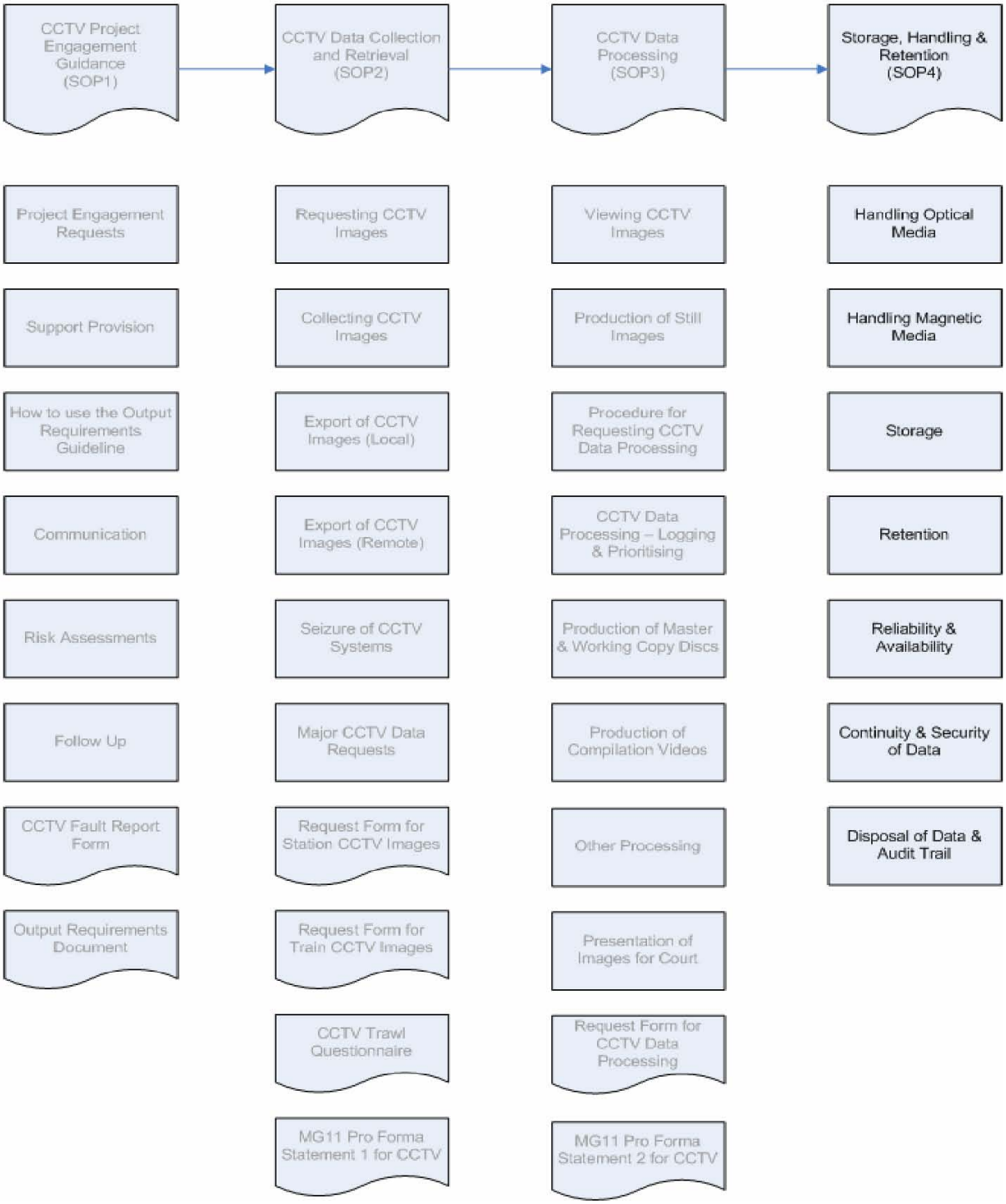
STORAGE, HANDLING AND RETENTION OF CCTV IMAGES STANDARD OPERATING PROCEDURE (SOP)

STANDARD OPERATING PROCEDURE	
REFERENCE.	SOP/184/09
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
2.0	29/05/09	N/A	Mark Leahy

CCTV Standard Operating Procedures – Road Map



CONTENTS

CCTV Data Storage Handling and Retention of CCTV Images (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.

1.2 This procedure enforces and is subject to the conditions of policies SOP/181/09, SOP/182/09 and SOP/183/09.

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

1.4 This procedure applies to England, Wales and Scotland.

1.5 This procedure applies to all British Transport Police (BTP) officers and staff.

2 KNOWLEDGE

2.1 Terms and Definitions

Archiving	The long term retention of imaging data in a system that allows ease of retrieval
Audit Trail	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event
CPIA	Criminal Procedures and Investigations Act 1996
Deletion	The apparent removal of information from a storage medium

Disposal	The removal of information from all police systems so that it cannot be restored
HOSDB	Home Office Scientific Development Branch
Indexing	An allocation of attributes to particular records allowing them to be arranged differently from a related record series and to speed the retrieval of relevant files
Metadata	Data describing the context, content and preservation over time
MOPI	Management of Police Information
NPIA	National Policing Improvement Agency
Replay	Replay is the ability to convert these data files into a viewable format
Retention	The continued storage of and controlled access to information held for a policing purpose which has been justified through the evaluation and review process
Retrieval	Retrieval is the process of accessing image data files
Storage	The long or short term holding of imaging data that has the potential to be used as evidence
TOC	Train Operating Company
Viewing	Viewing is the presentation on a Monitor
WORM	Write once read many

2.2 Responsibilities

2.2.1 It is the responsibility of all officers and staff coming into contact with CCTV data to ensure it is handled, stored and disposed of appropriately to ensure evidential integrity and ensure compliance with the Minimum Standards of Investigation, the Data Protection Act 1998, the Freedom of Information Act 2000 and the Management of Police Information 2005.

2.2.2 This is an interim SOP until a corporate SOP is produced on Information Security and Information Storage of all types of data.

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 PROCEDURES

3.1 INTRODUCTION

3.1.1 These procedures outline processes for storing, handling, retaining and disposing of digital evidential images for all staff handling CCTV data.

3.1.2 This SOP is part of a series of forensic controls for CCTV from cradle to grave. A lack of forensic control jeopardises the validity and integrity of CCTV Data.

3.1.3 This document incorporates recommendations from:

- ACPO (2007) practice advice on police use of digital images CCTV Home Office National CCTV Strategy.
- Home Office Scientific Development Branch publication on Storage, Replay, and disposal of Digital evidential images (53/07).

3.2 Handling: Optical Media (CDs & DVDs)

3.2.1 The recording layer in optical disks can be damaged by light, heat, moisture and a combination of these. Prolonged exposure to moisture allows water to become absorbed into the disk where it may react with the disk components causing failure. Disks should be stored in a dark environment to reduce the risk from light fading.

3.2.2 Optical disks can also be affected by airborne pollutants such as ammonia, chlorine, sulphides, peroxides, ozone, oxides of nitrogen, smoke and acidic gases. Ammonia and chlorine-based cleaners should not be used in optical disk storage areas. Discs should be stored in a jewel case.

3.2.3 Do not touch the recording area of an optical disk. When taking a disk out of the jewel case use the following procedure:

- Open the jewel case and put it down on a flat surface.
- Use a finger to push the mechanism of the centre of the case that holds the hub of the disk.
- Using the other hand pull out the disk from the jewel case, touching only the outside edge of the disk.
- Do not pull or flex the disk excessively as bending can increase the error rate of the disk.

3.2.4 When putting a disk back in the jewel case use the following procedure:

- Open the jewel case and put it down on a flat surface.
- Place the disk on the jewel case labelling side up with the central hub over the retaining mechanism.
- Push the central area of the disk onto the location mechanism. Do not touch data area of the disk.
- Optical disks can develop an electrostatic charge, particularly at low humidity levels. The disks then attract dust particles which can interfere with the reading and writing processes. Operations should be conducted in a clean, dust free environment particularly if the humidity is low.

3.2.5 Only approved rigid type jewel cases will be used. Take care to avoid surface abrasion when inserting or removing disks from such receptacles. Any adhesion may delaminate the disk when it is removed. For long-term disk storage any paper label or insert is removed from inside the case. Paper can retain moisture in the case and may release harmful pollutants.

3.2.6 Do not leave optical disks in the computer drive. Temperatures within a disk reader can exceed 40ºC and repeated thermal cycling can warp the disk.[1]

[1] Reference must be made to the Information Standards Unit webpage. Use of CDs and DVDs to store BTP records. This guidance covers the care, handling and storage of disks.

3.3 Handling: Magnetic Media (Tapes, Hard Drives, USBs & Memory Cards)

3.3.1 Magnetic media can be prone to shock due to the mechanical parts within. Therefore extra care should be taken to prevent damage. Consideration should be given to providing extra padding during transportation.

3.3.2 Particulate contaminants will block access to the material recorded on the media. Smoke, dust and debris generating materials (carpets, curtains, fibrous wall coverings and furnishings) should be avoided in areas where extended life tapes are being handled. Gaseous pollutants such as exhaust fumes and ammonia and chlorine based cleaners should also be avoided in these areas.

3.3.3 Magnetic fields are a concern for magnetic tape use and storage. External magnetic fields are most frequently observed near motors and transformers. A separation of a few metres from the source will usually provide sufficient protection. External fields of a more unanticipated nature may be produced by some headphones and microphones or by cabinet latches and magnetised tools.

3.3.4 Tapes should not be left in video recorders unnecessarily, particularly when the recorder is switched off.

3.4 Storage

3.4.1 In the first instance the DVD, USB, Memory card, hard drive or tape should be placed in the Area Video Library. Where there is no video library data should be placed in the police station property store in accordance with existing property handling procedures, all items should also be recorded on the KIM property database. As with any other items, which could be used as evidence, CCTV data should be stored securely to prevent unauthorised viewing or use.

3.4.2 CCTV property held in a Property Store (main or temporary stores) should first be placed in a specified Force jewel case if it is a DVD or CD and sealed with (2) corporate authorised seals placed top and bottom diagonally in such a way that access cannot be gained to the product without compromising the seal and showing the word "VOID". The rear of the jewel case will have affixed a sticky corporate Exhibit label which will also have the facility to show the movements of the evidence and whether or not the case has been opened and resealed. The corporate property label will be affixed to the outside of the jewel case in such a way that the front of the disc and the rear exhibit label can still be read. Video Tapes will be stored in a similar fashion by sealing across the top of the video case with two (2) corporate authorised seals. The sticky corporate exhibit label with be stuck to the case to allow "easy reading" with the corporate property label affixed on the outside of the case. The person depositing the property will complete the Property Store Register.

3.4.4 Eating and drinking in the storage area must be avoided because of the possibility of spilling crumbs or liquid onto the stored video data. Liquid spilt onto video storage mediums can cause warping and permanent damage.

3.4.5 Tapes should be stored in an upright position within the protective tape box in a cool and dry environment to minimise the warping effects due to gravity. Tapes should not be stored horizontally.

3.4.6 Where tapes are in storage for evidential purposes, including 'unused material' it is necessary to preserve the quality of the tapes by fast forwarding and fast rewinding them at six monthly intervals to ensure that any changes to the wind tension is corrected and no increased wind adhesion is present as a result of any chemical reaction that may have taken place during prolonged storage. Failure to do this could lead to the degradation of the tape. Video tapes that become unplayable should be identified during the rewinding procedure. If the recorded material is important, expert advice should be sought to recover as much as possible of the information stored. Similarly if a tape jams in a machine, expert advice should be sought.

3.4.7 Where data is stored at Area Video Libraries, all property should be logged and stored in a secure strong fireproof cupboard in a lockable room with authorised access only.

3.4.8 All Area CCTV / video units should adopt a clear desk policy with both CCTV data and its associated paperwork.

3.5 Retention

3.5.1 It is important that data is not held any longer than is necessary to comply with the Data Protection Act 1998 and Management of Police Information (MOPI).

3.5.2 The periods of retention for CCTV data depends on the use for which it was generated or acquired by BTP. Broadly CCTV data will fall into three basic categories:

- Evidential - where CCTV data or stills derived from CCTV contains evidence which will be placed before a court or other judicial tribunal then the data or stills assume the same status as a document. CCTV recordings form part of the whole case file for detected or undetected offences. At the time of a MOPI – generated file review, all the information related to a particular case (including CCTV) will be taken into consideration. Disposal decisions on elements within the file will be taken by the reviewing officer in accordance with the National Retention Assessment Criteria and recorded.

- Intelligence - CCTV data or stills derived that only contain material which is of intelligence use should be retained until the intelligence is of no use, or the information has been transferred to other systems.

- Management Information - CCTV data or stills derived for management information (i.e. custody) should be retained only as necessary for this purpose, and routinely for no more that one year. However there may arise some circumstance where information of this type requires extended retention periods. If that is the case the criteria will be set by the MOPI Review, Retention and Disposal process.

Retention of images relating to undetected crime

3.5.5 Images associated with undetected crime should be retained according to Management of Police Information (MOPI) principles. For example, records including associated evidential images, relating to undetected crime, as defined in the Criminal Justice Act 2003, should be retained for six years for standard offences and ten years for serious offences before the MOPI review takes place to assess for further retention.

3.5.6 When retaining undetected crime records, consideration should be given to ensuring that records are easily retrievable and accessible for replay and viewing, and an assessment of the possible value of the information to future cases should be made.

Retention of images relating to detected crime

3.5.7 Where CCTV data is no longer required for an investigation it should be returned to the owning rail company/tenant or organisation/individual who had originally supplied the images to police.

3.6 Reliability & Availability

3.6.1 If data is handled and stored correctly, it should prolong the life of the media to ensure that it is fit for evidential use. Where the preservation of the information contained is an analogue (VHS) tape and it is considered to be of high importance consideration should be made to transfer the information to digital information (DVD), (Assistance in carrying out this procedure can be obtained by contacting your local CCTV video unit), where long term preservation is more desirable.

3.7 Continuity & Security of Data

3.7.1 Images are treated no differently in principle from any other form of information. CCTV data should be afforded the same level of physical security as would be the case for any other evidential exhibit. (For example, it would not be appropriate to send a bloodied knife in the post to Scenes of Crime, and likewise it is not appropriate to simply a post CCTV images in the post on the CD to a video suite). The Government Protective Marking Scheme (GPMS) should also be adhered to as it may be that some images, in particular high level Special Branch images could attract a SECRET marking.

3.7.2 When an officer takes possession of a CCTV data recording, a statement of continuity is required from the system operator. (Refer to the CCTV Data Collection & Retrieval SOP for more details). When handling CCTV evidence, continuity must be maintained at all times. The transportation of any master CCTV data is not permissible other than where continuity can be proved. For the purpose of continuity, a written log of every movement of the data should be kept recording the time the CCTV data was moved and who moved it. All entries are to be countersigned by a witness. A record of the identity of those who have viewed the video data and the viewing conditions should be kept.

3.7.3 For further information on continuity, refer to the Minimum Standards of Investigation SOP (D55270), the Property SOP (D90296), CCTVSOP2 – CCTV Data Collection & Retrieval and CCTVSOP3 – CCTV Processing.

3.7.4. Security of data will depend on the grading applied under the Government Protective Marking Scheme. In the main, most evidential data will attract a protective marking of RESTRICTED. However evidence or intelligence connected to serious offences or Regulation of Investigatory Powers Act authorizations should be assessed using the guidance available on the Information Security Intranet page or advice from the Regional Information Security Officers.

3.8 DISPOSAL OF DATA & AUDIT TRAIL

3.8.1. Disposal is the removal of information from all police systems so that it cannot be restored. In the case of images stored in IT systems this should mean that any police officer or police staff member should not be able to locate an image or piece of information when carrying out their normal duties. Deletion should normally suffice. In addition, any audit record which holds any personal information as defined by the Information Commissioners Office and is linked to the information or image should also be subject to disposal.

3.8.2. When original property recovered or seized is no longer required for police purposes, it must be disposed of to the rightful owner or his nominee without undue delay as well as any other linked information. Consideration should be given to obtaining a disclaimer from the owner when seizing property initially especially when police are using master tapes / disks from TOC's or other third parties, this will enable early disposal of such items when no longer required - direct by the Force.

3.8.3. Data, which has been seized, but not used, should be returned as soon as possible. Property belonging to one of the Railway Businesses should be returned to the appropriate department for degaussing and either reuse or destruction.

3.8.4 Electronic images that have been processed by BTP will have an audit trail in terms of metadata. Metadata is information relating to the image data. It refers to that which is automatically generated by the capture device and/or subsequent indexing application. This may include, but is not limited to:

- Time and date of image capture
- Camera number and location

- Software owner
- Version of data
- Protective marking
- Disposal/review date
- Location and date of offence
- Offence/Crime group
- External reference numbers
- Associated nominals version

3.8.5 Metadata is important as it enables users to retrieve data and identify future disposal needs and identifies ownership, which assists with disclosure and Freedom of Information enquires.

3.8.6 Metadata associated with capture may be integral with the image file (often leading to a proprietary format). It is imperative that all metadata is retained and managed in a way that ensures its reliable association with the relevant image.

3.8.7 All images must have an audit trail associated with them (see ACPO (2007) practice advice on police use of digital images). This will include the metadata and, if the images have been processed, a history log.

4 MONITORING AND COMPLIANCE

4.1 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.