CCTV

This page is from APP, the official source of professional practice for policing.

First published 22 April 2024

21 mins read

The value of closed-circuit television (CCTV) cannot be overstated. Images and audio from CCTV footage play an important role in detecting crime, identifying potential witnesses, identifying and/or eliminating suspects, and identifying potential investigative opportunities, such as event timelines and further CCTV sources.

CCTV allows evidence to be presented in a unique way, letting the courts and jurors visualise aspects of the crime being described. Studies into outcomes using CCTV evidence demonstrate its importance and its direct benefits to crime investigation and achieving justice outcomes.

CCTV can also be a deterrent to potential offenders. It helps to reassure the public and also protects businesses, vulnerable premises and national facilities. It helps public authorities to manage ongoing incidents and is a useful tool when risk assessing scenes.

The Forensic Science Regulator (FSR), working closely with the National Police Chiefs' Council (NPCC), has developed quality standards for the recovery and processing of footage from CCTV and/or video surveillance systems (VSS).

Benefits

- Identify entry and exit routes from the scene of an incident.
- Identify behaviour and activities before, during and after an incident.
- Identify forensic opportunities, such as DNA and fingerprints.
- Help identify suspects, witnesses and vehicles involved.
- Verify a witness, victim or suspect account.
- Establish a timeline of events.
- Provide evidence of preparatory activities.

Outcomes

- Support with missing persons enquiries.
- Provide material for intelligence systems.
- Provide evidence of police actions or response.
- Help provide material to prove or disprove an allegation.
- Provide evidence of an offence that may lead to an early guilty plea.

Regulation

Anyone undertaking forensic science activities is considered a practitioner and therefore subject to the **FSR Statutory Code of Practice** ('the Code'). Irrespective of who does them, activities such as the retrieval and processing of CCTV images are regulated by the Code. These activities must be undertaken using methods that align with the Code.

Activities set out in this APP comply with the NPCC **Framework for video based evidence**and reflect the requirements of the Code.

More advanced activities can only be conducted by specialist units or departments that have been accredited to ISO17025 by the United Kingdom Accreditation Service (UKAS).

Retrieval activities covered by this APP are supported by an e-learning package created by the College of Policing and NPCC, which is available on College Learn. Practitioners must have completed Level 1 training before undertaking any retrieval activity from a CCTV system.

Overview of training levels

Training level	Activity				
Level 0 First responder	CCTV acquisition from third-party/owner operator				
Level 1 Initial training	**For level 1 and level 2:** CCTV acquisition/ retrieval at scene or relevant venue trained by police/ staff, using a simple manufacturer's intended method or escalated to level 2, where further competency/skills are required		Investigative viewing of CCTV	Creation of stills for PACE Code D recognition only	
Level 2 Technical training			Conversion to viewable format using validated processes, where native format is still available	Basic compilation of footage using SAI approved DEMS/DAMS	
Level 3 Forensic specialist training under ISO-17020/5	Image analysis	Specialist CCTV retrieval (lab-based) using non-standard methods	Image correction and enhancement	Advanced editing and compiling of footage/ data	Data recovery (from non-working systems metadata analysis)

Note: DAMS = digital asset management systems; DEMS = digital evidence management systems; SAI = senior accountable individual.

Image adapted from **NPCC. (2022). Framework for video based evidence, version 3.1**

For further information on authorised processes, see:

- **Defence Science and Technology Laboratory (2020). Digital imaging and multimedia procedures (DIMP).**
- **Defence Science and Technology Laboratory (2022). Recovery and acquisition of video evidence (RAVE).**

Glossary of terms

Systems

Public or private surveillance installations comprising cameras, recorders and associated equipment for monitoring, recording, transmission and controlling purposes, for use in a defined zone. These systems come in many different forms. The technology involved is continually developing and changing.

CCTV (closed circuit television) or VSS (video surveillance systems)

Refers to wired and wireless CCTV systems where digital and network systems are no longer required. The term VSS is becoming more common.

CCTV recorder

The video or audio recording unit often known as a DVR or NVR.

DVR (digital video recorder)

A stand-alone embedded system or a computer-based system used to record video and/or audio data. Some DVRs allow for remote access through a web client or mobile application.

NVR (network video recorder)

A network-based surveillance video recording system, typically using internet protocol (IP) cameras and internet connectivity, that allows for remote access through a web client or mobile application.

Hard disc drive (HDD)

An HDD is a data storage device usually located internally within a CCTV recorder. Removal of an internal hard drive must not be attempted, as this is a specialist activity.

Resolution

This is the number of pixels displayed in an image. A higher resolution corresponds with a higher potential for fine detail and a larger file size. However, this is often dependent on how compressed the imagery is and the method of playback.

Frame rate

The frequency at which images are recorded. This can differ depending on the recording or storage medium, and may be variable. Frame rate can have an effect on quality. This is usually expressed as the number of images or frames per second – for example, 30fps.

Proprietary file format

Any file format that is unique to a specific manufacturer of the system.

Downloading, exporting or digital CCTV retrieval

The process of acquiring audio, video, still images and data from a DVR system.

Cloud-based storage

Typically, using IP cameras and internet connectivity that allows for remote access through a web client or mobile application. The storage of data will be via remote third-party data storage, often internationally.

Aspect ratio

The relationship of width to height of an image. This is critical for correct identification and must not be changed from its original, as this distorts the image content.

Analogue CCTV

Rarely encountered, except for in legacy cases.

Authentication

The process of ensuring that the data is an accurate representation of what it claims to be.

Managed systems

This is a network of cameras sited in public areas, usually managed by the local authority, shopping centres or larger organisations. CCTV from some managed systems may not always be stored on site. Contact with the system manager is advised.

Strategic management

Chief officers must demonstrate support for the use of CCTV by:

- appointing a designated senior accountable individual (SAI) to give oversight of activities around CCTV in line with the FSR Code
- ensuring that investigators are provided with appropriate and up-to-date training and refresher courses on retrieval and preparation of CCTV material from the numerous systems in use
- ensuring that basic, fit-for-purpose equipment and facilities are available to investigators for the timely viewing, copying or retrieval of CCTV material, including software that enables compatibility between the various CCTV systems
- establishing, implementing and overseeing policies to ensure that the use of CCTV in investigations achieves its full potential
- ensuring that they have a service level agreement in place with their local authority CCTV control rooms, to ensure that all parties understand relevant processes and procedures

Initial investigative actions

The first opportunity to gather and use CCTV material in an investigation will be during the initial investigative response. During this phase, the police will usually be able to identify the location of the offence, the time it took place and the identity or descriptions of victims, witnesses and suspects. These details will form the basis of a first trawl for CCTV material. In some cases,

investigators will have more to work with, such as descriptions and registration details of vehicles that are relevant to the offence, and the access and exit routes used by suspects.

System time verification

It is important to carry out and record system time checks before reviewing potential CCTV footage. For example, compare the time displayed by the CCTV system with that given by a reliable and accurate time source. Any difference must be recorded in your report and statement.

When the clocks change from Greenwich Mean Time (GMT) to British Summer Time (BST) in spring, then back in autumn, it is worth taking extra care when verifying the recorded time on a CCTV system. Not all systems will update automatically. If an incident happens between midnight and 2am during the autumn change – when the clocks go back an hour – the system may contain an additional hour of footage, reflecting the hour of the clock change.

Initial review of footage

Where possible, the investigator should review the CCTV material immediately, on site, to assess its quality and value to the investigation and whether it is necessary and proportionate to obtain the footage. Relevant footage should be obtained as soon as reasonably practicable.

When judging whether footage is relevant, investigators should consider the **Code of Practice to the Criminal Procedure and Investigations Act 1996 (CPIA)**, paragraph 2.1.4, and apply the relevancy test set out in the Code.

CCTV material that would pass the relevancy test includes images that:

- capture the suspect committing the alleged offence
- reveal that the wrong individual has been arrested for the alleged offence
- do not support the account given by the complainant and/or witnesses – for example, mistaken identification
- reveal the alleged complainant as the perpetrator (and supports a defence of self-defence)
- show that the parties are not captured on the video when, on the eyewitness evidence, they should be (and there is no suggestion of a technical fault and/or video overrun)

- reveal the demeanour of witnesses
- capture the immediate aftermath of the alleged offence
- reveal the actions of witnesses
- reveal the crime scene
- reveal potential witnesses

Although the amount of information available will vary, an intelligence-led CCTV trawl will usually provide additional lines of enquiry, even when only the approximate time and location of the incident are known.

Setting objectives

In many cases, the objectives for a CCTV strategy will be obvious. They will include locating images of the alleged incident in progress, identifying those involved and/or images of victims, witnesses or suspects going to – or leaving – the scene.

As the investigation develops, the objectives may be more complex and may include verifying the accounts given by individuals or testing hypotheses that have been developed.

As a minimum, investigators should aim to identify any CCTV material that shows the offence being committed. This should be done even where other material gathered appears to confirm a suspect's involvement. During the early phases of an investigation, all available material should be gathered, whether it points towards or away from a suspect. It is not possible to predict what material will be relevant as the investigation develops.

CCTV footage that does not directly show the offence may be just as relevant as footage that does.

Setting parameters

Having set the objectives for the CCTV trawl, the next step is to focus the search on specific times and locations relevant to the objectives.

Time parameters

In some cases, setting time parameters will be reasonably easy. Victims and witnesses were present during the incident – for example, an assault – and can estimate when the incident happened with some accuracy. Even when nobody is present, information – such as the time an

alarm system was activated, or when someone heard a window break – may provide a time around which parameters can be set.

In other cases, this is not as easy. For example, a theft from an unattended vehicle, or a burglary while the homeowners were away, means that victims may only be able to provide the time they left the vehicle or building, and the time they returned and discovered the offence. This may cover several hours or even days.

Time known

When the time of the incident is known, parameters should include a contingency period both before and after. This will provide a margin of error and should capture events leading up to, and following, the incident that may be relevant. The contingency period will vary depending on the incident, but it is advisable to keep it as short as possible. In most cases, 10 minutes either side of the reported time should be sufficient.

- Note – extra time may be required around the time when the clocks change in spring and autumn. See System time verification.

Setting wide parameters can slow down the CCTV recovery process and may require the seizure of CCTV units. Some venues may have support and warranty contracts with CCTV system suppliers and the removal of a CCTV recorder may invalidate these contracts. In these situations, the system supplier should be consulted to arrange download or removal of the system.

If nothing of value is identified within the set time parameters after an initial review of the footage, investigators may need to review all available intelligence and/or information and adjust the parameters accordingly.

Any changes to the parameters should be recorded in the CCTV strategy, along with detailed rationales and intelligence supporting any changes.

Scene visits by suspects

Some suspects visit the scene before an incident as a preparatory act – for example, planning entry and exit routes or assessing security. Some suspects return to the scene after an incident to see the consequences of their actions – for example, a person who has committed an arson attack.

These visits may have been caught on CCTV.

Time not known

In cases where the crime could have been committed at some point over a longer period of time, investigators should focus the parameters on times when the crime was most likely to have been committed based on intelligence and available information. Doing so will enable the time parameters to be set more precisely and will avoid parameters that cover the whole of the period, which may be several hours or days, and may involve viewing a large amount of material.

Case example

Following a theft from a vehicle in a public car park, intelligence indicates that this, and several other thefts from motor vehicles, could only have happened during a narrow timeframe. This is because an attendant was always present in the car park, except for when they went to the office for their lunch break. The suspects most likely committed the offences during the attendant's lunch break to avoid discovery.

Investigators need to balance the risk of missing relevant information by not viewing the whole of the CCTV material, against a proportionate response to a line of enquiry.

Investigators should not request footage if they do not have a reasonable expectation that it will be useful to the investigation. Unfocused or speculative trawls can lead to an enormous amount of data being obtained, which can be frustrating for system owners to provide and will require extended viewing times. It is always more efficient to undertake an initial review of footage to assess its value prior to obtaining it.

Locating CCTV

Once the time and location parameters have been set, places from where footage can be obtained should be identified. A wide variety of public and private systems may be available that cover locations within the location parameters. Investigators should also check to see if any cameras sited inside premises are focused on the doorway or window and may catch images of any activity outside.

Record keeping

Investigators should keep a record of all CCTV locations visited and whether any relevant footage could be obtained. This will avoid duplication if the investigation is passed to another investigator. It also enables any premises to be revisited later if access could not initially be obtained.

Prioritising trawls

If there are several areas where CCTV trawls are to be made, it is advisable to prioritise them so that the ones most likely to be productive are visited first.

Retrieving CCTV

When retrieving CCTV, investigators should consider the following.

- Previewing CCTV footage at the premises (or remotely if available), to assess its value to the investigation.
- Verification of the time and date on the CCTV system.
- How to establish the overwrite period to prioritise retrieval.
- How much footage will need to be retrieved.
- Where the data is stored (for example, locally to the system or internationally via cloud providers).
- Retrieving proprietary or native format. Every effort should be made to obtain the footage in proprietary or native format, rather than more standardised or familiar file formats that may be available. These are usually conversions of the original proprietary format and can result in loss in quality or information during the conversion process. Conversion also reduces the opportunity for further forensic analysis if needed. If you can’t play it straight away, it can be converted by your force using an approved Digital Evidence Management System (DEMS) solution or audio visual (AV) unit.
- Force protocols for confirming that the footage received is genuine. This will avoid later questions around authenticity.
- DVRs are fragile devices. If they need to be removed, they should be handled carefully and ideally be stored in appropriate shock resistant packaging. Ensure that any power supply (often specific to each system) and remote control (if present) are also recovered.
- Force protocols when the system owner refuses to allow officers to view, retrieve or remove CCTV footage or the system.
- When using a universal serial bus (USB) memory device to retrieve CCTV footage, these should either be force-issued new, reformatted or sanitised according to local force policy. Once the data

has been transferred to appropriate secure storage system and a master version has been created in accordance with the DIMP, the USB device should be re-sanitised prior to re-use.

Prioritising retrievals

Where investigators need to delay retrieval of footage, they should ensure that the system owner is made aware of their obligation to retain third-party material. They should also notify the system owner when the footage will be retrieved, being aware of overwrite times. Every effort must be made to collect the material as arranged or to let the system owner know if the material is no longer required.

- Note – recording CCTV images from the system screen using body-worn video or camera phones is poor practice and should be avoided. This will not capture the original data, which will result in a significant drop in image quality, compromising the value of the imagery and making further analysis difficult or impossible.

These methods should only be used as a last resort where all other options have been exhausted or where there is a present and immediate risk of harm.

Authorisation must be obtained from the senior investigating officer (SIO) with rationale recorded. A copy in the native format must be obtained as soon as possible.

Retrieving CCTV from vehicles

CCTV may be available from vehicles such as taxis, buses and trains. However, there may be multiple similar vehicles – for example, several black cabs or ‘number 10’ buses – passing through the area where an incident took place and within the relevant time parameters. Where possible, identify the vehicle registration mark (VRM) or other identifying features to avoid wide or untargeted searches without significant justification. Untargeted trawls will place unnecessary resource burdens on transport operators and may lead to reluctance to help future investigations.

To obtain footage from trains or railway property, contact British Transport Police (BTP) CCTV Enquiries, who will arrange for retrieval or relevant images.

Post-retrieval, continuity and integrity

Mastering footage

The master is a definitive copy of the data. It is documented, sealed and stored according to established procedures. It can be examined by a court if it is necessary to confirm the authenticity of the evidence being presented.

Retrieved CCTV data must be mastered before it is viewed or converted using approved methods set out in **DIMP**. The master must be retained in native format so that it can be analysed using forensic processes.

For further information, see: Home Office. (2021). **Digital imaging and multimedia procedure, version 3.0.**

Continuity statements

The person who retrieves CCTV footage from a system must complete a record confirming continuity and integrity of the material gathered. Compare the time displayed by the CCTV system with that given by a reliable and accurate time source. Any discrepancy should be recorded in the audit record and supporting statement.

The audit record should include:

- time verification
- time difference
- date and time of earliest recording
- recording continuous or motion activated (if known)
- number of cameras or number of working cameras
- timeframe downloaded from and to
- make and model of DVR
- player included (if known)
- whether CCTV has audio (if known)
- download media used (USB or optical disc)
- exhibit number
- tamper evident bag seal number

Viewing CCTV

CCTV footage should be viewed as soon as possible to confirm that the correct footage has been retrieved and whether it contains relevant information.

Summarise what can be seen in the footage and pass this to the officer in charge (OIC) as soon as possible. This will help to identify relevant lines of enquiry and support investigative progress.

- Note – when footage is searched in the fast forward mode, individual frames or pictures will be skipped.

Layout plans

It is useful to draw up plans of the area showing the coverage of each CCTV camera. These plans can help viewers to change cameras and follow an individual. They are especially helpful where suspects, victims and witnesses move around large areas and are critical to major counter terrorism (CT) incidents.

Viewing areas

Viewing CCTV images can be demanding and affect health and welfare, especially where there are distressing or large amounts of footage that need to be analysed.

Viewing areas should:

- be secure
- be compliant with display screen equipment assessments
- have limited distractions

It is difficult to maintain concentration for long periods of time when viewing CCTV footage. Viewers should be supported by local force policy to take regular breaks from the viewing area and computer screen. Defence lawyers may question concentration levels when extended periods of viewing have taken place without appropriate breaks.

Viewing logs

A record of viewing should always be completed when viewing CCTV. This should contain, but not limited to, the following:

- exhibit details
- reason for viewing
- camera numbers and locations
- time and date checks
- persons and objects observed
- actions and events observed
- viewer details and viewing location
- time and duration of viewing (including breaks)
- any reference material (for example, reference images that were used by viewers to remind them what to look for)

Supervisors should quality assure the work of viewers – for example, spot checking viewed footage and logs.

Defence solicitors can apply to view unused and unviewed footage. If all relevant CCTV images have been viewed and viewing logs completed, this reduces the risk that relevant footage will be found by the defence in unused and unviewed material.

Further lines of enquiry

Viewing CCTV may generate additional lines of enquiry – for example, discarded cigarettes or discarded property may provide forensic opportunities. Images may identify clothing worn or weapons used, which can be recovered for examination.

By tracking the movements of offenders and witnesses to and from the scene through different CCTV systems, it may provide better-quality images that make it easier to identify the individual, associates, distinctive clothing or locations of interest.

Declarations of compliance and non-compliance

Anyone undertaking forensic science activities is considered to be a practitioner and is therefore subject to the FRS Code. This includes police officers and staff retrieving, analysing or processing CCTV footage from systems.

A practitioner is required under paragraph 37.2 of the Code to make a declaration of compliance or non-compliance in a statement or report for all FSAs referenced used in the retrieval, analysis or

processing of the footage.

After CCTV footage has been located, retrieved, analysed and processed, it can be presented to the court. Where forces have used forensic processes, they should comply with local standard operating procedures (SOP). This supports:

- compliance with the NPCC Framework for video-based evidence.
- a declaration of compliance against the framework set out in the FSR Code

Disclosure

All footage retrieved is subject to standard evidential processes. If an image is required by the criminal justice system (CJS), it should be viewable and accompanied by a full audit trail.

See **Disclosure**.

Trial preparation

Early liaison with the Crown Prosecution Service (CPS) and court is recommended to identify the best format for presentation of footage in court and any equipment required. Allow as much time as possible to prepare.

Court presentation

The purpose of the presentation is to help the jury understand the evidence. Investigators should aim for clarity and simplicity.

For volume crime offences, an elaborate presentation of the CCTV footage may not be required. In more complex cases, where there may be a large volume of data from multiple cameras, it may be necessary to provide a more detailed forensic court presentation with, for example, a compilation of graphs, charts, maps, stills and video clips. Working closely with the CPS and defence teams will ensure that whatever format is used, it will meet the needs of the legal representatives and the court equipment available.

If a more detailed presentation is required, early liaison with the local force video forensics team is advised. If external support is required the National Crime Agency (NCA) **Major Crime Investigative Support** can provide help and advice to select suitable practitioner support.

Feedback

If a CCTV system owner has provided footage to the police and it has been considered as part of an investigation, feedback should be provided to the owner on the outcome of the investigation. This may be a local authority, a business or a private individual.

Feedback can help to develop good working relationships with communities and can encourage CCTV owners to volunteer their footage if there is a need in the future.

Feedback can be formal or informal, such as a quick telephone conversation. The national CCTV strategy recommends that formal feedback is provided when a local authority has offered CCTV footage. This supports ongoing funding of local authority control rooms. Local authorities may provide their own feedback forms to complete. Alternatively, an example of a formal local authority feedback form is available via the **National Police Library**.

CCTV retention and disposal

Following an investigation, CCTV material may be retained but can only be used or disclosed for the same policing purposes for which it was gathered.

For further information see:

- Association of Chief Police Officers and National Policing Improvement Agency. (2007). **Practice advice on police use of digital images**.
- College of Policing. (2023). **Police information and records management Code of Practice**.
- Home Office. (2017). **PACE Code D 2017**.
- Ministry of Justice. (2015). **Criminal Procedure and Investigations Act 1996, Code of Practice**, section 5a ('Retention of material').

For decisions relating to the retention of footage, refer to:

- College of Policing. (2013). **Review, retention and disposal.**
- NPCC. (2021). **Retention, storage and destruction of materials and records relating to forensic examination**.

Tags

APP Investigation CCTV