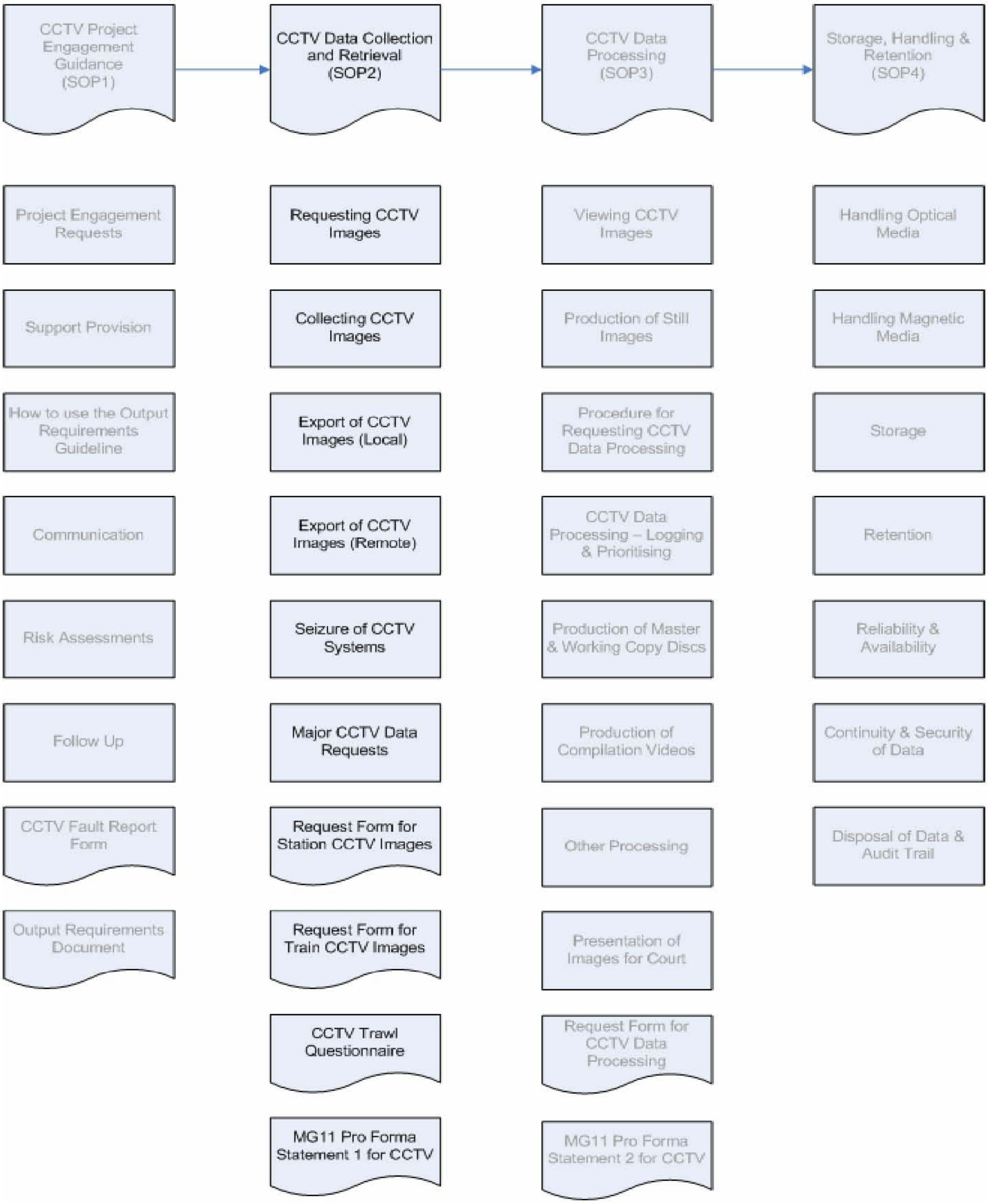
CCTV DATA COLLECTION & RETRIEVAL
STANDARD OPERATING PROCEDURE (SOP)

STANDARD OPERATING PROCEDURE			
REFERENCE.	SOP/182/09		
PROTECTIVE MARKING	RESTRICTED		
PORTFOLIO	Crime		
OWNER	National CCTV Manager		
START DATE	15th June 2009		
REVIEW DATE	15th December 2009		
THIS POLICY REPLACES:			
VERSION	DATE	REASON FOR AMENDMENT	AMENDED BY
3.0	29/05/09	N/A	Mark Leahy

CCTV Standard Operating Procedures – Road Map


CCTV Project Engagement Guidance (SOP1)
Project Engagement Requests
Support Provision
How to use the Output Requirements Guideline
Communication
Risk Assessments
Follow Up
CCTV Fault Report Form
Output Requirements Document
CCTV Data Collection and Retrieval (SOP2)
Requesting CCTV Images
Collecting CCTV Images
Export of CCTV Images (Local)
Export of CCTV Images (Remote)
Seizure of CCTV Systems
Major CCTV Data Requests
Request Form for Station CCTV Images
Request Form for Train CCTV Images
CCTV Trawl Questionnaire
MG11 Pro Forma Statement 1 for CCTV
CCTV Data Processing (SOP3)
Viewing CCTV Images
Production of Still Images
Procedure for Requesting CCTV Data Processing
CCTV Data Processing – Logging & Prioritising
Production of Master & Working Copy Discs
Production of Compilation Videos
Other Processing
Presentation of Images for Court
Request Form for CCTV Data Processing
MG11 Pro Forma Statement 2 for CCTV
Storage, Handling & Retention (SOP4)
Handling Optical Media
Handling Magnetic Media
Storage
Retention
Reliability & Availability
Continuity & Security of Data
Disposal of Data & Audit Trail

CONTENTS

GLOSSARY

BMP IMAGES Short for ‘Bitmap’. The BMP format is a commonly used graphic format for saving image files. The BMP format stores colour data for each pixel in the image without any compression. This method of storing image information allows for crisp, high-quality graphics, but also produces large file sizes. The JPEG and GIF formats are also bitmaps, but use image compression algorithms that can significantly decrease their file size. For this reason, JPEG and GIF images are used on the Web, while BMP images are often used for printable images.

CRT The term stands for ‘Cathode Ray Tube’ (CRT, is the main component of most computer display monitors and television sets. A CRT consists mostly of a specially-shaped vacuum tube that contains a screen coated with a thin film of phosphorous materials on the large end. A high-speed beam of electrons is shot from an *electron gun* on the other end. This beam moves back and forth across the screen at high speed, striking specific spots on the phosphor dots, causing them to glow and thereby creating images visible to the human eye.

DVI Stands for ‘Digital Visual Interface’. It is a video interface standard designed to maximize the visual quality of digital display devices such as flat panel LCD computer displays and digital projectors.

FIREWIRE This is a type of cabling technology for transferring data to and from digital devices at high speed. Some professional digital cameras and memory card readers connect to the computer over FireWire. FireWire card readers are typically faster than those that connect via USB. Also known as IEEE 1394, FireWire was invented by Apple Computer but is now commonly used with Windows-based PCs as well.

GIF

The ‘Graphics Interchange Format’ (GIF) is a bitmap image format. The format supports up to 8 bits per pixel, allowing a single image to reference a palette of up to 256 distinct colours chosen from the 24-bit RGB colour space. It also supports animations and allows a separate palette of 256 colours for each frame. The colour limitation makes the GIF format unsuitable for reproducing colour photographs and other images with continuous colour, but it is well-suited for simpler images such as graphics or logos with solid areas of colour.

IP ADDRESS

An ‘Internet Protocol’ (IP) address is a numerical identification (utilising) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes. Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166. The role of the IP address has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

JPG IMAGES

The term stands for ‘Joint Photographic Experts Group’. A JPEG is a compressed image file format. JPEG images are not limited to a certain amount of colour, like GIF images are. Therefore, the JPEG format is best for compressing photographic images. While JPEG images can contain colourful, high-resolution image data, it is a lossy format, which means some quality is lost when the image is compressed. If the image is compressed too much, the graphics become noticeably "blocky" and some of the detail is lost.

SCSI PORT

Short for ‘Small Computer System Interface’. It is a parallel interface standard used for attaching peripheral devices to computers. SCSI interfaces provide for faster data transmission rates (up to 80 megabytes per second) than standard serial and parallel ports. In addition, you can attach many devices to a single SCSI port.

SDI The term stands for 'Serial Digital Interface'. It is a physical interface widely used for transmitting digital video in various formats. For electrical transmission, it uses a high grade of coaxial cable and a single BNC connector with Teflon insulation. It also uses optical fibres with ST, SC and FC connectors.

USB This term stands for 'Universal Serial Bus'. It is a hardware interface for attaching peripheral devices.

VGA / DVI OUTPUT The term stands for 'Video Graphics Array'. The term refers to the 15-pin plugs and sockets that connect the computer to the monitor. In this context, VGA refers to the traditional analogue connection to a monitor in contrast to DVI, which is digital. Analogue CRTs use VGA, and modern flat panel displays have both VGA and DVI inputs.

VTR The term stands for 'Video Tape Recorder'. It is a videotape recording and playback machine. VTR may refer to consumer MiniDV and DV recorders or to professional machines such as Betacam, DVCPRO and DVCAM.

CCTV Data Retrieval Standard Operating Procedure (SOP)

1 INTRODUCTION

1.1 This SOP is part of a series of corporate controls for Closed Circuit Television (CCTV) from cradle to grave, to introduce a more forensic discipline around the handling and processing of CCTV product. British Transport Police (BTP) operates in a CCTV rich environment which if correctly exploited and managed can have a direct positive impact on crime reduction and detection.

1.2 This procedure enforces and is subject to the conditions of policies SOP/181/09, SOP/183/09 and SOP/184/09.

1.3 This procedure applies to England, Wales and Scotland.

1.4 This procedure applies to all BTP officers and staff.

1.5 The increased use of CCTV images within the force has necessitated the production of this SOP in order that the retrieval and subsequent use of CCTV images is carried out in a more professional and corporate manner.

1.6 It is important to remember that any items seized by Police will generally fall within three basic categories: Evidential, Intelligence, Management Information.

- Evidential – Any tape / disc / media storage device which contains evidence which may be placed before a court or other judicial tribunal.

- Intelligence – Any tape / disc / media storage device which is of intelligence use only (although judgement will be required in certain cases where such material could become evidential after a period of time).

- Management Information – Generally in cases of the police this will apply to storage media used within police station environment (custody etc).

2 KNOWLEDGE

2.1 Terms and Definitions

BTP	British Transport Police
CCTV	Closed Circuit Television
DCCTV	Digital Closed Circuit Television
DVR	Digital Video Recorder
IO	Investigating Officer
SIO	Senior Investigating Officer
SOP	Standard Operating Procedure

2.2 Responsibilities

2.2.1 The SOP is aimed at any personnel involved in CCTV data collection or retrieval (exporting) both locally and remotely and will ensure a consistent approach across all Areas. A lack of forensic control jeopardises the validity and integrity of CCTV data, and adherence to this SOP will protect the integrity of CCTV data and the reputation of the Force.

2.2.2 Data collection is defined as CCTV data produced by another party that is collected by BTP staff. Section 4 sets the standard procedure for collecting CCTV evidence.

2.2.3 Data Export is defined as the actual process of exporting CCTV data from the system either locally or remotely. Local export is defined as being at the location of the recorder; remote export is defined as being at a different location to the recorder (i.e. using a network from one site to another). Sections 5 and 6 set out the standard procedure for exporting CCTV evidence.

2.2.4 Seizure of CCTV systems is defined as an entire recording device seized under Section 19 Police and Criminal Evidence Act 1984. In the case of Scotland, such a seizure is carried out under common law. Section 6 of this document sets out the procedure for seizing CCTV systems.

2.2.5 CCTV is a valuable investigation tool and should be used whenever it is available. Images can be used to help identify suspects, show the actions of someone at a scene, or indicate areas where an individuals DNA or fingerprints may be recovered.

The role of front line staff

- Staff not trained in CCTV retrieval (export) such as front line officers may have to collect CCTV evidence from time to time; this document sets out the correct procedure to follow. Police Officers will not normally be expected to export CCTV evidence from systems; this should be done by either a representative of the CCTV system owner or dedicated (trained) BTP CCTV staff.

- Should personnel require CCTV to be exported and the system owner cannot provide the expertise then they should contact their local BTP Area video unit for advice.

The role of trained CCTV staff

- CCTV data export is primarily the responsibility of the system owner. Dedicated CCTV staff will be responsible for the routine retrieval of CCTV evidence from their respective Police Areas in cases where the export cannot be achieved by the system owner, is problematic, or of a sensitive nature.

- Trained CCTV staff should support the collection process carried out by front line staff to ensure continuity of evidence and the collection of relevant information is achieved at all times.

2.3 Equal Opportunities Statement

2.3.1 All employees have a responsibility to ensure that no discrimination occurs on the grounds of age, colour, disability, ethnic origin, family commitments, gender, gender dysphoria, marital status – marriage or civil partnership, nationality, national origins, political beliefs, race, religion or belief, sexual orientation, trade union activity or any other unacceptable grounds.

3 PROCEDURE FOR REQUESTING CCTV IMAGES

3.1 This section of the SOP deals with requesting CCTV images to be produced from a CCTV system and does not deal with any secondary processing of CCTV images such as editing, enhancement, or duplication of CCTV media.

3.2 CCTV systems on the rail network are owned by the rail companies themselves therefore any request for CCTV generally has to go to the company in question. BTP are linking some CCTV systems back to our own CCTV hubs, details of which can be found on the Gazetteer. The CCTV section of the Gazetteer is currently under development. In cases where a system is linked to BTP then the CCTV images may be produced by our own CCTV staff.

3.3 Broadly speaking CCTV images fall into three categories namely Stations (or depots), Trains, and other premises such as car parks, retail units or non-rail industry systems (e.g. local council CCTV).

3.4 Specific details of how to request CCTV images from stations, trains and car parks are held on the Gazetteer[1] (under Applications – Gazetteer on the Force intranet). To request images from a retail unit or non-rail industry system the CCTV owner / premises should be contacted direct. Should there be any issues with retrieving images from an outside source contact your local video unit for advice.

3.5 To request CCTV images from the rail network use the Gazetteer to search for the station name (or rail company in the case of train CCTV). Once you have found the station or company you require click on the "CCTV" button on the page, this will give you details of where to send your request. CCTV Request Forms can be found under A-Z of Forms on the intranet. Forms should be completed as fully as possible before sending. The "Request for CCTV Images" form can also be found in Appendix "A" of this SOP[2].

Note: You may have to ascertain specific train information (such as head codes) when requesting CCTV from on board a train. This information can be obtained from the train company themselves details of which should be on the Gazetteer page.

4 PROCEDURE FOR COLLECTION OF CCTV IMAGES

4.1 All CCTV evidence collected by staff should be checked for continuity i.e. all evidence is correctly packaged and a statement written by the person that produced the CCTV, see Appendix "B" MG11 Pro Forma Statement for Staff Producing CCTV. In the case of Scotland, a Form 283 should be completed by the person supplying the CCTV images, see Appendix "C".

[1] The CCTV Section of the Gazetteer is currently under development
[2] The CCTV forms can currently be found on the intranet under "C" for CCTV (in A-Z of forms)

4.2 An audit trail must also be kept to ensure evidential integrity. See Appendix "D" MG11 Pro Forma Statement for Collection or Retrieval of CCTV. Please note that police personnel should complete that part of the document that refers to Collection only.

4.3 CCTV images collected should be viewed as soon as possible to confirm that the correct images have been produced from the system.

4.4 CCTV media (disks, tapes etc) collected should be handled and stored as per BTP's guidance on Handling and Storage set out in CCTV SOP4, Storage, Handling and Retention.

4.5 In major investigations (such as serious incidents or terrorism) a CCTV Recovery Questionnaire (Appendix "E") should be completed before leaving the premises; the officer collecting the media should complete this form.

4.6 Personnel collecting images for major investigations should compare the time displayed by the CCTV system with the current time, which is determined by the use of the MSF Signal (formerly the speaking clock) by dialling 123. Any difference should be documented on the CCTV Trawl Form.

4.7 It is important that when carrying out the time check procedure a note is made and included in any subsequent statement and that a copy of the CCTV Trawl Form is included with any disk or tape given out for viewing.

4.8 Officers should ensure that if CCTV cannot be seized the reason is noted. In the case of evidential material CRIME should be updated. For all other purposes, the officers Pocket Note Book should be used to record the full details.

4.2 An audit trail must also be kept to ensure evidential integrity. See Appendix "D" MG11 Pro Forma Statement for Collection or Retrieval of CCTV. Please note that police personnel should complete that part of the document that refers to Collection only.

4.3 CCTV images collected should be viewed as soon as possible to confirm that the correct images have been produced from the system.

4.4 CCTV media (disks, tapes etc) collected should be handled and stored as per BTP's guidance on Handling and Storage set out in CCTV SOP4, Storage, Handling and Retention.

4.5 In major investigations (such as serious incidents or terrorism) a CCTV Recovery Questionnaire (Appendix "E") should be completed before leaving the premises; the officer collecting the media should complete this form.

4.6 Personnel collecting images for major investigations should compare the time displayed by the CCTV system with the current time, which is determined by the use of the MSF Signal (formerly the speaking clock) by dialling 123. Any difference should be documented on the CCTV Trawl Form.

4.7 It is important that when carrying out the time check procedure a note is made and included in any subsequent statement and that a copy of the CCTV Trawl Form is included with any disk or tape given out for viewing.

4.8 Officers should ensure that if CCTV cannot be seized the reason is noted. In the case of evidential material CRIME should be updated. For all other purposes, the officers Pocket Note Book should be used to record the full details.

4.9 CCTV images should be collected as soon as possible after confirmation that they are ready. Some organisations will only hold onto the images for a limited amount of time before disposing of them.

4.10 It is vitally important for continuity and evidential reasons that all personnel update the relevant systems when either CCTV is seized or viewed. CRIME – For all offences. Custody and Case Management System – For suspects who are arrested (when fully developed).

5 PROCEDURE FOR EXPORT OF CCTV IMAGES

5.1 Logging / prioritising requests

5.1.1 BTP CCTV staff will on occasions carry out local (on site direct from the recorder) export of CCTV images. When doing so they will carry out the following procedures.

5.1.2 Log the export request on the corporate CCTV database "Socrates"[3]. Check the request for urgency and prioritise accordingly. Urgent requests include images required immediately for an investigation or images that are due to be over-written by the system.

5.1.3 Seek the relevant authority from area supervision and ensure a risk assessment has been completed on the CCTV request form.. If required arrange for a police officer to accompany you to site.

[3] This database is still in the process of being designed

5.2 Scene Arrival

1. Notes should be kept in staff issue note books detailing the methods used and steps taken during retrieval. If the system is found to be in fault then complete Appendix "F" CCTV Fault Report Form and issue a copy to the system owner.

2. Determine if a manual is available to assist with system information (e.g. passwords, output options).

3. Compare the time displayed by the Digital CCTV (DCCTV) system with the current time. Any difference should be documented. The MSF Signal (formerly the speaking clock) should be used to determine the current time by dialling 123.

4. Establish that relevant video has been recorded by reviewing the recording. Preferably, a person with knowledge of the recording device should operate it during playback, if it is appropriate for them to do so.

5. Determine the earliest recorded date. This will determine approximately how much time there is to retrieve the data before the system begins to overwrite it.

6. Remove network cable, if necessary

7. Determine how much data needs to be retrieved

8. Determine native/proprietary file format the system uses

9. Determine best method of retrieval

10. Sketch DCCTV camera placement and position in staff issued notebook

5.3 Assessing the recording System for Output

5.3.1 A determination should be made as to how much and what type of data needs to be retrieved from the DCCTV recording device. An evaluation of the system's output options should help determine the best and most practical method of outputting the video. When making this assessment, collection of the native/proprietary video file should remain the highest priority to ensure image quality.

5.3.2 The amount of time and storage needed to retrieve the video data may dictate the best method of retrieval.

5.3.3 Performing a test retrieval will assist in estimating the time and storage for the chosen output option.

5.3.4 Administrative and / or Engineer login access to a DVR usually allows more options for retrieval, including native / proprietary files.

5.3.5 Once the appropriate output option is chosen and the video data retrieved, a master copy should be retained. Depending upon the data retrieval method chosen, additional steps may be needed to create the master such as transferring data from an external hard drive to DVD back at the video lab.

5.4 Output Options

5.4.1 CD/DVD Writer

Many DCCTV systems have a built-in or external CD/DVD writer to retrieve the recorded video. In some instances, an external CD/DVD writer can be connected through a USB/Firewire/SCSI port.

- Generally, the DCCTV system software will have an archive, backup, copy, or export function which you can retrieve the data directly to the CD/DVD.

- Generally, the system software will allow you to copy the proprietary viewer to the disc while burning, however, you may have to manually select this option.
- Write-once CD-Rs, DVD-Rs or DVD+Rs should be used.
- Some drives may only write to a specific brand(s) of media. If difficulties are encountered when writing video data, try another brand of media.
- Some DCCTV systems may only take a CD-RW/DVD-RW disc. At the earliest possible time, all data should be transferred from the CD-RW/DVD-RW to a CD-R/DVD-R/DVD+R to create the master evidence.
- The system may require you to format the CD/DVD, either in the DVR itself or in another computer.
- After retrieval, verify that the downloaded / exported file(s) play back correctly on another system, and that the proper dates and times were retrieved.
- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.
- The resulting produced CD/DVD is the master evidence. If more than one disc is created, each should be identified for proper order of playback.

5.4.2 Compact Flash Drives

Some DCCTV systems have a compact flash card option, which is usually intended for short video sequences and should be used as a temporary storage medium only. If video is recovered via these drives, at the earliest possible time, all data should be transferred from the compact flash card to a more permanent media to create the master evidence. Some systems that employ compact flash drives export files in real time and therefore may not be appropriate for the retrieval of a large amount of data.

5.4.3 USB/Firewire/SCSI Devices

USB/Firewire/SCSI ports can be used to connect external CD/DVD writers and devices. It should first be established that the port is a working port. Some devices may require activation by installing the necessary drivers on the recording system. It is recommended that the manufacturer be contacted before attempting to install drivers.

- External USB CD / DVD writers may be used for retrieving smaller amounts of data if no other options exist. External USB/Firewire hard drives are a good resource when large amounts of data need to be collected.

- On some PC based systems that utilise a “standard” Windows operating system, it may be possible to copy the native/proprietary file(s) using Windows Explorer. NOTE: This does not work on all systems as the files retrieved in this manner may require the use of the hardware/software during the retrieval process for playback later. It is strongly recommended to know the system before utilising this method or to consult the manufacturer to ensure the files copied will be capable of playback.

- Most DVR systems have a limitation on the amount of data that can be retrieved at any time, typically 1GB, sometimes 2GB. This limit may not be specified in the system manual or known to the manufacturer. It is best to keep your files under 1GB, unless you know for sure it is capable of more.

- Generally, the DCCTV system software will have an archive, backup, copy, or export function in which you can retrieve the data directly to the device you have attached. You may have to chose the device or navigate to it.

- Generally, the system software will allow you to copy the proprietary viewer to the disc while burning, however, you may have to manually select this option.

- After retrieval, verify that the downloaded / exported files play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- USB/Firewire hard drives are usually considered a temporary storage medium. Therefore, at the earliest possible time, all data should be transferred from the drive to a more permanent media to create the master evidence. This drive should then be wiped before re-using. It the files retrieved are too large, the USB/Firewire drive may be retained as the master evidence.

5.4.4 Network Connection

Many DCCTV recording systems have network ports. Furthermore, many DCCTC systems have their own proprietary “network viewer” software which allows for multi-computer connectivity and recovery of the native/proprietary recorded files.

If you do not have any experience with computers or networking, it is highly recommended that you obtain assistance prior to retrieving video data using this method.

By utilising an Ethernet crossover cable, computer, and network viewer, a connection to the DVR can be established and the native / proprietary files downloaded / exported. The remote or network viewer software is installed on a separate computer / laptop, the IP address of the DVR is usually put into the remote viewer software, and a connection is established.

Verify that the network viewer recovers the native / proprietary recorded video file. EXAMPLE: Some remote viewers only allow for the collection of .jpg or .BMP images and not the entire native / proprietary recorded video file.

- Ensure you have administrator rights on the computer / laptop to which you are downloading / exporting the files. Disable any firewalls.

- Screen savers should be disabled as they can interfere and / or disrupt the download / export process.

- WARNING: Power scheme settings for the computer to which you are downloading the files should be set to “always on” with hibernation disabled.

- The IP address may be required from the DVR. This usually requires accessing the menu functions of the DVR. Care should be taken not to change other settings on the DVR when doing this.

- If you have to change the IP address on the DVR, make a note of the original IP address so you can change it back when you are finished. Changing the IP address may also require rebooting the system.

- Some proprietary remote/network viewers are installed on the DVR system for easy access. Otherwise, searching the vendor’s website or contacting the vendor directly may be necessary.

- On some systems, setting up a standard Windows network connection between the computer and the DVR may be necessary (e.g., computer 192.168.10.1, and the DVR 192.168.10.2). NOTE: It is best practice to try and retain the existing IP settings on the DVR and change those on the computer to match.

- If a network viewer for the system does not exist, a connection may be possible utilising Windows Explorer, a web browser, and typing in an appropriate IP address.

- Most DVR systems have a limitation on the amount of data that can be retrieved at a time, typically 1GB, sometimes 2GB. This limit may not be specified in the system manual or known to the manufacturer. It is best to keep your files under 1GB, unless you know for sure it is capable of more.

- Some networkable systems may only allow for the video to be "streamed" out and may not provide native / proprietary data transfer. Metadata can be lost through streaming. Unless this is the only option, it is preferable to output to digital magnetic tape.

- Ensure network speed is sufficient to ensure that no data is lost and to prevent crashes / timeouts during downloading / exporting.

- You may have to disable any firewall installed, ensure you have administrator rights on the DVR. After completing video data retrieval, confirm you have re-enabled the firewall and various settings.

- After retrieval, verify that the downloaded / exported files play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- Ensure you have also retrieved the proprietary playback software.

- Return all changed system settings to their prior state after data has been retrieved.

- The computer / laptop or USB / Firewire drive(s) that you connected to the computer to retrieve the video files are usually considered a temporary storage medium. Therefore, at the earliest possible time, all data should be transferred from the laptop / drive to a more permanent media to create the master evidence. If an external drive was used then it should be wiped before re-using. If files retrieved are too large, the drive may be retained as the master evidence.

5.4.5 Replacing Hard Drives

In some situations, the quickest solution may appear to be to remove the hard drives from the system and replace them. This option should be considered carefully as there are many factors that come into play. Simply removing a hard drive does not ensure the video files contained on that hard drive will playback. Some DVR systems require the actual DVR hardware to playback the video files on the drive.

If you have limited computer hardware experience, consider calling someone for assistance. Care should be taken to follow appropriate health and safety, particularly with regard to potential exposure to electricity.

- The system should be properly shut down prior to removing any hard drive, even if the drive appears to be hot swappable.

- Ensure that all of the system's hard disc drives are retrieved. The system may have a removable drive in a caddy, but also additional internal drives.

- Document the master / slave drive configuration of all retrieved drives.

- The DVR may require a specific brand, model and size of hard drive to operate correctly. Consult the manufacturer, manufacturer's web site, or system manual for more information.

- The new drives may need to be formatted by the DVR before it will recognize and record to it.

- Once new drives are installed, restart the system and confirm that recording and playback are operational, as the system may require that vendor specific software / operating system be installed. Failure to install such software can render a system either partially or completely inoperable.

- If you remove the existing drives, be aware that you have removed the archive data stored on the CCTV system.

- The removed hard drive is the master evidence. If more than one hard drive is removed, each should be properly identified.

5.4.6 Drive Duplication

In some situations, drive duplication may be necessary. This option should be considered carefully as there are many factors that come into play. Drive duplication does not ensure playback. Some DVR systems require the original hard drive for playback.

It is recommended that a bit for bit duplicate of the original hard drive be produced, not an image set.

- The system should be properly shut down prior to removing any hard drive, even if the drive appears to be hot swappable.

- Some systems require the original hard drive for proper operation. Therefore, if the drive is duplicated, place the duplicate drive back in the system, make sure the system is operational, and retrieve the original drive from the scene. If the system is not operational, the recording device may have to be retrieved, along with the original hard drive.

- Ensure you duplicate all the drives in the system as the DVR may have internal drives.

- Document the master / slave drive configuration of all duplicated drives.

- External playback software may exist to access the video data on the duplicated hard drive.

- Upon initial inspection, a hard drive duplication from a system may not appear to contain data when viewed using a standard PC. Many systems utilize proprietary formats that prevent data from being recognized. If you don't see files upon inspection of the duplicate drive, do not assume that nothing has been recorded.

- The duplicate drive and / or original drive should be inspected using a write blocker and a separate computer / laptop.

- The duplicated drive and / or original drive retrieved from the scene are considered the evidentiary master from which working copies may be produced.

5.4.7 Legacy Output

The following output methods usually enable retrieval of the native video data and can be located inside the digital recording unit or as an attached external device. In some circumstances, this may be the only method on the DVR system for retrieval of the video data. Retrieval and playback may require additional steps. These can typically be connected through the SCSI port. Do not discount this as a retrieval method if you do not have these devices.

- DDS Tape (Digital Data Storage)
- Iomega Jaz
- Iomega Zip
- Floppy
- Magneto Optical

Except for DDS Tape, the above media should be considered a temporary medium. At the earliest possible time, all data should be transferred to a more permanent media to create the master evidence.

Note: It may not be possible to duplicate DDS cassettes; where possible consider uploading to the DVR and downloading the relevant portion to a more readily accessible medium and one capable of duplication.

5.4.8 Removal of DVR Unit

In circumstances where the above listed options have been determined to be either impractical or impossible, the decision may be made to remove the recording unit itself. **Authorisation should be sought from Force CCTV Management before doing so. Whenever possible the CCTV operator will also be consulted.**

This assumes that it is physically possible to do so, and that the removal is justified. For example, where the volume of data required is very large, it may be time efficient to temporarily remove the recorder and perform the retrieval in the lab, rather than on site. Alternatively, there may be no method for extracting the video data (e.g. CD writer or USB ports) and it may be necessary to remove the recorder and retain the unit as the evidentiary master.

- The recording device should be stopped and the system properly shut down prior to removal.

- Ensure all relevant components of the system are collected (e.g. power supply, remote control, dongle, manual, cables).

- Ensure all cables are uniquely identified (e.g. camera inputs) to facilitate reinstallation of the system.

- If no other method exists for extracting the video data from the DVR recording device retrieved from the scene, the DVR is considered the evidentiary master.

5.5 Non-native / Proprietary Data Retrieval

5.5.1 S-Video / Composite Output

- Video can only be retrieved in real time and the process should be repeated for each required camera view.

- When a system has both an S-Video and composite output, it is recommended that the S-Video be used.

- It is recommended that a digital video tape recorder (VTR) be utilized. Some examples of VTR's are Digital Betacam, DVC Pro, DVCam, Mini DV, and Digital 8.

- The video recording should be collected to digital magnetic tape.

- Ensure the time/date stamp is displayed on output; this may require checking several signals (e.g. composite and S-Video).

- It is recommended that the DVR output be directly connected to the VTR and a separate output from the VTR be made to a monitor to ensure that the signal is being received and recorded.

- Prior to recording the video data, check playback on the DVR.

- The collection of the video data to VHS tape of Video DVD should be considered a last resort and conducted if it is the only possible option.

- Taking analogue output from a DVR may produce a different frame size from the original native / proprietary file recorded frame size.

- The produced magnetic tape is considered the evidentiary master.

Note: Video capture cards can be utilised for digitizing a video signal from a DVR into a computer. Most capture cards can take an S-Video and composite input, while higher quality cards can input component, SDI, and /or HD video input. It is recommended that the highest quality input be utilised. Care should be taken to ensure that the recorded frame size is maintained when utilising this method. The digitized data should be captured as uncompressed (1:1) and retained as the master evidence.

5.5.2 VGA / DVI Output

Some DCCTV systems have a VGA or DVI output that allows the video data to be displayed on a computer monitor. These outputs can be converted to a video signal, usually analogue, through the use of a scan converter. This video signal could then be recorded to video format and retained as the evidentiary master. This method typically reduces the image quality below that of an S-Video / composite output and should be considered a last resort.

5.6 Important Information

- Do not change the time and date on the DVR system

- It is not recommended that any additional software be installed on the DVR system (e.g. CD writing software, if it is not present). If it is absolutely necessary to install software, it is highly recommended that the manufacturer be contacted prior to installation.

- If it is determined that the video data of interest has been overwritten, check to see if the venue retains backup files.

- Administrative / Engineer access to the DVR usually allows more options for retrieval, including native / proprietary files.

- Time/Date stamp with file. You may have to take the downloaded file without the time/date data to ensure the highest quality footage, and take a second retrieval of the footage which includes the time/date data utilising the output option that may be of lesser quality to ensure you have the information.

- On systems where the time/date stamp can be moved, ensure that this overlay does not obscure critical events.

- A review of the live monitor is not sufficient and may appear to be of better quality than the actual recorded video.

- Whenever possible, the system should remain recording during the retrieval of the video data.

- Many digital video recording systems allow you to auto copy the proprietary playback viewer while retrieving the video data. If the system does not allow this, steps should be taken to retrieve the correct version, with full functionality, required for playback / viewing.

- The native / proprietary video data should be retrieved. It time permits, and if the system downloads a file that is in a non proprietary format (e.g. AVI) for quick viewing, consider collecting that as well as the native proprietary file.

- If the DVR has multi camera capabilities, all the video data for the required area of interest should be taken as it was recorded. These cameras should be recorded in isolation, showing one camera full screen and non multi cameras on a single screen (e.g. not 4, 8 and 16 on a single screen).

- Ensure that the frame rate upon retrieval is as near to recorded frame rate as possible.
- Ensure that the aspect ratio of the video data upon retrieval is as near to the recorded aspect ration as possible.
- Working copies may be produced from the master evidence.

5.7 Evidence Handling

5.7.1 CCTV media (disks, tapes etc) collected should be handled and stored as per BTP's guidance on Handling and Storage set out in CCTV SOP4, Storage, Handling and Retention. Jewel cases should be used for CDs / DVDs, anti static bags and individual foam insert boxes should be used for hard drives.

5.7.2 To provide an audit trail, contemporaneous notes should be recorded detailing the course of actions taken.

5.7.3 A CCTV Recovery Questionnaire (see Appendix "E") and a witness statement should be completed before leaving the premises. See section 3 of this document for advice on the completion of a CCTV Trawl form.

5.7.4 Keep evidence away from magnets, excessive temperatures, and otherwise hostile environments.

5.8 Prior to leaving the scene, ensure that

- You have completed all the necessary documentation.
- You have collected all required video data.

- The retrieved video data plays back correctly, preferably on another system, and the proper dates and times were retrieved.
- The proprietary playback software, network viewer, backup player, and / or archive software have been retrieved.
- The recording system has been returned to its original state (e.g. any changes to the system have been reset).
- The recording system has been verified as operational.
- If removing the recording system, has the appropriate authority been given from Force CCTV management.
- If removing the recording system, ensure that all necessary peripherals have been retrieved.
- If you have retrieved the recording system, have legal implications been considered.

6 PROCEDURE FOR EXPORT OF CCTV IMAGES (REMOTE)

6.1 The procedure for exporting CCTV images remotely (i.e. a direct network connection between a BTP location and a CCTV system) differs somewhat from the local export procedure in that the network connection is already set up and configured.

6.2 Important system information such as the make and model number is generally already known with a connected networked system so there is no need to record this data for each export.

6.3 There are 8 key steps to be taken following an export request:

- Log the export request on the CCTV database.
- Check the request for urgency and prioritise accordingly. Urgent requests include images required immediately for an investigation or images that are due to be over-written by the system.
- Perform a time check on the system using the speaking clock. Log any discrepancies on a CCTV Trawl Form and save the form electronically in the same folder as the exported images.
- Establish that the relevant video has been recorded by reviewing the recording.
- Carry out the data export.
- Check that all files required are downloaded by reviewing the data.
- Archive the data to the local network storage for your area ensuring any audit trail files are saved in the same location as the video files.
- Update the CCTV database with the processing information and inform the requesting officer that the video is ready for review.

7 PROCEDURE FOR SEIZURE OF CCTV SYSTEMS

7.1 Should an entire CCTV system recorder need to be seized then consultation should take place with the Area Video Unit before doing so. Technical support may be required from a member of CCTV staff to ensure the integrity of the recordings on the device being seized.

8 PROCEDURE FOR MAJOR DATA REQUESTS OF CCTV IMAGES

8.1 There is no fundamental difference in the export or collection of CCTV images for major data requests and routine data requests. The same principles shall apply. However, the management of the process will vary when a request is determined to be a mass data request. If in doubt contact Force CCTV Management for advice.

8.2 Should a large amount of CCTV data be required for an investigation then the Major CCTV Trawl Process should be followed. Terrorist incidents should be managed through BTP Special Branch, non-terrorist related major incidents should be managed by an SIO / IO. Appendix “G” contains the Major Incident CCTV Recovery Process.

9 MONITORING AND COMPLIANCE

9.1 This SOP will be monitored for compliance by the Force CCTV Management team through a process of regular dip sampling. Failure to comply with this SOP could result in non-standard products being used by Industry, with subsequent impact across the Policing and Criminal Justice sector.

APPENDICES

10.1 Appendix A – Request for CCTV Images

10.2 Appendix B – MG11 Pro Forma Statement for Staff Producing CCTV

10.3 Appendix C – Form 283 (Scotland)

10.4 Appendix D – MG11 Pro Forma Statement for Collection or Retrieval of CCTV

10.5 Appendix E – CCTV Recovery Questionnaire

10.6 Appendix F – CCTV Fault Report Form

10.7 Appendix G – Major Incident CCTV Recovery Process