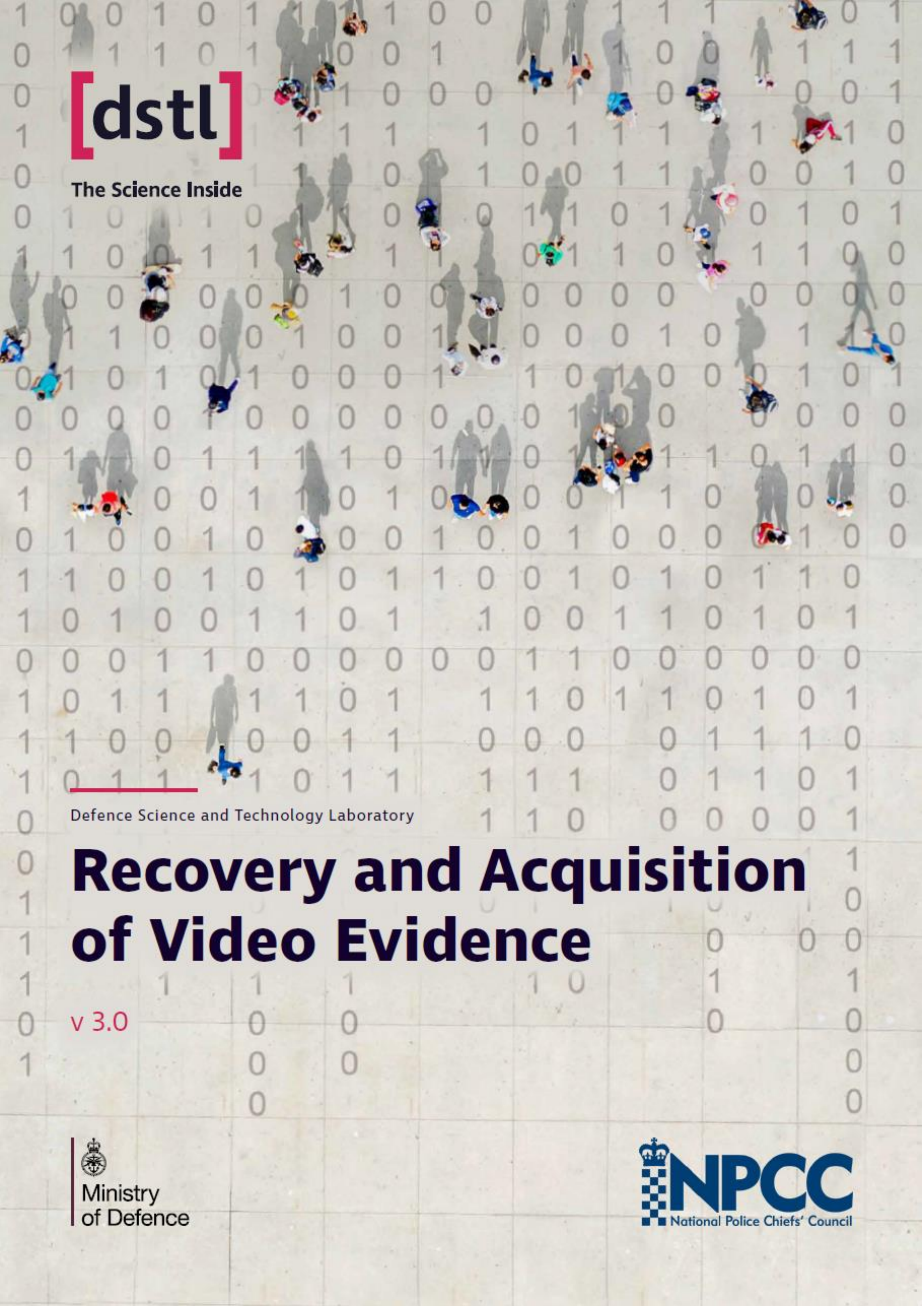

[dstl]

The Science Inside

Defence Science and Technology Laboratory

# Recovery and Acquisition of Video Evidence

v 3.0

Ministry of Defence

NPCC National Police Chiefs' Council

# Recovery and Acquisition of Video Evidence

Cohen, N, MacLennan-Brown, K

DSTL/PUB134170 3.0
28 February 2022

**Dstl**
**Counter Terrorism**
**and Security**
Porton Down
Salisbury
Wilts
SP4 0JQ

## Foreword

CCTV is commonplace in our society and has proved to be an invaluable tool in the investigation of crime ranging from petty theft to terrorism. However, the proliferation of different CCTV systems, together with the transition from static to cloud based systems has required a change in practices for the recovery and processing of video evidence. This is particularly evident in the increased level of technical knowledge required for retrieval of video evidence from the diverse range of CCTV systems in use.

It is therefore vital that the police have clear procedures and guidance to follow when retrieving video and processing images from digital CCTV systems, and maintain the integrity of the evidence.

We are confident that this procedure provides a sound framework within which to effectively gather and present evidence from CCTV systems.

Jenny Gilmer
ACC South Wales Police
Chair NPCC CCTV Working Group

# Contents

## List of figures

## Management Summary

This procedure and supporting guidance is issued to assist forces in formulating local policies and procedures for retrieving native video and audio from any CCTV system, and applies to all those who may need to retrieve CCTV footage. It assists in identifying the most appropriate method and contains information on the suggested levels of training and experience appropriate to the various techniques. It also provides guidance on the naming of exhibits in non-native file formats, where this is necessary to facilitate further processing or replay in court.

Primarily the document covers methods for the retrieval of video in its native file format from CCTV systems, leading to the creation of a Master exhibit of the evidence. It presents a checklist of actions that should be followed when retrieving data to ensure that all relevant information is captured and evidential integrity is maintained. It also contains a flowchart to help the user select the most appropriate retrieval method to use for any given CCTV system. Explanatory notes are provided for each option and guidance given for assessing the practicality and suitability of each technique.

This edition of the document follows on from Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0. It has been updated to take account of the revised guidance on capture and handling of digital images for police applications given in the publication *Digital Imaging & Multimedia Procedure v3.0* and Authorised Professional Practice*.* This document should be read in conjunction with other relevant publications as referenced in the text.

# 1 Introduction

CCTV installations vary greatly in terms of the recording methods and formats used as well as the picture export facilities provided. There are many manufacturers operating in the CCTV marketplace and each offers a slightly different solution with different capabilities and functionality. This makes the task of retrieving and replaying data increasingly complex, requiring the need to develop a familiarity with a broad range of systems, export technologies and retrieval software. It is essential that the selected method allows evidential integrity to be maintained so that maximum picture information is retained.

This publication is designed to:

- Assist compliance with the Forensic Science Regulator’s requirements for forensic science activities to be performed using approved processes and conducted by competent staff where accreditation to ISO 17025 is not mandated.

- Assist those designated to produce and/or approve processes based upon current practices in the selection of methods for effective retrieval and subsequent processing of CCTV and its associated data.

- Assist those authorising police staff to retrieve data by setting out the expected training and competence for the levels of activity expected.

- Assist decision making in outsourcing forensic science activities which fall outside of force capabilities.

# 2 Key Requirements

## 2.1 Authorised personnel

This document defines a set of activity levels, which grade the relative complexity of each retrieval method, and the appropriate training for each, and shows how these in turn relate to the Forensic Science Regulator's accreditation requirements (see section 3.5 for the activity levels definition). Forces or organisations wishing to adopt the activity levels model detailed in this document, and in particular use those levels that fall outside the ISO 17025 accreditation requirement, need to define how they authorise and re-authorise staff as competent to conduct the activity (i.e. as an alternative to the activity being ISO 17025 accredited). Those who are authorised through this process are deemed authorised personnel.

## 2.2 Approved processes

In house specific processes and procedures must follow the guidance given in this document, and should be overseen by competent practitioners from the force's forensic video unit. Accountability should to a specific senior member of the force or organisation.

## 2.3 Master and Working Copy

The Master is the definitive copy of the data, that is documented, sealed and stored according to established procedures and can be examined by a court if required, to confirm the authenticity of the evidence relied on in proceedings. The Master may be stored as a physical item or purely in digital form (for instance on a Digital Asset Management System (DAMS); and more law enforcement specific Digital Evidence Management System (DEMS)). The Master must be retrieved, wherever possible, in the native format of the device that created it. Further information can be found in the *Digital Imaging & Multimedia Procedure v3.0*.

The Forensic Science Regulator's document Video Analysis FSR-C-119 Issue 2[1] gives the following guidance on Master and Working Copies:

- A Master exhibit of the source/original data shall be preserved, the forensic unit should define in their procedures what constitutes a Master.

- Working copies of the video footage may be produced and these will typically be either:
  - A bit for bit copy of the Master in its native format, suitable for further analysis by specialists instructed by either the prosecution or the defence;
  - A bit for bit copy of the Master in its native format, supplied with a player suitable for investigating officers to view the footage; or
  - A "playable" format suitable for investigating officers to view the footage and potentially for supplying to the Crown Prosecution Service (CPS)

[1] At the time of publication of this retrieval document, details are in FSR-C-119 Issue 2. This will, however, be subsumed into the FSR Code of Practice. Updates to requirements will be published at Forensic Science Regulator - GOV.UK (www.gov.uk).

marking this as “Converted Format” and therefore no longer a true copy of the original.

- Any media produced whereby original data has been converted to a different format should be clearly marked as “Converted Format”, or identifiable as such in some other way defined in the procedure. Where applicable, quality limitations should be noted.

This is illustrated in Figure 1 below.

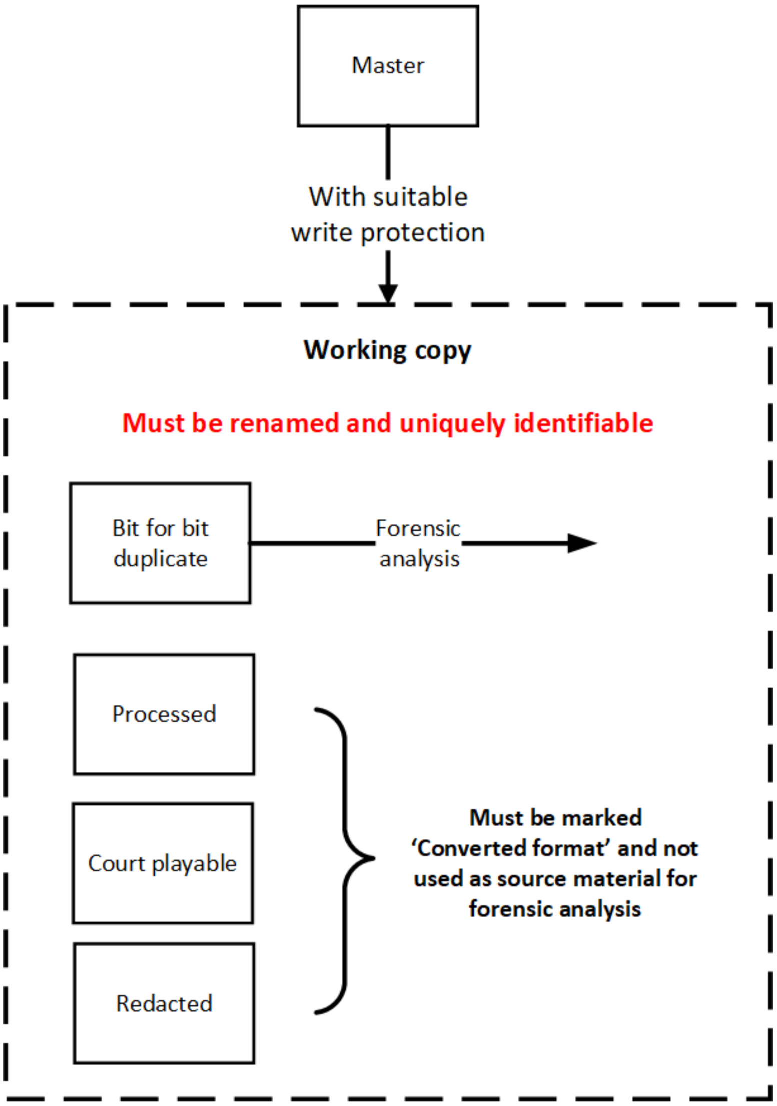
Master
With suitable write protection
Working copy
Must be renamed and uniquely identifiable
Bit for bit duplicate
Forensic analysis
Processed
Court playable
Redacted
Must be marked ‘Converted format’ and not used as source material for forensic analysis

Figure 1: Master and Working Copies

The purpose of the Working Copy is to provide a consistent start point for other processes without endangering the integrity of the Master. A Working Copy can take several forms. A bit-for-bit copy should be used as a starting point where forensic analysis is required. Non-native copies of the data may not contain the information required for forensic analysis. Working copies must be uniquely identifiable and may need associated audit trails.

Best image quality is provided by the native file format. This format, however, may need proprietary software or hardware for replay and this may not provide the required functionality to enable editing or processing to be undertaken. If this is the case a format conversion will be required.

Any copy of the Master must be renamed and have an audit trail associated with it that clearly shows what processing has been carried out. If that copy is not bit-for-bit the likely impact of that processing must also be recorded. At the very least it should clearly state that it has potentially reduced quality.

When making a copy that is not bit-for-bit then the following three things must be considered:

- Will the resultant drop in quality still yield a usable image?
- Will any associated metadata be retained?
- Will any associated audio be retained?

Care must be taken that the version of the file being worked on, or supplied to a third party for processing is actually what it purports to be. Some DEMs and DAMs systems will automatically process a file either on ingest or download in a process invisible to the operator.

## 2.4 Transfer Medium

This refers to any medium employed in an intermediate stage between the originating system and the Master. If this transfer medium is physical WORM media then it may be destroyed once the Master has been secured. If it is reusable media such as flash memory then it should be suitably sanitised using a force approved method, after the Master has been secured. Reusable media should be accessed via a write blocker wherever possible.

## 2.5 Further Processing or Analysis

Before deciding on the suitability of a particular CCTV clip for further processing and analysis it is important to ensure that the best quality data available is being used and that it is being viewed under appropriate conditions. This means that:

- The data is in native format if at all possible,
- The monitor is
  - of a sufficient size to see the required detail clearly
  - set to the correct aspect ratio
  - high enough resolution and bit depth to display the data correctly

- The device powering the monitor has sufficient processing power to display the imagery correctly

- The viewing environment is suitable, free from distractions and with no strong or coloured lighting.

# 3 Retrieval and Preservation of Video Evidence

## 3.1 Introduction

This procedure is designed to enable authorised CCTV officers, technical staff and specialists to select the most appropriate method for retrieving recorded video data from a digital CCTV system. It is intended to facilitate extraction of video data (and associated metadata, e.g. time and date) from digital media recording equipment, rather than to forensically examine the entire system. There are key differences between most CCTV retrievals and conventional computer forensic investigations; i.e. it is often the case with CCTV that the owner/operator of the system is not a suspect but a witness.

Forensic computer investigators are advised to refer to the relevant NPCC guidance for computer based evidence, as the processes involved in CCTV data retrieval and processing differ considerably from those used within computer forensics.

Having identified the CCTV required or received a request for assistance, this requirement must be assessed against the functionality provided by the CCTV system. The selection process is based around a flow chart (see section 3.5), which seeks to address four fundamental questions:

1. Is the request reasonable?

2. What native export methods are available that retain the original quality and metadata?

3. Is the method practical and achievable via a non-destructive process?

4. Does the method lead to the creation of an evidential Master copy?

The person tasked with obtaining the CCTV must ensure that the method selected fits within their training and competence or escalate the request to a more suitable person. The training and competence levels are described in section 4.

Priority is given to techniques that permit video data to be extracted in the native file format and that satisfy the requirements for Master copies detailed in the Digital Imaging and Multimedia Procedure v3.0 and the FSR's publications[2]. The preference for extraction of data in the native file format is to maintain evidential integrity and retain picture quality, thus ensuring further processing and analysis can be carried out, for example facial recognition, and forensic processes such as facial identification and speed analysis.

Methods such as recording the screen using Body Worn Video devices or camera phones are poor practice as they do not capture the original data. This will result in a significant drop in image quality, compromising the value of the imagery and making

[2] At the time of publication of this retrieval document, details are in the Codes of Practice and Conduct and FSR-C-119 Issue 2. Updates to requirements will be published at Forensic Science Regulator - GOV.UK (www.gov.uk).

further analysis difficult or impossible. These methods are only to be used as a last resort where all other options have been exhausted or where there is a present and immediate risk of harm to person. Authorisation must be obtained from the SIO and documented, and a copy in the native format must then be obtained, with a request made to the forensic video unit.

## 3.2 Integrity Verification vs Authentication

These two terms are frequently confused and often misused, the following definitions were taken from SWGDE publication Digital and Multimedia Evidence Glossary Version 3.0 June 2016

- Integrity verification is the process of confirming that the data (image, CCTV clip, etc.) presented is complete and unaltered since time of acquisition. Relevant questions concerning integrity might include: "Has data been added to, or removed from the file?"; "Has the data within the file been changed?"

- Authentication however, is the process of substantiating that the data is an accurate representation of what it purports to be. Relevant questions concerning authentication would deal with issues such as: "Was the image taken at the time stated?"; "Was the image taken at the place stated?"

It should be noted that standard image processing techniques such as lightness or contrast changes would affect the image integrity but not the image authenticity; however, an inaccuracy in the clock on a CCTV system could affect the image authenticity but not affect the image integrity. Robust audit trails are required in order to assure image authenticity. Various techniques such as generating and comparing MD5# values before and after data transfers are a good way of ensuring data integrity.

## 3.3 Download Checklist

The list of actions below should be followed when retrieving video data to ensure that all relevant video and information about the system is gathered. This is essential to permit future viewing and maintain evidential integrity, whilst minimising any potential disruption to the premises where the CCTV system is installed.

This checklist should be read in conjunction with the CPIA Code of Practice and Joint Protocol between the Police Service and the Crown Prosecution Service (CPS) on dealing with third party material, which provide further information on authority to receive material.

Shortened versions of the following checklist that are training level specific are included as an aide memoir in Section 4.

(a) **Time check** – initially compare the time displayed by the CCTV system with that given by a reliable, accurate time source. Any discrepancy between the system time and real time should be recorded in the audit trail and compensated for when conducting the retrieval. This is critical where several instances of footage from separate systems will need to be compared or synchronised. Also this will ensure that the correct section of data is copied. Additional caution should be shown when dealing with networked and IP based systems as these may reference more than one time clock.

(b) **Contemporaneous notes** should be kept, detailing the course of action taken, to provide an audit trail. Take photographs of the system if possible, particularly if the recorder is unfamiliar or the manufacturer uncertain.

The audit trail should include such details as:

- System Details;
    - Time check
    - Make and model of the CCTV system
    - Number of cameras – both recording and relevant
    - Any audio sources
    - Is it recording
    - Time period available on the DVR e.g. first recording
- **Basic system settings** (e.g. current record settings and display settings), so that if changes have to be made to facilitate the retrieval, it is then possible to return the system to its original state. Taking photographs of the system can assist, particularly if cable connections are changed during retrieval.

(c) **Determine time period** required in conjunction with OIC, if this has not already been specified in the request. When specifying time periods, due reference must be made to the proportionality guidance outlined in The Information Management APP incorporating MoPI (The Management of Police Information).

(d) **Check storage / overwrite time** – to determine how long the relevant data will be retained on the system. Generally the most accurate way of determining this is to check the earliest accessible data on the system. This is particularly important if the retrieval cannot be carried out immediately, or needs to be prioritised against other tasks. A maximum time period can then be estimated within which the retrieval must be carried out before data is lost.

(e) **Determine which camera views are required**, and whether they can be retrieved separately. It is good practice to draw a plan of the camera views to facilitate further decision making processes. Depending on the nature of the incident, there might, for example, be a requirement to retrieve all cameras with external views. Some systems permit video from individual cameras to be downloaded, but some do not, in which case data from all cameras will need to be taken.

Be aware of the possibility of hidden or covert cameras that may be apparent if a different set of access credentials are used. It may be possible to check that the number of camera feeds displayed matches the number of camera cables attached if there is some doubt over this. This is not always possible with IP based systems and there may also be independent cameras associated with the system that have standalone storage. The decisions taken and the reasons for them should be documented in the audit trail. In some circumstances it may be advisable to obtain a plan or map of the camera views within a scene or associated area, if possible.

(f) **Obtain system password**, if necessary. Be aware that the standard user password may provide only limited functionality and an administrator password may be necessary in order to enable data retrieval. Record the login credentials used as different login levels may show different cameras.

(g) **Replay Data**. Check that the requested video exists on the system.

(h) **The recording should not be stopped during the retrieval process** unless:

1. This is an unavoidable feature of the system or

2. There is an immediate risk that important data will be overwritten before it can be retrieved.

(k) **Protect data**. Some systems allow write-protecting a selected video sequence to prevent it from being overwritten before it can be retrieved; however, it should not be assumed that this facility will be present.

(l) **Confirm that the data can be retrieved in its native file format**. It is strongly recommended that the CCTV sequence is extracted in its native file format in order to maintain image quality, even where this file format is proprietary to the CCTV manufacturer. Non-native format downloads may cause the loss of metadata such as time and date information, along with any stored bookmarks. (Note that when copying data files manually via Windows File Explorer, the metadata and index files may be stored in a separate directory to the video files and the file structure may need to be maintained in order to facilitate replay.) This is particularly important with systems that are accessed remotely.

(m) **Replay software**. Is the data format proprietary? If so, it is necessary to retrieve a copy of the correct version of replay software alongside the data. Some CCTV systems provide this facility, but others do not, and the software has to be obtained separately, e.g. from the manufacturer’s website. It should be established that the facility exists to replay the data before leaving the scene and allowing the system recording to be overwritten.

(n) **Confirm success of retrieval**. The retrieved data should be checked before leaving the scene (or as soon as possible afterwards) to confirm that (i) the retrieval process was successful, including associated metadata and audio if present, and (ii) that any associated replay software functions correctly. This check should be done on a machine other than the original recorder to ensure that replay is not device specific.

(o) **Restore the system to the owner**. Ensure that video is being recorded onto the system as well as being displayed as a live view. Confirm in the presence of the owner/operator that it is operating as it was originally and obtain a signature. This step may not be necessary with cloud stored video.

(p) **Complete evidence sheet**. The following information should be included with the evidence to assist the investigator with subsequent replay and analysis:

- Discrepancy in display time and date
- Time period covered by download
- Earliest recorded data
- Map of camera locations and coverage
- Include replay software if available
- Make and model (important when trying to identify suitable replay software or hardware)
- Transfer media used.

(q) **Media handling**. Physical media should be packaged to minimise the likelihood of damage or loss in transit, especially small devices such as USB sticks or other flash media. If USB flash drives are used as transfer media they must be individually identifiable and noted in the audit trail. CDs and DVDs should be kept in individual hard cases rather than on a spindle, flash cards should be stored in their original protective packaging and, particularly during forensic examination, care should be taken to protect hard drives if removed from systems. These should preferably be stored in individual boxes with protective inserts and in anti-static bags. All evidence should be bagged and labelled according to established procedures, and the label on the box should contain sufficient information to link it to the evidence sheet that contains the full details. Also, if there are multiple discs, the labels should identify the correct order for replay.

(r) **Loss of Media**. Note separately what data is on each item of evidence as part of the audit trail. Any loss of an exhibit in transit or at any point prior to its official destruction must be reported to your information security department. Any loss of media containing personal data will further need to be reported to the Information Commissioner’s Office.

### 3.4 Equipment

A range of equipment will be needed to enable technical recovery staff who are undertaking on-site retrieval to be able to deal with the variety of systems that are likely to be encountered. The following is a suggested list of equipment that should permit the most common systems to be dealt with and retrieval methods to be undertaken:

- Appropriate forms for documenting the audit trail
- Blank media, e.g. CD-R, DVD-R, DVD+R

- USB flash memory in a variety of capacities and from different manufacturers and formats, these must be uniquely identifiable. Refer to your in house specialist audio visual team for advice.
- USB hard drives (capacity 500GB+)
- USB mouse
- Laptop with network connectivity (to permit network downloading), and USB ports (to enable downloaded data and playback software to be checked).
- USB write blocker
- Memory card reader
- USB optical disc reader
- 4 port USB hub
- Network cables (crossover and patch)
- Network switch
- Toolkit (plus mains tester, torch, inspection mirror, pens and labels for cable marking)
- Extension cables (e.g. 4-way power distribution cables)
- Camera – to record cabling, connections and settings before disconnecting system
- Analogue/digital video monitor
- Replacement (loan) DVR units. Caution should be applied to this approach as several incompatible technologies exist.

Level one staff would only require the relevant documentation forms and suitable capacity storage media from the above list.

### 3.5 Selecting Method for Video Retrieval from CCTV Systems

The chart presents the various options available for retrieving data in its native file format. Explanatory notes are provided for each option and guidance given for assessing the practicality and suitability of each technique.

Most of the techniques described should be undertaken by a competent and experienced user of computers and/or DVRs who has received appropriate training. This training and experience can be split into four levels as outlined below:

- Level zero – basic acquisition – receipt from the owner. This level is covered by online awareness training provided by the College of Policing, or as mandated by force policy.
- Level one – allows operation of a functioning device in situ, using manufacturer's documented standard procedures, and requires force approved training and competency checks based on the information within this document.
- Level two – as level one but using more involved techniques and more in depth training. It is likely that at least the majority of equipment listed in Section 3.4 would be required. Requires a higher level of training based on the information within this document.
- Level three – specialist methods that require accreditation to ISO 17025. This includes non-standard download techniques and any of the above processes not carried out on a working machine in situ.

Level zero is not a forensic science activity, however, all other levels are considered technical activities and require adherence to the Forensic Science Regulator's requirements. A force may issue procedures based upon this guidance along with appropriate training and competency checks. As long as these are formulated and overseen by the force's own accredited specialist capability, level one and two may be conducted outside of ISO accreditation.

A full definition of the levels is given in NPCC Framework for Video Based Evidence (to be published), but in essence levels one and two cover operation of a working machine in situ using the manufacturer's intended and documented methods, the split into two levels being a recognition that some installations are more complex than others. Level three is anything not covered by levels one and two and any process including those outlined in levels one and two that are carried out on a machine that has been removed from its installation.

Forces or organisations may choose to include level two in their ISO 17025 accreditation. If this is not the case, forces must take care that work requiring ISO 17025 accreditation is not carried out by non-accredited staff. In any instance the force or organisation must have a suitably competent person who has responsibility and accountability for any processes or procedures agreed.

Each retrieval method has been allocated an appropriate activity level to indicate the competence required, however, any post recovery processing and reporting may require additional competencies and force policies should reflect this.

Each technique results in the production of a Master exhibit, although some processes may require the use of a transfer medium to create a permanent Master. This use of a transport medium is perfectly acceptable, but the weight a court will place on the evidence will be determined by how it has been handled. As long as each transfer is bit-for-bit then the image quality and integrity is retained. It is therefore essential that continuity of evidence is maintained and documented.

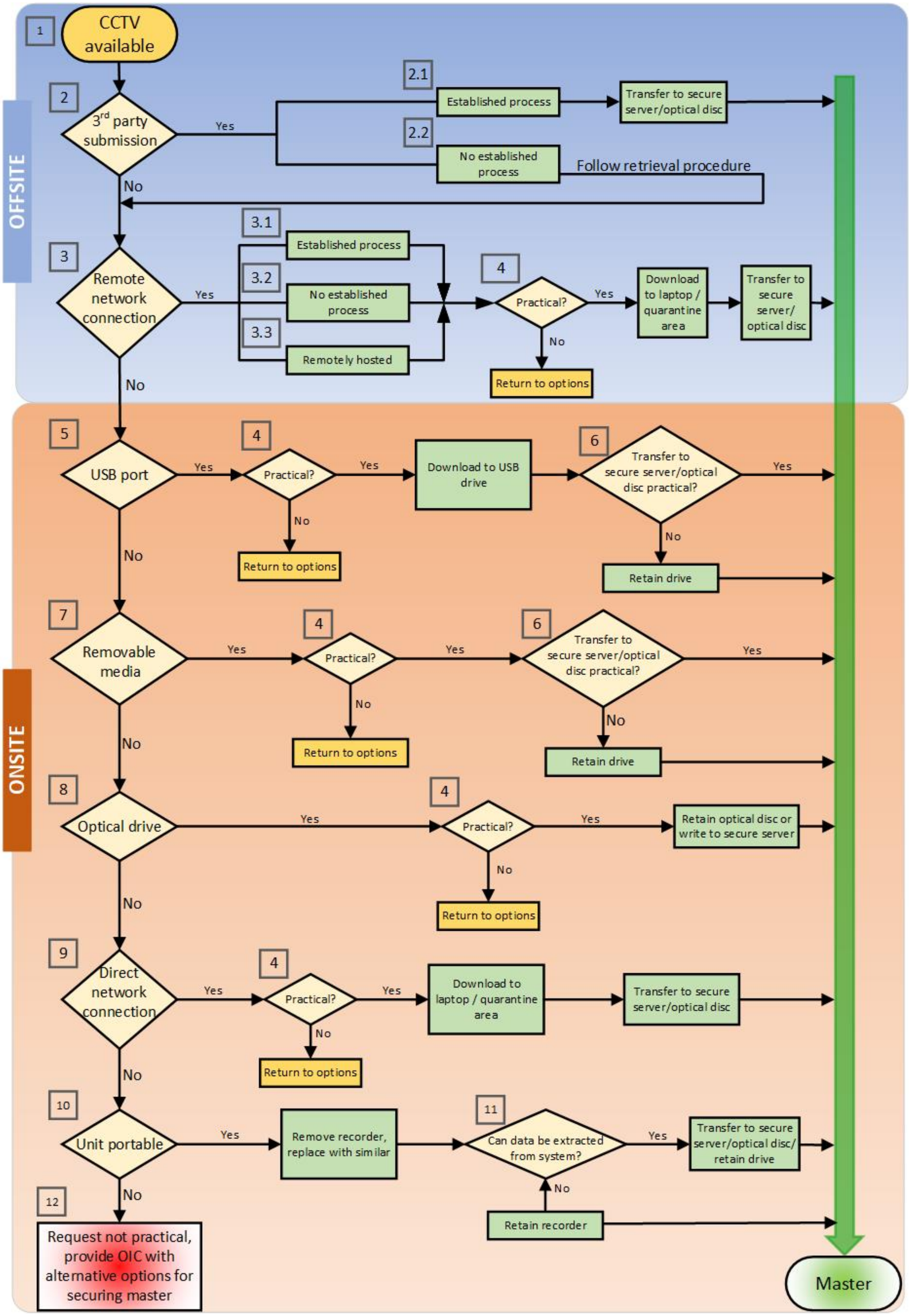
OFFSITE
ONSITE
1
CCTV available
2
3rd party submission
Yes
2.1
Established process
Transfer to secure server/optical disc
2.2
No established process
Follow retrieval procedure
No
3
Remote network connection
Yes
3.1
Established process
3.2
No established process
3.3
Remotely hosted
4
Practical?
Yes
Download to laptop / quarantine area
Transfer to secure server/ optical disc
No
Return to options
No
5
USB port
Yes
4
Practical?
Yes
Download to USB drive
6
Transfer to secure server/optical disc practical?
Yes
No
Return to options
No
Retain drive
No
7
Removable media
Yes
4
Practical?
Yes
6
Transfer to secure server/optical disc practical?
Yes
No
Return to options
No
Retain drive
No
8
Optical drive
Yes
4
Practical?
Yes
Retain optical disc or write to secure server
No
Return to options
No
9
Direct network connection
Yes
4
Practical?
Yes
Download to laptop / quarantine area
Transfer to secure server/optical disc
No
Return to options
No
10
Unit portable
Yes
Remove recorder, replace with similar
11
Can data be extracted from system?
Yes
Transfer to secure server/optical disc/ retain drive
No
Retain recorder
No
12
Request not practical, provide OIC with alternative options for securing master
Master

Figure 2: Retrieval flowchart

In the following sections the Master Copy of the retrieved CCTV can be in a variety of formats, though most often this will be secure server or optical media. The term secure server is used in this context to cover a variety of network options that include: cloud based systems; Digital Asset Management System (DAMS); and more law enforcement specific Digital Evidence Management System (DEMS). These systems must be approved by force IT, and are described in the Digital Imaging and Multimedia Procedure V3.0.

The following sections are numbered to correspond with the references in Figure 2 above.

### [1] CCTV available

An initial assessment should be made to determine whether the request for CCTV seems reasonable, i.e. is the request proportional to the nature of the incident being investigated. If a general request has been submitted for all available video from a site, or relating to an incident, then an attempt should be made to narrow down the period and area of interest.

The OIC should be aware of the time and resource implications around processing and viewing large volumes of data, e.g. 24hrs from a 48 camera system may result in 230 days of officer viewing time.

It should also be confirmed that all routes for obtaining the data have already been explored before requesting technical support, i.e. has the owner been asked to undertake the download, or is help available from the installer or manufacturer of the CCTV system? Downloads should only be undertaken by a suitably trained and competent person.

### [2] Third party submission

CCTV may on occasion be provided proactively by the public, as well as in response to a direct request. For example, it may be offered by a witness to an incident in a public place, or in response to a more general appeal following a major incident, road safety campaign, an initiative to curb vandalism or similar.

The material may be made available either via the handing in of media or devices at a police station, digital link to the file e.g. on a domestic CCTV system, email, or by electronic upload to a portal site.

Where there is an established process for obtaining the material, for example an upload portal, or force SOP, this should be followed (2.1). This would be a level zero activity. Where there is no established process for obtaining the material, then the retrieval procedure and flowchart are applicable, with the level of this retrieval being determined by the retrieval route selected (2.2).

It is important to note that for both routes, or if provided directly by email, USB etc. the final step of creating a Master on permanent storage must be completed. Seek assistance from the forensic video unit if required. This storage may be a secure server or physical media.

Extraction of video or photographic evidence directly from a mobile phone is a specialist area and should only be undertaken by a suitably trained and competent person.

The provenance of third party data should be checked to ensure authenticity where possible. Direct uploads in native format from a recording device are unlikely to have been tampered with, but anonymously supplied data in non-native format may not be as reliable.

When accepting third party supplied media, suitable virus/malware protection should also be in place along with physical protection against devices that have been designed to electronically damage a system, such as ‘USB killers’.

Audit trails begin at the point at which the media is uploaded or handed in i.e. at the point that it comes under police control. It would be unreasonable to expect the general public to have a high level of technical expertise in terms of file formats and quality settings, however, it may be possible to request a further, or technician assisted, capture of the data if it is particularly pertinent.

## [3] Remote network connection

Some systems may provide a remote network connection for off-site monitoring or data download. Before using this facility the network speed should be checked and it should be confirmed that the transmitted video is of the same quality as that which is stored locally. It may be advisable to have a quarantine area established for downloaded data to allow for suitable virus and malware checks to be carried out. Remote systems broadly fall into three categories in terms of the processes for retrieving the data. It is important to note that for all of these categories the final step of creating a Master on permanent storage must be completed. Seek assistance from the forensic video unit if required. This storage may be a secure server or physical media.

### *[3.1] Established process*

Large corporate systems such as those run by local authorities, transport operators and retail parks may provide direct remote access to police to retrieve data, via established processes and agreements. In these situations it is vital to ensure that the quality and format of the CCTV data accessed is of the same as that which is stored locally. Direct access to the data may be required should issues arise with the network accessed product.

If the retrieval activity is simply a request for a specific time/date/camera that is actioned by the system owner/operator then this is a level zero activity. If there is a need to directly operate the system via an interface to facilitate the download then it is level one.

### *[3.2] No established process*

For smaller systems and one-off investigations there will be no existing access agreements and facilities in place. However, the system owner may provide remote download access to the police on a case-by-case basis, and it may be preferable to use this route rather than undertaking an on-site retrieval. The caveats given above surrounding quality and format apply equally in this scenario. If this approach is used suitable measures need to be in place to address issues relating to data protection and related legislation. Care should also be taken not to leave an ‘open’ download route at the end of the retrieval as this may constitute directed surveillance and fall within RIPA legislation. Direct access to the data via site attendance may be required should issues arise with the network accessed product.

This is a level one or two activity depending on the complexity of the system.

### *[3.3] Remotely hosted*

Increasingly, devices are being marketed that have no local storage. In these instances there is no data held on the device and it is remotely stored by the supplying company with no at-scene access to the data. All the protections and safeguards given above apply in this scenario as well. However, if issues arise with the network accessed product, there’s no option for direct access.

If the retrieval activity is simply a request for a specific time/date/camera that is actioned by the system owner/operator then this is a level zero activity. If there is a need to directly operate the system via an interface to facilitate the download then it is level one.

## [4] Download method practical?

The practicality of a particular export method is determined by the resource (e.g. staff hours or training level), cost (e.g. media/hardware), time (e.g. data transfer time), and quality implications for the volume of data to be retrieved. Before an export method is chosen it should be assessed against each of the criteria to determine whether it is appropriate. For example:

- An internal CD writer may be present, but long sequences of video from multiple cameras may require an impractically large number of CDs for storage. The download process may also take several hours to complete. Archiving to a USB hard drive or via a network connection may be a more practical option as it would require less time and resources.
- It may be more time-efficient to remove the DVR and undertake the download in the laboratory using specialist software, although this may be more expensive in staffing and replacement hardware/media costs.
- It may well be that the availability of CCTV from remotely hosted systems is constrained by the level of subscription, and the quality and quantity of exported product is constrained by factors outside the control of operators.

To assess whether a particular download method is practical and time-efficient, the time taken to download five minutes of data should be ascertained, and the proportion of the required data that this represents noted. From this information, the total amount of storage required and the total archiving time can be calculated.

**[5] USB port**

It may be possible to connect a USB flash drive or hard drive to the CCTV system for data retrieval. Archiving data to USB drive is often the simplest or only option. It should be ensured that the drive is only accessed by write protected means following recovery. It should be noted that most CCTV systems are not capable of writing to encrypted USB thumb drives.

The USB flash drive is normally just a transfer medium, and the data is then copied to optical disc or secure server to make the Master exhibit.  However, for very large volumes of data it may be necessary to retain the drive, in which case advice should be sought from the relevant specialist unit.

Particularly when used as a transfer medium it is essential that USB flash drives are individually identifiable and audit trails of their use kept. If these drives are re-used records must be kept, including details of when and how they are sanitised (erased and reformatted). These drives have a finite number of read/write cycles, so a record of their use and regular replacement will reduce risk of unexpected media failure.

If the data is provided by the third party then this is a level zero activity. However, if the requirement is for the officer to operate the machine then it is a level one activity. If problems occur there may be other issues specific to the system (USB compatibility etc.) and the task should be escalated to a level two officer.

**[6] Transfer to permanent storage**

Where a USB drive has been used to download the data at the premises, either for convenience or out of necessity, it is strongly recommended that a Master copy is then made from this on a secure server or on a write once medium such as optical disc. Copying the data is more cost-effective than retaining the USB drive permanently as evidence and also the lifespan of stored drives is uncertain, so using a secure server for Master storage is preferable. The USB drive must then be sanitised using a force approved method before reuse.

If very large volumes of data have been extracted, it may be deemed impractical to archive to optical disc, in which case if a secure server is not available a decision could be made to retain the USB drive as the Master. This should then be stored and handled accordingly, and only accessed via write protected methods. A bit for bit Working copy could be made on another HDD. It is permissible to make Working copies of sections of the Master provided that they are suitably labelled and records are maintained. The forensic video unit should be contacted for advice.

### [7] Removable media

If the facility exists to back-up data to removable flash media such as CF (compact flash), SD (secure digital), Micro SD, etc., then this may be utilised for extracting video sequences.

Alternatively, if the recording device uses removable media as its primary storage medium then it may be required, in the first instance, to remove and retain that media. In some instances this removable media is a caddied drive and not a memory card, though this is the exception not the rule with caddied hard drives. See section 12 for guidance on removable hard drives.

Removable flash media memory cards are not the ideal medium for storing Master copies as cards are less stable and more expensive than the alternatives. Thus if a memory card is used, it is recommended that this is treated as a transfer medium only, and the data files are then copied to the Master medium.

If the original flash media can be ejected and is retained or transferred directly to secure server (following force SOPs), then this is a level zero activity. However, if the requirement is for the officer to operate the machine then it is a level one activity. Data retrieval from a corrupt or erased memory card is a level three activity.

Extraction of video or photographic evidence from a mobile phone is a specialist area and should only be undertaken by a suitably trained and competent person.

### [8] Optical drive

Some digital CCTV systems have a built-in optical drive for downloading data, though this is becoming increasingly uncommon. Write-once discs should be used, even if the intention is to use the CD/DVD as a transfer medium and store the Master evidence on a secure server. If the optical disc is used for Master storage it is strongly suggested that a duplicate is made as soon as possible and all work carried out from that. This is because of the risk of physical damage to the disc.

If the data is provided by the third party then this is a level zero activity. However, if the requirement is for the officer to operate the machine then it is a level one activity.

### [9] Direct network connection

Where CCTV unit provides network connectivity, a laptop could be linked to the system to create a local network and allow transfer of data.

DVR-based systems may require remote viewer software to be installed on the laptop, although this can sometimes be downloaded directly from the DVR via a web browser. Video data can be downloaded to the hard drive on the laptop or to a USB hard drive connected to it, and a Master copy then created from this on an appropriate medium, with the laptop/drive treated as a transfer medium. It may be advisable to have a quarantine area established for downloaded data to allow for suitable virus and malware checks to be carried out.

This is a level two activity.

### [10] Unit portable

In circumstances where all other retrieval options have been rejected as either impractical or unavailable then the decision may be made to remove the recording unit itself. This assumes that it is physically possible to do so, and that removal is justified by the significance of the incident being investigated. For example, where the volume of data required is very large, it may be time efficient to temporarily remove the recorder and undertake the download in the lab, rather than wait at the site for a download to complete. Alternatively, for some systems, there may no straightforward method for extracting the required video (e.g. no CD writer or data output ports and a hard drive that cannot be replayed in another machine). In this scenario, it may be necessary to take the recorder and retain the unit as evidence.

If the DVR is removed, the implications (legal, insurance, etc.) of this should be considered, and a decision taken as to whether a replacement recorder should be provided, or other arrangements made in order to maintain security at the premises. Provision of a replacement recorder may not be straightforward as there are several incompatible technologies current within CCTV installations. A further consideration is that the data on the machine remains the property of the system owner and they have a right of access to it (unless the data constitutes an offence in its own right, or the data they need access to would compromise the investigation).

If the recording unit is to be removed from the premises, then at a minimum the following information must be captured:

- Time check
- Passwords
- Photograph to show what cameras are working
- Photograph of the rear to show connections – preferably labelled
- Power cable and any power supply transformers
- Remote control if present
- Mouse if present

This is a level one activity. Once the CCTV system has been disconnected from its installation, any further retrieval procedures or processes are level three.

### [11] Data extractable

If a DVR unit has been removed from the premises because it was more time efficient to do so than to wait while the video was downloaded, then the data should be transferred to a suitable Master format on returning to the lab, and the DVR then returned. For those systems where it is impossible to extract the data in a format that can be replayed, the DVR unit itself may need to be retained as evidence. Any retrieval activities carried out in a lab environment are level 3.

In some cases direct access to the hard drive may be considered as a suitable route for acquiring the CCTV data. If this is the case then the following points should be noted, particularly that while hardware and software facilities exist to read data directly from the hard drives of some systems, this only applies to a limited subset of systems.

- The direct replacement of hard drives can be a quick method for extracting large volumes of data from a system. The recorder may be equipped with a removable hard drive in a caddy, or the casing of the unit may need to be opened and the storage drives extracted and replaced. Depending on the system, the hard drive could be replaced with a blank (the quickest option) or a clone could be taken and the original drive replaced. Once the drive has been removed or cloned either the data can be written to a secure server or the drive can be retained. It should be noted that the CCTV recorder may not recognise any replacement drive fitted, even a clone of the original. A suitable method of replaying the data as outlined above would still be required. The original must not be returned until it has clearly been established that the data can be replayed in the laboratory.
- Where the casing of the DVR/NVR needs to be removed to access the drive, care must be taken to follow appropriate health and safety procedures, particularly with regard to potential exposure to electricity, biohazards and other contaminants. The probability of invalidating the manufacturer's warranty or damaging the storage media by undertaking this procedure also needs to be considered.
- The data may appear to be contained on a removable hard drive in a caddy which is thus easy to extract. However, there may be a second hidden data drive within the DVR, which is only accessible by removing the case. This could mean at best some of the data may be missing, and at worst the drive is part of a RAID which could make replay impossible without the original configuration of drives.
- A hard drive removed from a standalone DVR/NVR is not usually in a Windows compatible format, and therefore the data files will not be accessible via connection to a PC. Some software/hardware solutions exist that allow direct replay from the hard drive but they are not universally applicable to all systems. It may be possible to replay the data from the hard drive by fitting it to another CCTV recorder of the same make model and configuration as the one from which it came. There are several risks with this approach, however, and it should only be attempted with caution, and by suitably trained and competent persons.

Operations that do not require opening the machine (e.g. caddied hard drives) are level two activities. Anything that requires removing the cover on the machine is level three, as is any retrieval activity carried out after the recording device has been separated from its system.

### [12] Request not practical

Where it is impractical or not economically viable to download the required data and the CCTV recorder is too large or complex to be removed, the request should be referred back to the SIO for a policy decision. The SIO should be presented with alternative options to enable data to be retrieved. For example:

- It may be easier for an investigator to review and note the content of the CCTV system in situ. This may save considerable time and resources awaiting recovery and potential processing.
- It may be possible to reduce the volume of data required by reconsidering the time period of interest or the number of cameras needed. By reducing the volume of data, it may then be possible to use some of the methods that had previously been rejected.
- It may at this stage be necessary to consider using other techniques such as screen scraping, or recording the monitor feed (streaming), which do not provide exact copies of the original data, but which may be the only practical way of retrieving video evidence from the system. This would be a level three activity.

# 4 Training and Checklists

As mentioned in section 3.5 training and experience can be split into four levels as outlined below:

- Level zero – basic acquisition – receipt from the owner. This level is covered by online awareness training provided by the College of Policing, or as mandated by force policy.
- Level one – allows operation of a functioning device in situ, using manufacturer's documented standard procedures, and requires force approved training and competency checks based on the information within this document.
- Level two – as level one but using more involved techniques and more in depth training. It is likely that at least the majority of equipment listed in Section 3.4 would be required. Requires a higher level of training based on the information within this document.
- Level three – specialist methods that require accreditation to ISO 17025. This includes non-standard download techniques and any of the above processes not carried out on a working machine in situ.

Level zero is not considered a forensic science activity, although appropriate handling of the received media or files is nevertheless required, as the purpose of acquiring the data is to identify evidence. The remaining levels are considered forensic science activities and are therefore covered by the Forensic Science Regulator's Codes of Practice, however only level three currently requires accreditation to ISO 17025.

A full definition of the levels is given in NPCC Framework for Video Based Evidence (to be published), but in essence levels one and two cover operation of a working machine in situ using the manufacturer's intended and documented methods, the split into two levels being a recognition that some methods are more complex than others. Level three is anything not covered by levels one and two and any process including those outlined in levels one and two that are carried out on a machine that has been removed from its installation.

## 4.1 Level Zero Checklist

This sets out the important factors when requesting CCTV from a third party. It is expected at this level that the owner will operate the machine. The points listed under requirements should be checked with the system owner before download as the owner may not be aware of what is important from a police perspective. The sections highlighted in yellow should be amended to match force procedures.

**Don't**

1. **Don't video the screen for evidential use.**
2. **Don't unplug anything.**

3. **Don’t switch the machine off.**
4. **Don’t operate the machine.**
   (unless there is an immediate risk that important data will be overwritten before it can be retrieved - seek further advice from…).

5. **Don’t change times, dates or any other settings.**

**Requirements**

1. **Time check**
   Compare the time displayed by the CCTV system with that given by the speaking clock. Record in the audit trail and compensate if necessary when requesting the data.

2. **Contemporaneous notes**
   These should be kept, detailing the course of action, to provide an audit trail.

3. **Evidential integrity**
   If possible (and used), ensure USB is blank and has been formatted before use – this can be done in the CCTV system

4. **Native format**
   Request that the recovered data is in its native format.

5. **Replay software**
   Request the replay software is included with the data.

6. **Internet links**
   As per force policy – usually handled by specifically trained staff.

7. **Escalate**
   If you do not understand or cannot achieve any of the above seek advice from your forensic video unit or

### 4.2 Level One Checklist

This checklist is designed for first responders who have received the training outlined above. The sections highlighted in yellow should be amended to match force procedures.

**Don’t**

1. **Don’t video the screen for evidential use.**
2. **Don’t attempt to operate a machine you are unfamiliar with.**
   (You will have to evidence your actions)
3. **Don’t unplug anything.**
4. **Don’t switch the machine off.**

(unless there is an immediate risk that important data will be overwritten before it can be retrieved - seek further advice from…).

5. **Don’t change times, dates or any other settings.**

If in doubt about any systems please contact your forensic video unit or

**Do**

1. **Time check**
   Compare the time displayed by the CCTV system with that given by the speaking clock. Record in the audit trail and compensate if necessary when conducting the retrieval.

2. **Contemporaneous notes**
   These should be kept, detailing the course of action, to provide an audit trail.

3. **Evidential integrity**
   a. If used, USB drives should be force issue or approved.
   b. Ensure USB drives are individually identifiable.
   c. Sanitise (erase and reformat) USB drives between uses.

4. **Native format**
   Ensure that the recovered data is in its native format.

5. **Replay software**
   Ensure the replay software is included with the data.

6. **Internet links**
   As per force policy – usually handled by specifically trained staff.

7. **Escalate**
   If you do not understand or cannot achieve any of the above seek advice from your forensic video unit or

### 4.3 Level Two Checklist

This has all the points described in section Download Checklist, (key points given here for convenience) with reminders from other sections of the guidance. The section highlighted in yellow should be amended to match force procedures.

1. **Don’t video the screen for evidential use**

2. **Time check**
   To the nearest second if possible.

3. **Evidential integrity**
   a. If used, USB drives should be force issue or approved.
   b. Ensure USB drives are individually identifiable.
   c. Sanitise (erase and reformat) USB drives between uses.

4. **Contemporaneous notes**

   The audit trail should include such details as:

   i. System Details;
   ii. Time check
   iii. Make and model of the CCTV system,
   iv. Number of cameras – both recording and relevant,
   v. Any audio sources,

5. **Is it recording?**
6. **Time period existing on the DVR e.g. first recording**
7. **Basic system settings**

   E.g. current record settings and display settings

8. **Time period required**

   Due reference must be made to the proportionality

9. **Check storage / overwrite time**

   To determine how long the relevant data will be retained on the system

10. **Determine which camera views are required**

    It is good practice to draw a plan of the camera views to facilitate further decision making processes.

11. **Hidden or covert cameras**

    May be apparent if a different set of access credentials are used.

12. **System password, if necessary**

    Be aware that the standard user password may provide only limited functionality.

13. **Replay Data**

    Check that the requested video exists on the system.

14. **The recording should not be stopped during the retrieval process unless:**

    a. This is an unavoidable feature of the system or
    b. There is an immediate risk that important data will be overwritten before it can be retrieved.

15. **Protect data**

    Some systems allow write-protecting a selected video sequence.

16. **Confirm that the data can be retrieved in its native file format**

    Native file format maintains image quality.

17. **Replay software**

    Vital if the data format is proprietary.

18. **Confirm success of retrieval**

The retrieved data should be checked before leaving the scene (or as soon as possible afterwards).

**19. Restore the system to the owner**

Ensure that video is being recorded onto the system as well as being displayed as a live view.

**20. Complete evidence sheet**

The following information should be included:

i. Discrepancy in display time and date
ii. Time period covered by download
iii. Earliest recorded data
iv. Map of camera locations and coverage
v. Replay software included
vi. Make and model
vii. Transit media used.

**21. Media handling**

Media should be packaged to minimise the likelihood of damage or loss in transit.

**22. Loss of Media**

a. Note separately what data is on each item of evidence as part of the audit trail.
b. Any loss of an exhibit in transit or at any point prior to its official destruction must be reported to your information security department.
c. Any loss of personal data will further need to be reported to the Information Commissioners Office.

**23. Escalate**

If you do not understand or cannot achieve any of the above seek advice from your forensic video unit or

### 4.4 Level Three Checklist

No checklist is provided at this level as procedures will have their own ISO 17025 processes. However, it is a useful reminder that forensic analysis should not be carried out on data that is not in native format, as this could seriously compromise the results.

## Glossary

**BNC**

Bayonet Neill-Concelman connector used to connect camera feeds to a CCTV recorder.

**CCTV**

Closed Circuit Television. System where video is transmitted for display or capture without being broadcast. Commonly used for surveillance and security applications.

**CD**

Compact Disc. Digital optical recording medium. Available both in write once (CD-R) and re-writable (CD-RW) form. CD-R versions are preferred in order to ensure evidential integrity.

**Cloud**

Cloud based storage is a variation on server based storage, though it refers to a particular storage architecture the term is often used to describe any off-site storage.

**CPS**

Crown Prosecution Service

**DAMS**

Digital Asset Management system, sometimes referred to as a Media Asset Management system and is a searchable repository usually of “media” i.e. audio, video and photo files. These systems often include input and output decoders deployed automatically when items are added to or exported from the system. This may or may not be hosted locally.

**DEMS**

Digital Evidence Management system, similar to a DAMS or MAMS but optimised for storing evidence and related files. Often with enhanced functionality.

**DSTL**

Defence Scientific and Technology Laboratory

**DVD (DVD+/- R, +/- RW, RAM)**

Digital Versatile Disc. Optical recording medium similar to a compact disc, but with closer track and pit spacing allowing for greater storage capacity (up to 4.7GB for a single layer DVD disc).

Like CD, DVD is available in write-once and re-writable forms; however, two competing and incompatible standards exist, denoted by either ‘+’ or ‘-’

labelling. Many modern DVD drives can read both formats. An additional, less common re-writable form exists, known as DVD-RAM, which can be written to in a similar way as a computer hard disk drive.

**DVR**

Digital Video Recorder. A generic term for a CCTV recorder, usually has analogue camera feeds via BNC connectors, though these are rapidly being replaced by IP systems that have RJ45 connectors and digital feeds. (See NVR)

**GB**

Gigabyte. A unit of information or storage equivalent to 1 billion bytes or 1 thousand megabytes. Typical computer hard disk drives have a storage capacity measured in hundreds of gigabytes.

**IP**

Internet Protocol. A standard that allows for the transmission of data across networks. Every machine on the network has a unique identifying number, known as an IP address.

**Master**

The definitive copy of the data, that is documented, sealed and stored according to established procedures and can be examined by a court if required, to confirm the authenticity of the evidence relied on in proceedings. The Master may be stored as a physical item or purely in digital form.

**Metadata**

Data about the data. This data provides description and context to enable a deeper understanding or confirmation of the data. It is often essential in a policing context providing information such as time and date, location, speed, frame rate etc.

**Native File Format**

The file format of the primary image or the manufacturer specific file format of the CCTV download.

**NPCC**

National Police Chiefs’ Council

**NVR**

Network Video Recorder. Generally has digital camera feeds connected using RJ45 connectors

**OIC**

Officer in Charge

**PACE**

Police and Criminal Evidence Act

**Sanitisation**

The procedure by which reusable media such as USB ‘flash drives’ are cleared of data to prevent file corruption or easy restoration of deleted files.

**Secure Server**

The term ‘secure server’ or secure police network should be taken to mean a system that has been accredited by the local force Information Security Officer, as per the Information Assurance section of the Information Management APP, for storage of Master evidence.

The term ‘secure server’ covers a variety of server based storage solutions including DEM and DAM systems, cloud storage and variants of these.

**SIO**

Senior Investigating Officer

**SLA**

Service Level Agreement

**SOP**

Standard Operating Procedure. These are local protocols developed by the force to suit their working patterns. These must follow the guidance given in this document where appropriate.

**SWGDE**

Scientific Working Group on Digital Evidence swgde.org

**USB**

Universal Serial Bus. A standard interface port between a computer and add-on devices. Though the term refers to the interface it is often used interchangeably for storage media.

**USB Write Protection**

A software based utility which helps protect data written to connected USB device and prevents data on USB drives from being modified or deleted. (Recommended for use when viewing USB based data).

**USB Killer**

A USB thumb drive constructed to send an electrical pulse designed to disrupt or disable any machine it is plugged into.

**Working Copy**

A copy of the data made either from the Master copy, or at the same time as the Master copy, and used for investigation, technical investigation, briefings, circulation and preparation of prosecution or defence evidence.

**WORM**

Write Once Read Many. Used when discussing computer storage media that can be written to only once, but read from multiple times, such as CD-R and DVD+/-R.

**Write Blocker**

See write protection

**Write Protection**

A one way method of accessing the information on a storage such that no data is written from the host machine to the drive. This can be implemented by either hardware or software methods. Different methods are more or less efficient and workable depending on the operational environment.

This information is released for Defence purposes and whilst it does not attract a national Security Protective Marking, elements of the information may be of a sensitive nature and therefore the information is to be:

- Handled, used and transmitted with care.
- Basic precautions against accidental compromise, opportunist or deliberate attack are to be taken.
- Disposed of sensibly by destroying in a manner to make reconstruction unlikely.

Ministry
of Defence