only trained officers and support staff will use Watchguard 4RE, access EVIDENCE LIBRARY and or Watch Commander web sites. In line with the Computer Misuse Act. All interaction with these web sites is audited.
- Officers and staff must complete all training in order to become an authorised Watchguard user.
- There is an iLearn on Watchguard for officers and staff to complete.

Usage

General

- Individuals must log into the 4RE system at the start of a shift.
- If double crewed, the driver of the vehicle must log in and Events will initially be tagged using their details.
- If the driver is not the OIC for that event recording, then they must edit the officer details tag once the event has been uploaded to Evidence Library 4. All edits to event details are recorded in the audit log.
- The only exception to this is when a user has to respond immediately to an incident using a vehicle in a 'dark' state and they have not had opportunity to log on. The user must then log on at the first opportunity afterwards.
- Officers must ensure that all 3 cameras (Front HD, cabin and rear) are functioning prior to using Watchguard. All 3 camera feeds will be displayed on the 4RE screen.
- Officers must ensure that there is a USB memory stick installed. This is signified by two vertical bars on the left hand side of the screen.
- Watchguard records all 3 cameras at all times to an 80 hour loop on an internal hard drive whilst the vehicle ignition is on, and for 30 minutes after the ignition is turned off.
- Audio is **only** recorded on the system during an 'Event recording'. During routine patrol, no audio is recorded.
- Officers can turn the microphone on at any time during routine patrol by pressing the 'microphone' button on the 4RE control panel and touching 'Cabin' on the screen. A live microphone is indicated by an orange illuminated '3' on the 4RE control panel.
- To aid the investigation of public complaints or Police collisions all blue light response drives will be event recorded. Unless it is an evidential recording, these will be tagged as 'Non evidential' when the recording is stopped.

Recording

- In all cases, officers and staff must use their professional judgement with regard to recording. Recording must be:
  - Incident specific; and
  - In pursuit of a legitimate policing aim
- Only Event Recordings will be uploaded to the force network. Any other footage will be retained on the car's hard drive until it is naturally overwritten – normally 2-3 shifts.
- Watchguard will go into an automatic Event record upon one or more electronic triggers being activated. Those triggers are the activation of the vehicles emergency blue/red lights or sirens.
- There is a 5-second grace period between the trigger being activated and an event recording commencing. If the blue lights are turned off within this 5 seconds and event will NOT be started. The purpose of this is to allow for momentary use of lights as a warning, to attract attention without the need to record an incident.
- Officers may also initiate a manual event recording without use of external triggers by pressing the record button on the 4RE control panel.
- When members of the public are intentionally video recorded, officers must inform them of the use of in car CCTV using straightforward (plain English). This must be at the time of activation or as soon as practicable after the incident which can easily be understood by those present, e.g. **"I am using an in car CCTV system, I just need to tell you that you're being video and audio recorded."**
- All significant comments **must** be recorded in writing in a PNB and offered to the individual to sign, even if they are recorded using Watchguard (PACE Act 1984).
- An Event Recording can be created retrospectively using '**Record After The Fact'.** This must be done before footage is recorded over.
- It is evidentially important to record as much of an incident as possible, therefore, it must begin at the earliest opportunity, i.e. as soon as the officer witnesses an offence, or start to respond to the incident or considers stopping a vehicle.
- Watchguard will automatically add 1 minute to the beginning of the recording prior to the automatic or manual triggered event recording. **This one minute pre-recording will not have sound.**

Post Recording and Tagging

- As soon as practicable, after the desired recording has concluded officers must press **STOP** on the 4RE control panel.
- Officers are then required to choose and appropriate event tag in accordance with training. This screen is compulsory and is used to manage MOPI (Management of Police Information) compliance for the event recordings.
- A recorded event **must** be categorised immediately upon pressing stop. It is not acceptable to leave the system on the Event Category screen, as this will save the recording as 'unknown' and will fail to comply with MOPI. This

is a breach of Data Protection, as the video will never be deleted from Police systems.
- Recordings that do not contain any evidential material must be tagged as 'NON EVIDENTIAL' so that they are purged from the system after 90 days
- The secondary tag screen 'Notes' is optional, and for officers to include any pertinent information relating to that recording.
- It is **not** necessary to save any notes with non-evidential videos
- If officers do not have an opportunity to tag a recording at that time then they must edit the tag either before it is uploaded via Wi-Fi or once it has been successfully uploaded to EVIDENCE LIBRARY.
- Untagged videos are not acceptable and do not comply with MOPI. It is the recording officer's responsibility to manage tags.

Live Streaming

- Authorised supervisors and certain users that are not of the rank of Sergeant and oven are able to connect to any Watchguard equipped vehicle and see a live video stream from any of the 3 installed cameras and if and event is being recorded they can also hear live audio.
- The live stream connects to the force network by 4G APN. Live video is viewed using the 'WatchCommander' website.
- When a user connects to a live stream, officers in the vehicle are informed by an audible beep and an icon of an eyeball in the top left corner of the screen.
- Users must only connect to a vehicles live stream for policing purposes:
  - In the interest of supporting a live incident,
  - To offer tactical advice; and/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.

Tagging Categories and MOPI Retention Periods

Information

- After pressing stop officers **must** choose one of the following categories based on the type of recording and necessary retention period.

Category	**Quality** (Saved in….)	**Retention Period** (Deleted after…)
Non-Evidential: Non-evidential footage from blue light responses, and stop checks that do not result in any further action.	Standard Definition	90 days
Traffic Offence: Traffic tickets & reports – these will be TOR	High Definition	2 years

offences / fixed penalties and low level 192 file summary offences that would generally be finalised within 2 years		
Driver Training: This will include video recorded in the driver training vehicles for training and debriefing purposes.	Standard Definition	90 days
Crime: This will be any low level crime including OPL, Dangerous driving, burglary, any offence that would require an MG file rather than a 192 traffic offence report.	High Definition	7 years
Crime Serious: Fatal's, Murder, and any other high-level crime.	High Definition	100 years
Fail to Stop: Any fail to stop pursuit that does not fall into one of the above categories. Generally used for FTS pursuits that do not result in an arrest, or prosecution or have on going enquires. If a fail to stop pursuit results in an arrest or prosecution then change it to CRIME or TRAFFIC OFFENCE category instead.	High Definition	7 years
Firearms: Any incident involving firearms offences or operations. If the incident results in a fatality, or substantial offices then must use CRIME SERIOUS instead.	High Definition	7 years
Encounter: Used to tag any recording that is non-evidential but worthy of separating out as of interest. This could include any recording such as potential complaints, unusual encounters with members of the public that have not yet developed into investigations. Categories can be changed on Evidence Library at a later date – within 31 days.	Standard Definition	90 days
Road Traffic Collision (RTC): This will include evidential RTC and Police RTC's which do not fall into one of the other categories. Also includes Police RTC's and POLVEH	High Definition	7 years

damage. If you attend an RTC and do not video anything evidential then tag as Non- Evidential.		
In Car Interview: Any interview carried out in the vehicle for which you wish to retain the video recording. If this relates to a crime or traffic offence then use that category instead. However, please consider force policy on use of Body Worn Video for such interviews.	Standard Definition	90 days
Section 59: Video evidence of 'due care' offences, which have been dealt with by either a section 59 warning or a seizure.	Standard Definition	2 years

Managing and Storing Footage

Storing

- Video will be recorded to a hard drive within 4RE system in the vehicle; Events are also copied to a USB memory stick as a backup until events are automatically uploaded over Wi-Fi after which time footage on the memory stick will be deleted.
- Dedicated Wi-Fi at selected sites with wireless access points will be used to upload the footage and officers must provide a full audit trail to maintain evidential continuity.
- USB upload is to be only be used if the vehicle cannot attend an approved Wi-Fi upload site (EG: RTC damage), or subject to IoPC / Post Incident Procedure incident where event upload is kept in separate dedicated storage location. In all cases, the USB memory stick **must** be returned and re-inserted back into the same 4RE system it came from as soon as possible.
- Each event carries a unique identifier known as an 'Event ID' and is time and date stamped throughout. Once recorded, footage **cannot** be amended or deleted by the user.
- Best practice is to use the Event ID when referring to the video on any police systems or documents as this is unique.
- All Events recorded are the property of West Yorkshire Police and will only be uploaded via dedicated Wi-Fi access points and retained on the West Yorkshire Police ISILON storage network.

- Non-evidential recordings will be uploaded and retained for 90 days in line with national guidelines. During that time they are searchable and can be retrieved and marked as evidential if circumstances dictate.
- Evidential recordings will be retained in line with the Authorised Professional Practice – Information Management. MOPI and the retention period is pre-set by West Yorkshire Police according the specific event category. This is why it is important to tag the event, and to tag it with the appropriate tag.
- In **rare** circumstances, it may be necessary to prevent the event from purging at its pre-defined expiring date. This **must** be justified on the event notes. As soon as the need to retain that event has elapsed then the event **must** be deleted.
- Images are recorded and retained for policing purposes and as such **must not** be shown or given to unauthorised persons.

Exporting

- Watchguard footage is primarily stored and viewed from West Yorkshire Police's internal network with no necessity to export it.
- Events can be exported to DVD or local hard drives. This must only be done for a policing purpose, and when necessary. Ideally, footage will be viewed or played back direct from EVIDENCE LIBRARY.
- EVIDENCE LIBRARY comprises of a fully auditable networked system. Footage can be viewed via standard computers where footage trimming can take place. This footage is viewable by others involved in the investigation process.
- There may be times when footage is required to be exported to another medium in order to be disclosed or played off-line.
- Footage can be exported to DVD or as a file on USB or sent online via DADS (Digital Asset Delivery System) in multiple formats.
- WYP Prosecution team have agreed with CPS that the format to be used is MP4 (H.264 codec). This preserves the original quality and picture size.
- It is possible to export in DVD format however; this reduces the quality of the video from the original, and can take considerable time to export, as the video has to be transcoded.
- It is the OIC's responsibility that all DVD copies will be exhibited, securely transported and stored.
- The production of DVDs and their **secure transfer** to other partners must be recorded to ensure compliance with the Data Protection Act and in accordance with Information Sharing Agreements. This process serves to protect the individuals involved and the organisation in the event of a data breach. .
- Footage **must not** be shared with the media without authority of West Yorkshire Police press office.

Responsibilities

All officers and staff

Responsibilities

Police officers and police staff are responsible for:

- Ensuring that they log into 4RE and that it is working correctly before leaving police premises;
- Reporting faulty cameras or 4RE via a RT11 form, and emailing immediately to Unit 41 garage;
- Recording all blue light runs by triggering a recording using the light control panel – individuals **must not** stop the recording until at scene or cancelled.
- As far as practicable, avoiding collateral intrusion by restricting the recording to areas and persons necessary in order to obtain evidence and intelligence relevant to the incident;
- Being aware of personal and community sensitivities and the necessity to record;
- Recording continuously, i.e. without interruption, from the start of the incident to its end and the resumption of normal duties, unless the incident has ended before they arrive or the specific nature of the incident makes them re-consider the rationale for recording it, e.g. incidents of a sensitive nature.
- Recording their decision in a PNB or similar log and including their rationale, where the recording of an ongoing incident is interrupted or stopped.
- Stopping the recording as soon as practicable after the incident or the need for Event recording has concluded;
- Tagging a recording with the appropriate Event tag and notes as soon as STOP has been pressed;
- Updating the occurrence OEL / 192 accordingly to assist any subsequent investigation by pasting the **Event ID** (from EVIDENCE LIBRARY);
- Ensuring that any confidential personal information is not revealed at the disclosure or interview stage to the suspect or solicitor;
- Uploading all footage recorded on the device to the server via the dedicated Wi-Fi access points – or emergency USB sticks;
- Identifying evidential footage by the Event ID, exhibit number, incident type, vehicle registration, and name(s) of any accused person(s);
- Only producing a DVD at the point of charge. The master copy will be retained on the West Yorkshire Police secure server and the working copy (DVD) forwarded with the case file;
- Ensuring they are aware of all content on the footage prior to any disclosure. If the working copy contains sensitive information, ensuring the DVD is marked ***'DO NOT DISCLOSE'***. Alternatively, considering using several trimmed clips to protect sensitive information. Footage that is confidential can then be outlined on the sensitive material schedule.

- Ensuring that if a recording contains sensitive audio or images then these must be redacted by the force imaging unit prior to disclosure;
- Providing written statements which must include the audit trail for the capture of the footage and the subsequent production of the working DVD. Both the networked stored master copy and any subsequent cropped copies require exhibiting along with any DVDs produced. For copies stored on the secure server, this can be achieved by using the EVIDENCE LIBRARY Software.
- Indicating that the footage has been viewed before writing the notes, if this has been done;
- Providing a single witness statement in relation to the incident and including the Watchguard footage and subsequent handling;
- Logging out of 4RE at the end of a shift, ensuring that recordings of events are in someone else's name; and
- Leaving the 4RE system turned on so that Events can be uploaded automatically over Wi-Fi. The system will shut down after 60 minutes.

Supervisors

Responsibilities

Supervisors' on Watchguard are any authorised officer of the rank of Sergeant and above. Supervisors and SLTs have a duty to enforce the use of Watchguard effectively and lawfully. They have additional privileges in addition or normal user rights.
These include the ability to view 'restricted' events.
Supervisors are responsible for:

- Ensuring staff are sure of their obligation to use the Watchguard system proportionately when circumstances arise;
- Reviewing recordings of incidents for development purposes i.e. assessing the individuals performance and how they could improve the ways they deal with them;
- On receiving a complaint, ascertaining if Watchguard was used during the incident. If yes:
  - Ensuring the recordings are marked as one of the evidential tags; informing the complainant; endorsing the incident log;
  - Making the log and the information about the use of Watchguard available to the person reviewing the complaint; and
  - Arranging for the 'restricting' of footage if appropriate.
- Ensuring any footage used in interview/proceedings has been considered and redacted to safeguard inappropriate disclosure of sensitive personal information. This can be during the quality assurance of file submissions.

District SLT SPOCs

Responsibilities

District SLT Single Points of Contact (SPOC) are responsible for:

- Ensuring the use of the devices is in line with legislation and codes of practice;
- Collecting usage data for performance monitoring;
- Monitoring and reviewing operation of the policy locally;
- Investigating any breaches of security and reporting them to the Information Management;
- Ensuring any newly appointed or returning officers or staff / transferees are trained in the use of the device; and
- Setting the appropriate level of user rights.

District Super Users

Responsibilities

District super users are officer or staff members who have been trained in the use of Watchguard and chosen for this role. They are responsible for:

- Supporting and guiding colleagues in the effective use of Watchguard, due to their high level of knowledge and physical use of the system and EVIDENCE LIBRARY as well as their understanding of the legislative requirements.

Professional Standards Department

Responsibilities

The Professional Standards Department (PSD) are responsible for:

- Adhering with the national direction on dip sampling; interrogating the system only if a complaint is received and if this is an appropriate line of enquiry.

PSD will **not** routinely search the back office system for misdemeanours or offences committed by users.

Additional Information

Compliance	This policy complies with the following legislation 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 • Computer Misuse Act 1990 • 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 • MOPI
Further Information	Further guidance in relation to this policy can be sought from: • The Watchguard iLearn