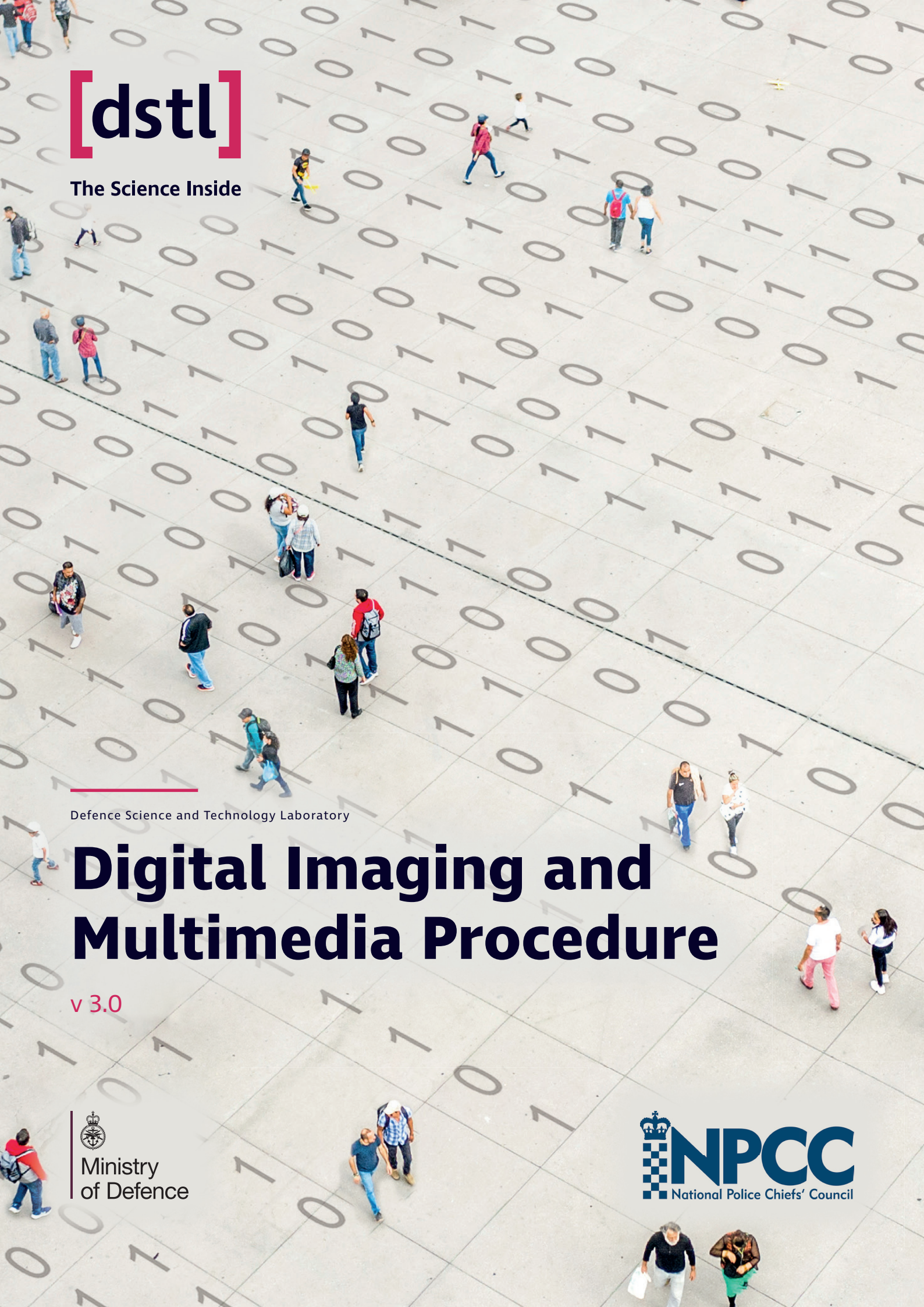


[dstl]

The Science Inside

Defence Science and Technology Laboratory

Digital Imaging and Multimedia Procedure

v 3.0

Ministry of Defence

NPCC National Police Chiefs' Council

Digital Imaging and Multimedia Procedure v3.0

2020

Ken MacLennan-Brown
Neil Cohen

With acknowledgement to Jim Aldridge and the project team who developed the original Digital Imaging Procedure on which this publication is based.

DSTL/PUB127782
PolicingAndSecurityEnquiries@dstl.gov.uk

Contents

Foreword

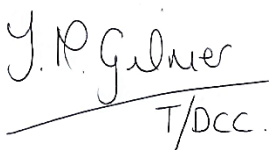
Digital imagery, and the audio frequently associated with it, is now an intrinsic part of everyday life and is a key enabling technology for the Police Service and public alike. With this in mind it was time to revise the Digital Imaging Procedure, first published in 2002 and last updated in 2007. The aim of this latest version is to build on the successes of the original document and not only reflect current advances in technology, but also look to the future. The purpose of the procedure remains the same, i.e. to detail the processes involved in the proper capture and handling of digital data for police applications and to define best working practice. The target audience also remains broad, encompassing operational, administrative and judicial staff involved throughout all stages of the Criminal Justice System (CJS).

The key to the process is the creation of an identifiable, isolated and suitably stored Master reference copy at the earliest opportunity. The exact method of storage is unimportant provided it can be shown that the Master is unchanged from the moment of its definition. With current data trends and retention timescales the most suitable long term solution is a secure network environment.

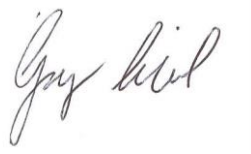
This procedure enhances the integrity of proper evidential gathering processes whilst reducing the risk of malicious manipulation. Every effort has been made to keep the document as generic and technology neutral as possible, however specific technologies and processes are addressed as necessary and reference given to sources of more in-depth advice.

Digital imaging has enormous benefit for the swift and accurate outcome of investigations, particularly given the fuller use of network technologies. Whilst such technology has a price tag in terms of infrastructure and skilled technical support, this is an enabling document that allows for the adoption of suitable technologies as the opportunities present themselves.

We expect that operational implementation and court proceedings will continue to refine some of the procedures set out in this document, although the framework itself is considered robust and defensible, and has been widely adopted since its original publication in 2002. The information contained in this procedure has been derived, developed and reviewed through wide ranging consultation with practitioners from the Police Service and related CJS organisations, as part of the NPCC national CCTV working group, and supports the SCC Codes of Practice. We commend it to forces and other organisations for adoption as current ‘best practice’.



T/DCC Jenny Gilmer
South Wales Police
NPCC Lead for CCTV



Gary Aitkenhead
Chief Executive
Dstl

Introduction

The Digital Imaging and Multimedia Procedure is a guide for those practitioners within the Police and CJS who are involved with the capture, retrieval, storage or use of evidential digital images, and associated audio and metadata, either generated by the police themselves or recovered from witnesses under the CPIA (Criminal Procedure and Investigations Act 1996). When applied to equipment seized under PACE (Police and Criminal Evidence Act), further safeguards may be required. It is focused around a flowchart that guides the reader through the process from the initial preparation and capture of images, through the transfer and designation of Master and Working Copies, to the presentation in court and finally the retention and disposal of exhibits. Supporting notes are provided for each step in the flowchart. For the purposes of this document the term image can be used interchangeably for either still images or moving image sequences.

This version (v3.0) of the Procedure maintains the overall structure of the preceding editions, but has been updated in three key respects. Firstly, it is recognised that there is now a broader range of technologies available for the capture and storage of digital imagery, which frequently has associated audio and metadata. Hence the broadening of the document title to explicitly include the term multimedia. Secondly, it is recognised that the police increasingly realise the benefits of storing Master and Working Copy data on a secure server, instead of physical WORM (Write Once Read Many) media such as CDs and DVDs. This secure server environment is often configured as a DEMS (Digital Evidence Management System) or DAMS (Digital Asset Management System). Both server storage and a move away from physical exhibits brings many advantages but also raises questions around integrity and tampering. This concept of the evidence being separable from the media and steps to preserve its integrity and authenticity are addressed in this document. Thirdly this document also reflects the changes in data protection legislation, Protection of Freedoms Act and other relevant codes since the previous version.

This procedure should be read in conjunction with the Information Management Authorised Professional Practice (APP), CPIA Code of Practice, the National Disclosure Standards, Disclosure Manual, and the Protocol between the Police Service and the Crown Prosecution Service (CPS) on dealing with third party material which provide further information on the roles and responsibilities of the police and the prosecution. Also of relevance is the Control of Data section of the Forensic Science Regulator's Codes of Practice (Section 23 in Issue 5, plus subsequent amendment Notice 02/2020).

The bulk of this document comprises notes that should be read in conjunction with the flowchart on the back page. However, there are several issues that are not covered within the Procedure itself. These are introduced and discussed briefly in this section to answer some frequently asked questions about digital image evidence.

What is the evidence?

Evidence, in terms of still or moving image data, and/or related audio data, and associated metadata is the presentation of facts about the crime or an individual that the prosecution presents to the court in support of their case. The image data could be presented either as hard copy or on a screen, with or without audio. The evidence is not normally all the data contained on the recording device but a sub-section of it. For these reasons the term 'image file' refers to an image or video stored electronically, not a forensic disk image of a drive or folder.

As it is possible to make a bit-for-bit identical copy of digital image data, in evidential terms there is no distinction between the copy and the primary or original data because the data are the same and have the same evidential weight. It is not important whether the data is on a stand-alone or networked computer, a server, or on any type of storage medium. This assumes the operation of adequate security against unauthorised and unrecorded access, with appropriate traceability.

The core principle of this document is that there is a definitive copy of the data (Master Copy), 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. In either case the principle stated above and the conditions below apply. If no discipline is applied there can be any number of identical files. For evidential purposes it is essential to be able to demonstrate that the images are authentic and are a true representation of the data captured in the originating device and recorded to the first medium.

The Master must be:

- labelled or named (with due care to the longevity and readability of label and of medium)
- preserved in a form and manner, with software if required, so that the images may be viewed in the future
- Stored in a manner that prevents alteration or accidental erasure; this can be by either physical or electronic means
- kept in accordance with exhibit protocol[1], see
    - Criminal Procedure and Investigations Act 1996, Code of Practice, Section 5a - Retention of Material
    - Management of Police Information (MoPI)
    - CPS/NPCC Guidance Regarding the Storage, Retention and Destruction of Records and Materials that have been Seized for Forensic Examination and
- not used, except to make further copies, in whole or in part, together with appropriate audit trail, or by order of the court to verify authenticity. If viewed directly, suitable write-protection must be in place.

[1] Where material has been seized in the exercise of powers of seizure conferred by the Police and Criminal Evidence Act 1984, the duty to retain it under this code is subject to the provisions on the retention of seized material in section 22 of that Act.

Force policies should be developed to cater for these requirements.

Furthermore the Master files should be in the same format as:

- received by the force in the case of third party images
- first captured on medium in/or attached to camera
- recorded after transmission from camera.

Where a DEM or DAM system compresses or transcodes files on ingest, this would preclude its use for Master storage.

The Master should be designated at the point at which the data is under police control and has been stored according to the conditions described above. This may be on physical media but is increasingly likely to be some form of networked storage. There is no requirement for the Master to be on physical media if these conditions have been met.

There may be intermediate steps between the initial capture and the designation of the Master Copy, involving for example transmission or the use of a transfer medium (see Section 4, Transfer and Transmission).

There must be an accompanying audit trail showing its provenance (see Section 2). Audit trails can be written, electronic or a combination of both and may incorporate information automatically generated by the hardware or software used to store or process the data. Electronic audit trails if available can augment or replace the written audit trails.

Digital image and audio data is stored in a vast array of different formats and variants of formats of varying quality levels. Some lower resolution digital images displayed on a computer screen or as hard copy might not appear very lifelike but then neither do many simulations. The important and overriding factor is that the content of the image should be fit for purpose and that the quality is adequate. To this end for reproduction and viewing the use of desktop printers for hard copies of stills and low resolution video footage should not be ruled out. It is not always necessary or feasible to produce the highest quality images to demonstrate the facts required for evidence. However any known reduction in quality should be disclosed and audited in order for the court to assess evidential weight. Any consideration of whether an image is fit for purpose should fully take into account the uses to which it may be put, in particular whether it is likely to be subject to forensic analysis, in which case the highest quality native format should be available, with any associated metadata.

Image and audio capture devices use a multitude of complex processing techniques to combine the signals received into a representation of the event. These representations are admissible as evidence and the digital storage of them does not alter that.

Compression

There are various compression algorithms used to reduce the amount of data in a file to cut both storage capacity and transmission bandwidth requirements. All compression algorithms remove data from the file and some are more effective than others at reconstruction of the data for replay. Generally, the greater the compression ratio, the more seriously affected is the replay.

If image or associated audio data is being presented as evidence and illustrates the facts of the offence then it is evidentially irrelevant whether the data has been compressed or not. What is important is the content of the data should be fit for purpose and that the quality is adequate. It should be noted that various transmission methods used throughout the capture, retrieval and replay chain may adversely affect the quality of the data and steps should be taken to mitigate this.

Some compression algorithms are more suitable for fast movement, some for ‘talking heads’ scenarios. The compression can produce some artefacts which may mask the information or contaminate it with movement, patterns, outlining, etc. Where the capture, conversion or transmission is under police or CJS control the algorithm must be tested on typical scenes. The image quality must be agreed and performance tests carried out to ensure suitability. Image processing cannot make up for inadequate data. Images should not be excluded because they are compressed and whilst there may be reasons to prefer some algorithms for reasons of quality, there is no reason to exclude any from evidential material.

File format

Digital data files can have a variety of formats. The still camera industry is mostly using widely supported (or open) formats (TIFF, JPEG) although their highest resolution images are often in their own proprietary (raw) format. This may mean these latter images have to be downloaded in a proprietary software package. An open format allows for ease of incorporating images into publications, printing and transmitting to others, but will be a representation of the data held in the raw file. Generally raw files are read only with any changes either saved to an .XMP sidecar file or the processed result to another file format.

Currently digital handheld video cameras mainly record to Solid State memory (SD and its variants, CompactFlash, XQD, etc.). The market seems to be stabilising around fewer formats, but faster read/write speeds and ever larger capacity are still the trends. Large amounts of video are now shot on mobile phones and stored on their internal drives, though some offer external storage options, including cloud storage.

The manufacturers of closed circuit television (CCTV) video recorders use a multitude of open, proprietary and mixed compression formats to meet the needs of massive amounts of data versus the cost of storage. Again the format is not relevant to the admission of the evidence, only that the quality is fit for purpose.

Many file formats record metadata along with the content, commonly time and date information but potentially many other fields that may be of value, if accurate. Metadata is often lost if files are converted between formats.

Server Storage

Server storage has many advantages particularly with regard to long term storage. The data can be migrated automatically and with no loss should a more effective media become available. Also server storage is more fault tolerant; failures within a RAID array can normally be rectified with no loss, ensuring that the data is accessible, as compared with a CD or DVD where once it has been noticed that the media has failed it is usually too late. Increasingly police services are deploying a DEM or DAM system that is capable of suitably storing Master evidence and providing output for court in an appropriate format.

Cloud based storage is a variation on server based storage, where the storage may be provided off-site by a third party, and has its own set of problems and advantages. These must be carefully considered and steps taken to mitigate perceived risks before this route is chosen. Cloud services may or may not be geographically located within the force area, and the implications of this need to be considered. For further information see the National Cyber Security Centre's Cloud Security Principles. Also of relevance is the Control of Data section of the Forensic Science Regulator's Codes of Practice (Section 23 in Issue 5, plus subsequent amendment Notice 02/2020, in particular paragraphs 23.3.30-31).

The use of a cloud or server system for secure storage of evidence should be accredited by the local force Information Security Officer, as per the Information Assurance section of the Information Management APP.

Integrity Verification vs. Authentication

These two terms are frequently confused and often misused[2].

- 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, a change to the clock on a CCTV system could affect the image authenticity but not affect the image integrity. Robust audit

[2] Definitions taken from SWGDE (Scientific Working Group on Digital Evidence) Digital and Multimedia Evidence Glossary Version 3.0 June 2016 https://www.swgde.org/documents/published

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.

Data Protection

Care should be taken to ensure that the processing of personal data complies with UK data protection law. UK data protection legislation is designed to protect the rights and freedoms of individuals and is outlined in both the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA2018). The Information Management APP incorporating MoPI (The Management of Police Information provides further detail on how the DPA2018 applies to the processing of personal data for law enforcement purposes.

Forces should be aware that many of the safeguards employed in this procedure are the same safeguards that will allow them to comply with their obligations with under the DPA2018. It's also important to note that whilst many of the requirements of the GDPR will be relevant, the provisions for processing personal data for purposes of law enforcement are set out in section three of the DPA2018. The following data protection principles (described in part three, chapter 2 of DPA2018) are most relevant when handling digital images and evidence;

- Principle 3 (Relevance) - Data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Principle 5 (Retention) - Data should only be retained for as long as it is necessary for the purpose it was originally collected. Policies should be in place setting out standard periods of retention.
- Principle 6 (Security) - Appropriate security measures should be in place to protect personal data.

It should be noted that the requirements of Principle 5 (Retention) must be harmonised with the retention requirements in the CPIA and Information Management APP.

Protection of Freedoms Act 2012

The Protection of Freedoms Act 2012 require the police to pay due regard to the Home Secretary's Surveillance Camera Code of Practice. Failure to do so is admissible in criminal and civil proceedings and the Crown Prosecution Service Disclosure Manual reflects this. The focus of the Code is on the operation of surveillance cameras however parts are relevant here, in particular:

- Principle 11 – When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

Preparation

These elements of the procedure include the preparatory steps before images are captured. This may be directly before the images are taken, or at an earlier stage or date where work can be anticipated. The steps identify the importance of:

- obtaining relevant authorisations;
- starting an audit trail at the earliest opportunity when it is known that the images are to be captured; and
- checking equipment, either routinely or at the commencement of the image capture activity.

Such checks will avoid the reputational damage of failure and/or challenges about conformance with an accepted procedure. Digital image capture systems may increasingly be used by non-specialists in operational situations and locations so adherence to an established procedure will assist in safeguarding those captured images.

Obtain authority [1]

This instruction applies to all image capturers, who by virtue of their role or position within the Police Service are empowered to capture images for the purposes of their particular work, where trained or deemed competent. Specific roles and responsibilities, for example for a Scenes of Crime Officer or a Collision Investigator, will be written into their job descriptions, training and instructions together with any verbal instructions. Obtaining authority is not necessarily required for each separate operational task.

However, Police Forces need to be aware that authorisations do need to be in place before data is taken, for example authorisation to permit images to be taken where ‘Directed Surveillance’ is requested under the Regulation of Investigatory Powers Act 2000. That authority must be obtained and recorded within the audit trail of the operation. Further restrictions and/or authorities may result from Data Protection legislation. It is the responsibility of the person obtaining the data to ensure all required permissions are obtained and that all legislation is adhered to.

At this point the first three principles of the DPA 2018 Part 3 Chapter 2 are particularly relevant. In summary:

- Principle 1 - the use of the data must be lawful and fair.
- Principle 2 - the use to which the data will be put must be specified, explicit and legitimate.
- Principle 3 - the amount of data retrieved must be adequate, relevant and not excessive.

Start audit trail [2]

One of the fundamental requirements of digital imaging is the need to safeguard the integrity of images; part of this process involves an audit trail being started at the earliest stage. This may be as a written audit trail, and/or incorporate an auto-generated electronic audit trail mapping the movement and changes of files on computers. When relating to third party images, the audit trail should begin at, and detail, the point of transfer.

This Procedure relies on the written audit of activities. The audit trail should include the following information (with date and time of action) when available and if appropriate:

- Details of the case;
- classification of the image(s) (and any special handling instructions, if relevant) and the name of the person who classified the image;
- If the image is third-party generated, information about point of transfer including whether the image is the Master, a Working Copy or an exhibit derived from a Working Copy;
- Information about capture equipment and/or hardware and software used, including details of the maintenance log relating to capture equipment and calibration of hardware and software;
- Identity of the capture operative including third parties and image retrieval officers, where applicable;
- Where third party data is requested;
    - Letter to third party
    - Explanatory note
    - Third party response letter
- Details of exhibits and disclosure officer(s);
- Description of the images captured, including sequencing;
- Details of retrieval or seizure process and point of transfer, if applicable;
- Creation and defining of the Master Copy and associated metadata;
- Storage of the Master Copy;
- Any access to the Master Copy;
- Viewing of the Master and Working Copies, including a record of any associated viewing logs;
- Details and reasons for any selective capture;
- Any editing applications which may alter the image;
- Any details of processing applications allowing replication by a comparatively trained individual;
- Electronic history log of processing applications;
- Any copying required to ensure preservation and longevity of the data;
- Revelation to the CPS of the Master and Working Copies;
- Any copying carried out as part of a migration strategy to ensure the replay longevity of the image;
- Disposal details and retention time periods.
- Hash value or equivalent at point of receipt

- Reason for collection or receipt of the imagery

The practices may not be familiar where imaging is a new feature of the work and it may be worthwhile to consult the Forensic Support Manager or equivalent adviser.

Check operation of equipment [3]

The correct operation of any equipment is essential to gathering evidence.

In particular it is suggested that checks are made to ensure that:

- operator adjustable settings are made appropriately;
- the time and date settings are correct;
- there are adequate supplies of recording media, including spares in case of media failure;
- the media should either be new, reformatted or sanitised in a suitable manner, according to force policy;
- any media protection settings will not prevent recordings being made;
- if the equipment is battery operated, there are sufficient fully charged batteries available;
- a scheme of checks is carried out before deployment particularly for equipment that is used less frequently;
- Ensure DEMS or DAMS are capable of receiving the data in the required format.

It is essential that time and date settings are correct, any inconsistencies should be documented and the equipment monitored to ensure that further drift of these settings does not occur.

This list is not definitive and detailed information should be obtained from the equipment manuals.

Specific advice relating to re-using USB thumb drives is given later in this document.

Capture, Protection and Storage

Police-originated images

These steps cover the capture of still or video images onto the chosen medium with due regard for the image quality and integrity of the images.

Third party origination

This section should be read in conjunction with the Protocol between the Police Service and the Crown Prosecution Service (CPS) on dealing with third party material, which provides further information on the roles and responsibilities of the police and the prosecution.

The Procedure diagram should be used to establish the 'point of transfer' at which the responsibility for the handling of third party images transfers to the police. That 'point of transfer' will depend on the nature of images being transferred, the recording format and equipment used by the third party. At whatever stage this 'point of transfer' occurs the police audit trail must start. Continuity of image handling should be demonstrated throughout by ensuring that the police audit trail links directly to any audit trail that is available from the third party. Some imagery may have little or no provenance i.e. images uploaded to the police website by members of the public in response to an appeal. This imagery must be treated with caution until its authenticity and integrity can be verified.

Third party image systems

Town centre CCTV cameras, for example, should follow established and standardised procedures and comply with the Surveillance Camera Commissioner's Code of Practice. These systems should allow the police to;

- take receipt of evidential recordings in order to safeguard them;
- replay the recordings in order to view and copy them;
- make authentic (not materially different) copies in formats suitable for use by investigators, Crown Prosecution Service (CPS) and the courts; and
- access viewing facilities if the original recording has to be viewed.

Whichever still or video camera or format of medium is chosen for the capture and initial storage of images, effective means must be available for transferring the images to the computer system where they are to be used and possibly archived.

It is becoming increasingly common for the police to be granted remote access to systems either on a permanent or ad hoc basis. However, care must be taken to ensure all data protection legislation is adhered to and proper safeguards and necessary authorisations are in place before this facility is utilised. Service Level Agreements (SLAs) should be in place

between the police and local authorities to govern access to town centre systems. Live access to a town centre system may enable a level of surveillance of an individual that would require a Directed Surveillance Authority (DSA) under the Regulation of Investigatory Powers Act 2000. Data Protection legislation would be contravened by retrieving more information from a system than was necessary and agreed with the owner (DPA principle 3).

Take images. Do NOT delete images [4]

Capture

The image quality setting should be selected appropriate to the operational requirements rather than to minimise the storage capacity. Operators should anticipate their requirements and have sufficient empty storage media available.

Selective capture involves the switching on and off of recording devices and should not be confused with other editing processes.

Still images can be captured on many different types of camera using a multitude of memory storage devices/memory cards. The manufacturer's manual should be referred to for instructions on correct use of this equipment.

There are several technologies for capturing video images digitally. Each is illustrated in the Procedure:

- reusable, removable, media, for example memory cards
- computer hard disk drive (HDD)
- WORM (write once, read many times) media, for example CD-R and DVD±R
- Direct network storage
- magnetic tape – includes digital recording to conventional video tape, special digital video tape and data tape

Because of the high data rates associated with digital video, the image data is usually compressed in order to:

- reduce the stored data volume
- reduce the time taken to transmit and/or the transmission channel bandwidth
- lower the cost of storage media, for example by using low read and write speeds

Where image sequence(s) have come from a non-removable medium the Working Copy or copies could be made:

- at the same time as making the Master
- from the non-removable media after the Master has been made
- subsequently from copying the Master

Deletion of images

One crucial aspect of the Procedure is that none of the images obtained for the purposes of an investigation should be deleted without authority. This does not apply to images on a transfer medium which may be deleted once a Master Copy has been verified on more suitable storage. Any deletion of images, intentionally or accidentally, may be the subject of a 'challenge' or legal debate during any prosecution. Where such authority is given, deletions must be recorded in the audit trail and be subject to the requirements of the CPIA Code of Practice and Disclosure Manual.

In CCTV systems, video is recorded directly to an HDD, which is often designed to over-record automatically after a set period. Before this happens some or all of the images may be protected on the HDD preventing them from being overwritten.

Transfer and Transmission

In the simplest case, images will be transferred directly from the source to create the Master (e.g. copied from HDD to WORM). However, in some instances the images will be transmitted across a network or physically moved via an interim transfer medium. This may occur either at the point of capture (e.g. IP CCTV cameras) or during transfer from the initial storage medium to the Master.

The security, stability and longevity characteristics of different transmission methods should be considered and where necessary documented in the audit trail. This particularly applies to wireless transmission methods that may be susceptible to interception or unauthorised access, or transport media such as flash media that is prone to loss. This should also be considered when using wired network transmission, particularly if the internet forms any part of the network transmission.

The Master should be designated at the point a verified copy of the imagery reaches the optimum storage medium available, even if earlier stages are via media that is suitable to be designated as Master, e.g. if data were transferred via DVD to a secure server the Master would be designated on the server and the DVD could be destroyed. Figure 1, below, gives a graphical representation of this process.

Comprehensive audit trails are required in order to document the processes shown in Figure 1. In particular any transfer media must be uniquely identifiable, and suitable checks and verification carried out to ensure data integrity when transferring from the transfer media to permanent storage. These checks should be carried out at each transfer stage after the initial retrieval. A comparison of hash values such as MD5 or SHA-1 is an example of such checks.

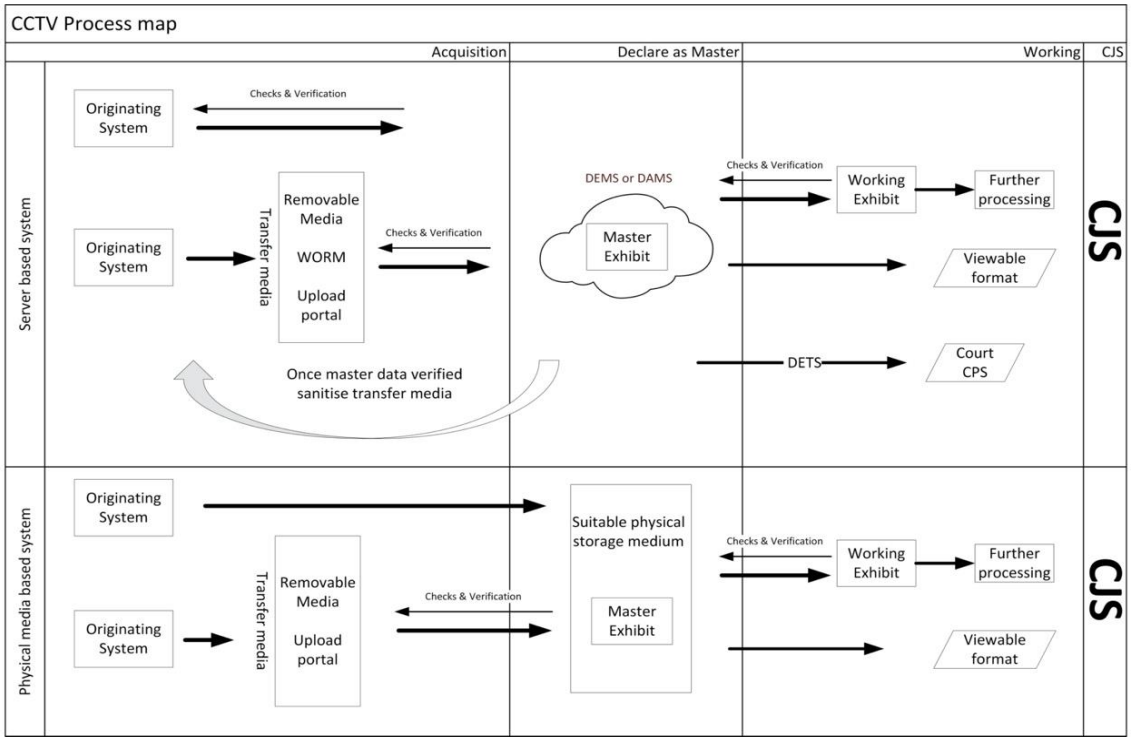


Figure 1: Transfer routes from recording device to court

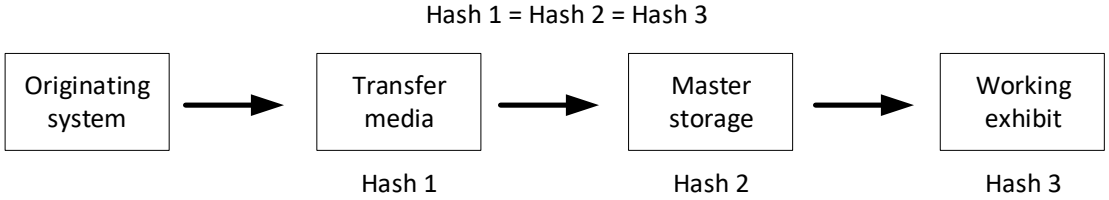


Figure 2: Data integrity checks

Figure 2 gives an example of how these checks would work in practice.

Protection, preservation and storage [5]

Images on reusable media should be copied from the original storage medium in the original file format onto secure media. This secure media could be WORM or secure network storage.

The generation of the secure copy should be carried out as soon as possible after the capture to reduce the time and opportunity for the accidental or malicious alteration to images.

All imagery Master or Working Copies should be appropriately identified in order to facilitate the storage, retrieval and eventual disposal of case material.

In terms of evidential value there is no difference between bit-for-bit copies of the data on the Master, Working Copies and the images on the storage medium. This does not remove the necessity to protect the Master as an exhibit in case of challenges to evidence handling procedures or image manipulation. It is suggested that the before and after hash value (MD5 or SHA-1) of a file is created, recorded and compared at any time it is transferred between media.

The correct software required for viewing proprietary formats must be available otherwise the images will be inaccessible. It is advisable to store any replay software with each recording to assist with the correct viewing of the files.

The choice of using network storage or WORM media is a matter for force policy and should be guided by factors such as volume of data, predicted storage time and longevity of WORM media. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs. Appropriate measures also need to be taken when the data has to be retained on a storage medium that is not WORM and can’t be write protected, for example drives from a CCTV recorder, or complete CCTV recording units.

Non-reusable removable medium (WORM) [5a]

Non-reusable removable medium technology includes CDs, DVDs, Blu-ray etc. They represent the theoretical ideal in that once closed the recording on the disk cannot be altered. However, optical discs are prone to damage that can make them unreadable and they do degenerate over time. In addition the computer industry is moving away from optical disc storage which places it at risk of becoming a redundant technology. For these reasons a DEMS or DAMS would be a better long term repository for Master evidence. If the Master is stored on such a system then the optical disc would be considered a transfer medium and could be destroyed (once a verified copy is on the DEMS/DAMS).

The WORM medium must be closed to prevent any of the image data files being subsequently changed and further data written to the disk. Optical disks (CD-R, DVD±R) must be 'finalised' or 'closed' in the camera or CD-writer before the disk is removed otherwise the images may not be viewable on a computer.

Video Data

To facilitate the use of the recordings for investigations and appeals, etc., the video data should be part of a package, containing the following information:

- clear identification of the image sequence or sequences
- an easily-read text file stating any requirements for special hardware or software for replay
- all associated metadata (time and date should be bound to the relevant images)
- licence-free software enabling the sequences to be viewed correctly

Other items that could be included:

- text data about the originating camera or system
- audit trails
- authentication or verification software
- short test sequence to confirm that the recorded image sequences are being replayed correctly
- Contact details for Force Information Security Department in case of media being lost / found

These items need to be robustly associated but may take many forms such as separate files, database entries, physical labels etc.

Still images

In general, still images are stored in widely supported formats and there is no need for viewing software to be stored with the images, but where proprietary formats are used then the viewing software should be included on the media in line with the information given above for sequences.

Storage

The WORM media can be stored as the Master. However, the creation of a network server based Master should be considered and may be preferable for reasons of storage efficiency or data longevity. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Reusable memory [5b]

These include solid state memory devices such as USB thumb drive, SD card CompactFlash, or any other reusable media such as CD-RWs and DVD±RWs.

Some imaging devices have the ability to set a flag preventing accidental erasure of images that can be helpful in some scenarios. Some media also has either a manual switch or protective seal that can be applied to prevent the disc overwriting; these tend to be easily reset or circumvented so should be used with caution.

Media cards may have to be formatted in the particular device, or in a particular file format prior to use otherwise they may not be useable. There is no universal format / file system that is readable by all devices, though some are more widely useable than others.

Reusable media particularly USB sticks and SD cards are now a cheap and common form of storage used across the range of imaging devices. This media is however, only designed for short term storage and any data stored on it is vulnerable to corruption or accidental deletion and therefore if practical should be transferred as soon as possible to secure storage.

Once images are transferred to the Master, the reusable medium must be reformatted / sanitized to remove all of the previous image files in preparation for reuse. This reformatting should be carried out in preparation for the work ahead and the officer should have sufficient empty media for such purposes. Reusable media cards should be erased / sanitized in accordance with force policy as soon as all data has been transferred. It is important to maintain traceability of media used particularly if it is reformatted and reused, in order to prove there is no possibility of cross contamination. It should be noted that whilst it is relatively easy to clear solid state memory so that no cross contamination of files could occur, in some instances remnants of files may still be recoverable using an intensive forensic data recovery regime. Re-usable memory has a finite lifetime related to use cycles and storage conditions. For this reason force policy should also stipulate a working lifetime for re-usable media.

Some imaging systems (e.g. third party CCTV recorders) cannot recognise encrypted transfer media; where it is necessary to export data to unencrypted media then suitable physical protection should be applied in order to achieve the same level of data security.

Storage

Reusable memory should be treated as a transfer medium and as such needs to be copied onto secure storage as soon as possible. Individual Force procedure will indicate whether WORM or secure server is the most appropriate route. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Network [5c]

It is becoming increasingly common for direct access to third party networks (e.g. corporate IP based CCTV systems) to be granted to the police. Images can therefore be retrieved directly from the third party network. This is also becoming prevalent with smaller scale installations and for standalone NVRs (Network Video Recorders) in small businesses and domestic premises. At the time of writing there has been a marked increase in single camera networked devices installed in domestic premises that can only be accessed remotely over an IP connection.

Corporate and or Local Authority systems that allow remote access are usually governed by an SLA that will set out levels of access. This is usually not the case with small businesses and domestic premises. In these instances careful consideration of the requirements of data protection legislation should be taken into account and force SOPs referred to.

Access to third party networked systems can be abused. Therefore the user ID and passwords provided by the system owner must be kept secure and relevant legislation complied with (Regulation of Investigatory Powers Act 2000, Investigatory Powers Act 2016).

The choice of whether to copy retrieved images to a secure police network or WORM media for final storage will be a matter for individual force procedure. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Secure Police Network [5d]

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.

Server storage has many advantages particularly with regard to long term storage. The data can be migrated automatically and with no loss should a more effective media become available. Also server storage is more fault tolerant, failures within a RAID array can normally be rectified with no loss, ensuring that the data is accessible, as compared with a CD or DVD where once it has been noticed that the media has failed it is usually too late. Increasingly police services are deploying a DEM or DAM system that is capable of suitably storing Master evidence and providing output for court in an appropriate format. Where a DEM or DAM system compresses or transcodes files on ingest, this would preclude its use for Master storage.

Cloud based storage is a variation on server based storage, where the storage may be provided off-site by a third party, and has its own set of problems and advantages. These must be carefully considered and steps taken to mitigate perceived risks before this route is chosen. Cloud services may or may not be geographically located within the force area, and the implications of this need to be considered. For further information see the National Cyber Security Centre's Cloud Security Principles. Also of relevance is the Control of Data section of the Forensic Science Regulator's Codes of Practice (Section 23 in Issue 5, plus subsequent amendment Notice 02/2020, in particular paragraphs 23.3.30-31).

If the data is captured directly onto such a secure server (e.g. ANPR) then it can be designated 'Master' in-situ and Working Copies created as required. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs. Further explanation of Master evidence is given in the "What is the evidence?" section. The requirements for Master evidence detailed there apply whatever type of storage solution is used.

Non-removable medium [5e]

Most non-portable storage solutions associated with imaging systems use non-removable media as their main storage type. This can range in size and complexity from a single HDD contained in a CCTV system through several HDDs arranged in a local RAID to vast numbers of interconnected drives used commercially for bulk data storage by one or more clients.

Because of the high cost and finite capacity of HDDs, images stored on them will usually be overwritten after a pre-set time or after the images have been transferred (backed-up) to some other medium for transport or archive. The back-up might be selective, by automatic or manual selection. It may be necessary to bring in specialists to ensure that the data is safeguarded. Any difficulties with obtaining evidential material should be referred to the force TSU or video units.

The normal mechanism for erasing data recorded on hard disks is to delete the directory entry only. The computer controlling the HDD then reallocates the space ready for a fresh recording. The new recording will then erase the previous recording by writing over the top of it and a new directory entry will be made. This means the data still exists and is recoverable until it has been overwritten.

When an incident or offence has occurred and there is a requirement to take information from the HDD as evidence:

- check whether the required data has already been copied to a back-up medium;
- check that what is needed is not being over-recorded while arrangements to save the data are being made;
- stop the recording process only if necessary to preserve the data – this may put the system out of action until the data transfer can be completed;
- be prepared to seize the entire system if necessary, and practical;
- transfer the data in a file format with software for accurate replay that can be used by the police, retaining original file format if possible; and
- transfer to a recording medium suitable for use by the police.

Storage

Data held on an HDD could be written to WORM, copied to a secure network, or the original system could be retained as the Master. Retention of the HDD alone is strongly discouraged due to the difficulties of data access and uncertainty of its lifespan. If it is necessary to seize a large amount of data from non-removable media then it may be impractical to transfer it to WORM, as it may take a considerable time to copy and require many disks. It should be noted that if the data is not transferred to WORM then write-blocking measures will need to be implemented before the HDD is accessed. Hardware write blocking is recommended as software write blockers can be

ineffective on non-windows compatible file structures. Furthermore, checks should be made to ensure that the data on the HDD is in a playable form, as an HDD from a CCTV system, for example, may not be readable on a standard computer.

It may not always be possible to make the Master directly from the HDD (e.g. a CCTV system with a network port but no CD writer). The data would first be copied to a transfer medium such as a laptop, from which the Master could then be created. Once the Master has been produced, the data would be deleted from the transfer medium. It may also be possible to utilise a network transfer directly from the recording system into a DEMS or DAMS. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Removable tape medium [5f]

There are several types of tape onto which digital video can be recorded, though this method is now largely obsolete.

Where the video footage has been recorded onto a digital tape in a handheld camcorder it was the policy to designate this video tape as the Master. With legacy systems such as these, however, it may be preferable to copy the data onto another media as the original may not be robust.

In the case of CCTV, the images may be recorded onto a data tape format. Digital Audio Tape (DAT) is one example. Whilst these tapes are removable it may not be feasible for the police to view the evidence without first transferring the data to another more convenient removable medium.

Where hard disk recording systems use tapes for back-up, the recording format may be non-standard to accommodate time lapse and multiplex recordings. These recordings will require special playback and copying facilities.

Copy recordings, whether from analogue to digital or transcoded from one digital format to another will often result in a marked drop in quality and often cause the loss of metadata.

As soon as an evidential tape has been removed from its recording device, the write-protect mechanism should be activated where available. It should be noted however, that this will not prevent damage or erasure due to careless handling, proximity to magnetic fields or poor storage conditions, etc.

Storage

Whilst it is most likely that digital video tape will have its write protection enabled and be designated as Master, the option exists for a Master to be created on a WORM medium or secure network storage.

If imagery stored on data tape is to be transferred to secure network storage it must be ensured that the data is in a replayable form or the software required to access it is available and capable of reading the data from its network location. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper proof usage logs.

Supplementary protection

There are various media on which images can be captured, both reusable and non-reusable. Irrespective of their nature, early transition from ‘capture’ to ‘defining the Master’ phases is extremely important. The integrity of images needs to be protected at the earliest stages as this reduces the opportunities for challenges at court.

Alteration or erasure could be detected by noting image number sequences or MD5# values and must be prevented by at least one of the following means:

- designating the file as read only;
- Storage in an access controlled, write protected area of the server/DEMS/DAMS
- transferring to WORM media
- only accessing via a write blocker

Protection can also be achieved by controlling access to the file or media by electronic password and/or controlling the viewing of images by electronic encryption.

The Procedure does not rely on any form of electronic protection but neither does it preclude its use. There are several methods for electronically authenticating an image file. Once applied, any change to the pixel values will be detected although the nature and location of the changes may not be indicated.

File integrity techniques

If a ‘hash’ function is applied to an image, a unique numerical value is calculated for the whole image. The number can be embedded in the metadata of the image file or stored separately. A change in pixel value causes the hash function value to change. This is the basis for most authentication software. Manufacturer specific software for image authentication is becoming increasingly prevalent, as are non-destructive (i.e. fully reversible) editing techniques.

Watermarking

Watermarking describes visibly insignificant changes made to the pixel values to incorporate information which changes if the image file is altered. The watermark may then become visible on the picture or even make it unreadable.

The primary use for watermarking is to protect the intellectual property rights of the photographer or film maker. Its use may lead to claims that the image is not authentic because the pixels have been changed, therefore the use of watermarking is not recommended for image integrity.

Overt watermarks may be added to copies of images that are being shared, to maintain traceability or to limit further use.

Encryption

The image file or indeed the whole drive can be encrypted so that the file cannot be opened except with the correct decryption key. This has particular value if images are to be transmitted to or from remote sites. Encryption does not change the data contained within the file. Loss or corruption of the encryption key may make files unrecoverable. Encryption systems that progressively decrypt on demand, rather than decrypting the whole file prior to replay may affect image quality on replay systems with low processing power.

Some systems will employ a form of encryption known as Digital Rights Management (DRM) that prevents access to the file without the correct credentials.

The use of electronic protection is mandatory in the digital imaging used for roadside cameras where there is unattended capture, the image is the only evidence of an offence having taken place and the images are transmitted from the roadside to a central facility. Refer to Home Office and ACPO Traffic, Outline Requirements and Specification for Automated Traffic Enforcement Systems, S Lewis, PSDB 3/96[3].

Handling

Images should also be protected from accidental deletion by the careful handling of media. Media should be stored in clean, dry environments and kept away from strong magnetic fields, strong light and chemical contamination.

Some media such as CDs and SmartMedia will be damaged if allowed to become dirty or scratched.

[3] As amended by 'Requirements for the Remote Recording from and Control of Unattended Home Office Type Approved Traffic Enforcement Devices' by Dr S R Lewis, PSDB 25th July 2002
and 'Home Office Requirements for the Protection of Digital Evidence from Type Approved Automatic Unattended Traffic Enforcement Devices' by Dr S R Lewis HOSDB 12th October 2005.

Use

The Master is defined and will be documented as such. It will then be stored securely pending its production (if required) at court as an exhibit. Only in the event of any doubt being cast on the integrity of the images will the Master (or a verified bit for bit copy thereof) be viewed.

A Working Copy is usually produced simultaneously, or immediately after the Master is defined. The Working Copy, as its name implies, is the version that will be used for investigation and to assist in the preparation of the prosecution file.

All use and movement of the Master will be logged in the audit trail. Similarly any significant use, enhancement and distribution of Working Copies should be logged. The aim is to support the presentation of evidence through legal proceedings. All audit trails should be disposed of when the image files and any analogue copies are disposed of.

Define Master and produce Working Copy [6]

The core of the Procedure is the production, definition and storage of a Master which can be examined if required by the court to confirm the authenticity of the images. The Master must be:

- labelled or named (with due care to the longevity and readability of label and of medium)
- stored in a form and manner, with software if required, so that the images may be viewed in the future
- Stored in a manner that prevents alteration or accidental erasure; this can be by either physical or electronic means
- kept in accordance with exhibit protocol[4], see
    - Criminal Procedure and Investigations Act 1996, Code of Practice, Section 5a - Retention of Material
    - Management of Police Information (MoPI)
    - CPS/NPCC Guidance Regarding the Storage, Retention and Destruction of Records and Materials that have been Seized for Forensic Examination and
- not used, except to make further copies, in whole or in part, together with appropriate audit trail, or by order of the court to verify authenticity. If viewed directly, suitable write-protection must be in place.

Force policies should be developed to cater for these requirements.

Furthermore the Master files should be in the same format as:

- received by the force in the case of third party images
- first captured on medium in/or attached to camera
- recorded after transmission from camera.

If the Master is to be stored utilising a DEMS/DAMS or similar system the Master would be defined at the point it is ingested into that system. This would require an audit trail referencing any and all transfer media deployed in the process and verification of file integrity through each step (e.g. by comparison of MD5# values).

In other cases a Master needs to be defined on the media dictated by force policy. This can be done by:

- making two copies simultaneously and defining one as the Master and the other the Working Copy
- making two copies, consecutively and defining one as the Master and the other a Working Copy
- making one copy, the Master, and making a Working Copy from that Master

[4] Where material has been seized in the exercise of powers of seizure conferred by the Police and Criminal Evidence Act 1984, the duty to retain it under this code is subject to the provisions on the retention of seized material in section 22 of that Act.

Working Copies can be in many forms. The files can be copied onto any suitable medium or distributed electronically (if a secure system is in place) for circulation to the investigating officers and CPS. Issues of quality control, security and resource management need to be considered. The Forensic Science Regulator (FSR) requires that all exhibits need to be uniquely identifiable by reference and description[5].

[5] Forensic Science Regulator, Codes of Practice and Conduct, Section 24, Handling of Test Items

Document and securely store Master [7]

The Master is defined, will be documented as such and retained in secure storage as an exhibit for court purposes.

Local force policies need to be established to ensure that the integrity of the data is maintained throughout the storage, to include the period before, during and after any court proceedings during which the images might be used.

There will be times when the Master may need to be viewed and/or a fresh Working Copy produced. Force policy needs to be developed concerning this access. Whether this storage is on a physical, separate piece of medium such as a tape or disk, or on a networked location such as a DEMS or DAMS, procedures will need to be in place to maintain the integrity of the Master. The location and any access to the Master or movement of the Master should be recorded in the audit trail.

Whatever form the Master takes it is essential to label it adequately, protect it from damage and contamination and store it securely. For physical media this could be a room or locked cabinet which should have a clean dry atmosphere with temperature variations limited to normal room temperatures to prevent condensation. Storage servers generally have similar environmental requirements, though often need more extensive artificial means to maintain them.

Retain as exhibit [8]

The Master should be labelled, protected and stored in accordance with force procedures in order to fulfil statutory requirements.

Audit trails started at the outset of the image capture process should be completed and documented contemporaneously. A similar process may be necessary for those Working Copies that may be produced as evidence.
All images obtained in the course of an investigation are subject to retention rules laid out in[6]:

- Criminal Procedure and Investigations Act 1996, Code of Practice, Section 5a - Retention of Material
- Management of Police Information (MoPI)
- CPS/NPCC Guidance Regarding the Storage, Retention and Destruction of Records and Materials that have been Seized for Forensic Examination and

and Data Protection legislation (see Data Protection section).

[6] Where material has been seized in the exercise of powers of seizure conferred by the Police and Criminal Evidence Act 1984, the duty to retain it under this code is subject to the provisions on the retention of seized material in section 22 of that Act.

Produce Working Copies [9]

Once the Master has been defined and stored, all use of images should be from a Working Copy. Bit-for-bit copies should be used (where possible) for further reproduction of additional Working Copies or where precise detailed analysis is to be carried out or when images are to be enhanced.

Where further analysis is undertaken, the Video Analysis Appendix to the Forensic Science Regulator's Codes of Practice should be complied with.

The Master should not be used, except to produce additional Working Copies when no other Working Copies are available to copy, or by order of the court to establish authenticity. Force procedures will need to detail the circumstances and the relevant processes involved. All actions will need to be entered in the audit trail.

Working Copies produced for the investigation, technical investigation, briefings, circulation, and preparation of prosecution evidence and defence can be in any of the forms described:

- Digital file
- Hard copy stills from still or video cameras
- Edited video
- Enhanced still or video
- Converted to non-proprietary format

This list is not exhaustive and other media may be utilised if suitable technology is available. The copying and distribution of Working Copies should be in accordance with force procedures with appropriate audit trails as required.
The copying of files within a computer is easy and so needs to be disciplined to prevent unnecessary files being produced.

It is not suggested that all Working Copies should require individual audit trails, although certain application specific situations and/or enhancement processes e.g. identification will require audit trails to be maintained for additional Working Copies. Where this is the case records need to be kept contemporaneously. Working copies should however be uniquely identifiable. Reference should be made to individual force procedures.

Prepare prosecution file [10]

Officers responsible for file preparation should:

- ensure that the Master is kept in suitable and secure conditions by the police and copies made available to the prosecution or defence, upon request;
- Be cognisant of any redaction requirements where personal data is not to be shared with defence or third parties.
- liaise with the relevant CPS prosecutor at an early meeting to discuss the processes and capture systems used, where relevant;
- provide the CPS with full information accompanying any evidential digital images, this might include audit trails, maintenance logs, viewing logs and disclosure schedules;
- list and describe any unused and/or un-viewed material clearly;
- ensure that viewing logs used for moving images highlight relevant sequences;
- provide the CPS with accurate information about the preferred format for revelation in order to reduce the loss of image quality;
- consider the format in which the image is provided to the CPS in order to facilitate viewing and replay;
- liaise with relevant departments within the CPS to ensure that viewing and replay is possible prior to trial. It should be noted that it is often not practical to play the native format at court.

Present exhibits for court [11]

All images should be presented so that evidential content is not compromised. Where possible, images should be presented in their native or original format. If there is pertinent material that can only be seen when the image is viewed in proprietary form then provision should be made for appropriate playback equipment to be provided in court, if these arrangements are not already in place.

It should be understood that images may look different depending on the transmission and display equipment used. In particular, images viewed on different screens or by different media players may appear different from one another. An accurate replay facility should be provided wherever possible.

Retention and Disposal [12]

CDs, DVDs, digital tapes etc., are designed for short-to-medium term storage periods. To ensure the integrity of the data the files need to be transferred to new media regularly, possibly as often as every five years, or transferred to professionally managed data management archive systems (DEMS/DAMS). Data on these systems needs periodic review to ensure that the format is still accessible with currently available software and codecs. More detailed advice can be found in MoPI.

Dispose of exhibits and complete audit trail [13]

Each force needs to consider mechanisms for the disposal of images and complete audit trails once the statutory periods of retention are completed, in line with MoPI.

Glossary

APP
Authorised Professional Practice, developed and owned by the College of Policing

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.

CJS
Criminal Justice System

CPS
Crown Prosecution Service

Cloud Storage
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.

DAM
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.

DEM
Digital Evidence Management system, similar to a DAM or MAM system but optimised for storing evidence and related files.

DPA
Data Protection Act 2018. Of particular relevance is the Law Enforcement Directive, and which applies to the processing of personal data for the law enforcement purposes as defined therein. More generally, all police information is subject to management in line with the DPA, and national guidance in the form of the APP.

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)
Digital Video Recorder. Often a standalone CCTV recorder with attached cameras or attached to a larger networked CCTV system.

GDPR
General Data Protection Regulations. Applies to most UK businesses and organisations. See also the Data Protection Act 2018.

HDD
Hard Disk Drive, specifically magnetic storage of data on spinning platters within an enclosure. Though used here to include any internal storage drive including SSD.

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.

MD5#
A hash function used as a checksum to verify data integrity against unintentional corruption of a file.

MP4
A digital container format, primarily for video and audio. Can also contain other data such as still images and subtitles.

NVR (Network Video Recorder)
Networked Video Recorder, connected to IP cameras, often accessed remotely.

RAID
Redundant Array of Independent Disks, a system that improves data access times and can protect data from drive failure.

Sanitised
The procedure by which reusable media such as USB ‘thumb 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.

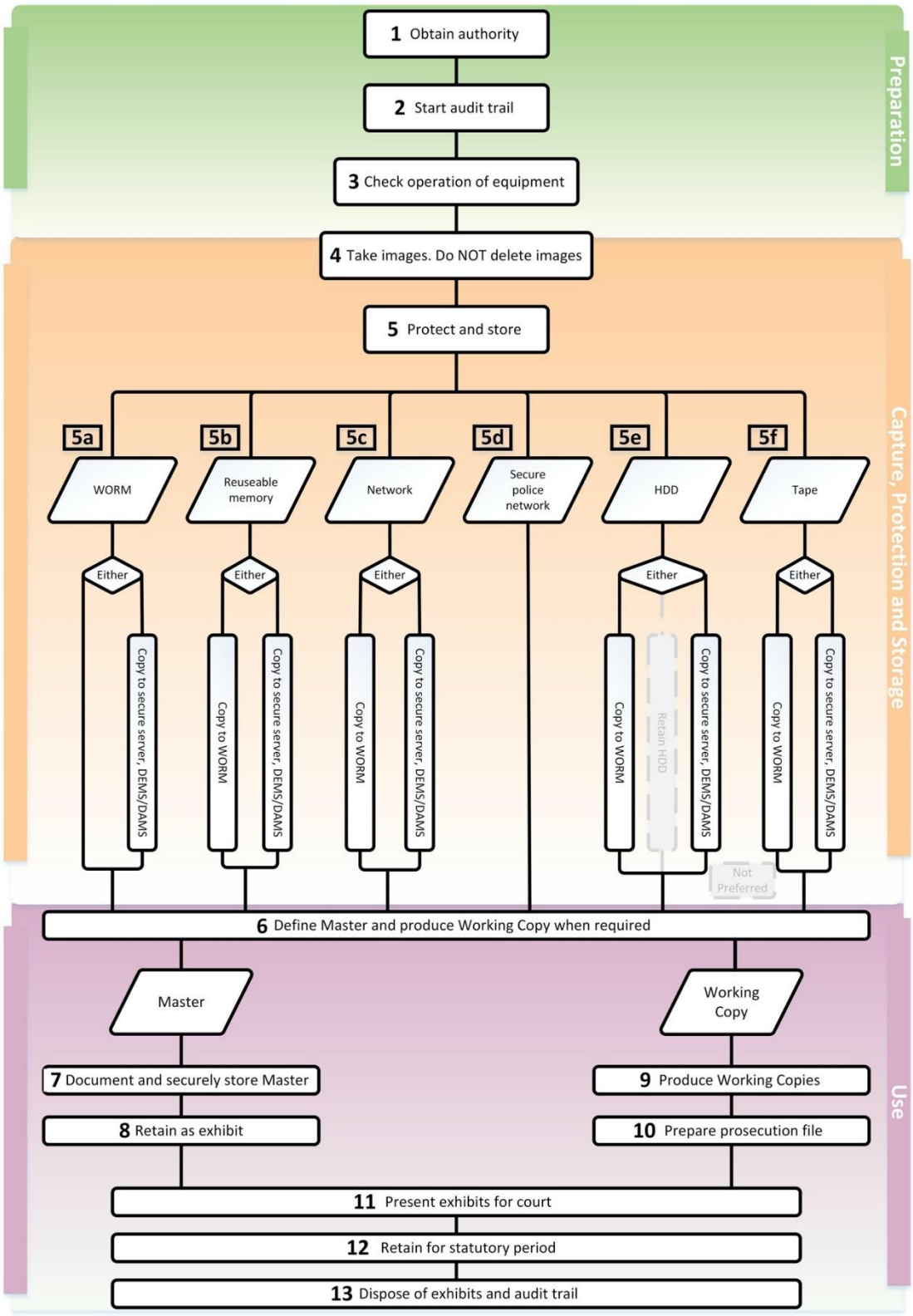
SOP
Standard Operating Procedure, a standardised way of achieving a task. Could be individual to the force or adopted on a wider level.

SSD
Solid State Drive, similar to HDD but using Solid State technology with no moving parts. SSD have faster access times and are slowly replacing HDDs in the computer industry.

USB
Universal Serial Bus

WORM
Write Once Read Many

Flowchart



For further explanation use accompanying notes and refer to force policy.