NPIA
National Policing
Improvement Agency

PROFESSIONAL PRACTICE

This PDF file contains interactive links to help you navigate the document quickly.

- ▶ Clicking on any of the items in the main list of Contents will take you directly to the page listed. Or click on any item in the list of Contents at the start of each section.
- ▶ To immediately access items cross-referred within this document, and any web links shown, click on those items appearing in colour.
- ▶ To return to the main list of Contents, simply click on the title line at the foot of each page.

NPIA
National Policing
Improvement Agency
PROFESSIONAL PRACTICE

PRACTICE ADVICE ON

POLICE USE OF DIGITAL IMAGES

2007

Produced on behalf of the Association of Chief Police Officers
by the National Policing Improvement Agency

This practice advice contains information to assist policing in the United Kingdom.

It is not protectively marked under the Government Protective Marking Scheme.

PRACTICE ADVICE ON POLICE USE OF DIGITAL IMAGES
This document has been produced by the National Policing Improvement Agency (NPIA) on behalf of the Association of Chief Police Officers (ACPO). It will be updated according to legislative and policy changes and re-released as required.

The NPIA was established by the Police and Justice Act 2006. As part of its remit the NPIA is required to develop policing doctrine, including practice advice, in consultation with ACPO, the Home Office and the Police Service. Practice advice produced by the NPIA should be used by chief officers to shape police responses to ensure that the general public experience consistent levels of service. The implementation of all practice advice will require operational choices to be made at local level in order to achieve the appropriate police response.

All enquiries about this practice advice should be addressed to:

Specialist Operations Centre
Wyboston Lakes, Great North Road, Wyboston, Bedfordshire MK44 3BY

Telephone: 0870 241 5641
Email: soc@npia.pnn.police.uk

Acknowledgements
ACPO and the NPIA would like to express their thanks to all those involved in the drafting of this document and to members of the Project Board, members of the technical workshops and the Project Assurance Group who gave their advice. All of the responses during the consultation phase of this project were appreciated and contributed to the final document.

CONTENTS

CONTENTS

Summary of Checklists

Summary of Tables

PREFACE

The value of evidential images cannot be understated; they allow those engaged with the criminal justice system to visualise crimes and present evidence in a unique way.

The proliferation of methods of digital recording and the potential use of digital images as evidence in the criminal justice system must be balanced against the ability to provide both safeguards and routine auditable processes which assist in their use.

Digital images are a useful source of evidence for criminal justice purposes. They should not, however, take primacy over other types of evidence, such as a statement from a police officer or another eye witness. The Police Service and other criminal justice agencies should resist any suggestions that an absence of digital images in a case in any way weakens it.

The police have a key role in managing digital images, including those generated by officers, specialist police staff and those supplied by third parties, such as members of the public. All images should be subject to standard evidential processes which ensure that if an image is required by the criminal justice system it is viewable and is accompanied by a full audit trail.

The **priorities** of the Police Service in using digital images are to:

- Support criminal justice processes and assist courts to reach a verdict;
- Use digital images appropriately, according to the current legislative framework;
- Ensure public confidence in the processing of digital images by the Police Service by, for example, providing full details of any processes applied to a digital image and limiting editing and processing techniques to only those which make the images viewable;
- Facilitate case preparation, disclosure and revelation of images to the Crown Prosecution Service (CPS) as a seamless process;
- Adopt a long-term strategic approach to storage of images, based upon clear guidelines for retention and archiving;
- Ensure that disposal of images is carried out according to time limits and legislative requirements.

The guidance contained in ***ACPO and Home Office (2007) Digital Imaging Procedure v2.0*** (hereafter referred to as ***DIP v2.0***) continues to apply and should be read in conjunction with this practice advice. This practice advice only relates to overt policing methods and overt use of digital images although many of the principles relating to capture, evidential continuity and retention are equally applicable to covert use of images. Any specific covert imaging issues are covered separately in ***ACPO/HMRC/SOCA (forthcoming) Guidance on the Use and Management of Surveillance Techniques, ACPO/SOCA/HMRC (forthcoming) Guidance on the Use and Management of Undercover Techniques*** and ***ACPO/HMRC/SOCA (forthcoming) Guidance on the Lawful and Effective Use of Covert Techniques – The Legal Framework and Covert Operational Management.*** Recovery of data and images from computers (apart from computer based closed-circuit television (CCTV) systems) is not included in this document and specific hi-tech crime issues are covered in ***ACPO/NHTCU (2004) Good Practice Guide for Computer Based Electronic Evidence v3.0.***

Chief officers should establish and implement policies which ensure that the police use of digital images reflects and achieves these priorities. In achieving these priorities and fulfilling these obligations, partnership working with other criminal justice agencies is essential to ensure that, where possible, images form part of the prosecution case and are displayed appropriately, facilitating effective viewing.

The purpose of this practice advice is to provide the Police Service with clear information about all stages of police use of digital images. Management issues are summarised at the end of each section. The practice advice is linked to the following documents, which are published by the Home Office Scientific Development Branch (HOSDB).

- ***HOSDB (2007) Storage, Replay and Disposal of Digital Evidential Images.***
- ***ACPO/Home Office (2007) Digital Imaging Procedure v2.0.***
- ***HOSDB (forthcoming) Guide to Technical Standards for Police Imaging Applications.***

See: **http://www.scienceandresearch.homeoffice.gov.uk/hosdb/publications/**

The practice advice is structured to follow the pattern of capturing, editing and processing, case preparation, disclosure and revelation to the CPS, and retention and disposal of digital images.

For chief officers the following strategic issues emerge from the practice advice:

- Implementing a comprehensive force policy that incorporates this practice advice and which works alongside associated policies such as ***ACPO (2006) Guidance on the Management of Police Information;***
- Developing information systems which support the implementation of this practice advice;
- Focusing on police responsibility for the use of digital images as evidence and for fulfilling its role in the criminal justice system to ensure that images are presented effectively, thereby facilitating the criminal justice process.

Section 1

MANAGING DIGITAL IMAGES AS POLICE INFORMATION

This section identifies the legal and policy framework within which digital images are managed as police information. It includes legal duties such as those relating to disclosure, human rights, data protection and freedom of information. It should be read in conjunction with *ACPO (2006) Guidance on the Management of Police Information; ACPO (2006) Data Protection Manual of Guidance, Part 1: Standards; ACPO and Hampshire Constabulary (2007) Manual of Guidance: Freedom of Information, Version 4* and *Information Commissioner (2000) CCTV Code of Practice* (currently being updated).

CONTENTS

1.1 DIGITAL IMAGES AS POLICE INFORMATION

Digital images include any image (moving or still) captured digitally and stored electronically. This document relates to images taken overtly by the police or images given to the police by third parties such as small business CCTV users or members of the public.

This practice advice is based on the assumption that all images generated by the police, or passed to police from third parties, have the potential to be used as evidence in the criminal justice system. Such images may also constitute valuable intelligence and information which may be useful to the police and multi-agency partnerships (eg, for planning crime prevention initiatives). For these reasons all images should be subject to the same standards, as outlined in this practice advice and other related national guidelines.

The principles outlined in ***ACPO (2005) Code of Practice on the Management of Police Information*** and ***ACPO (2006) Guidance on the Management of Police Information*** apply to the use of digital images by the Police Service.

Other documents provide more detailed guidance or standards (where they exist) about the individual applications of digital imaging. For further information on documents linked to applications, see **2.2 Sources of Police Generated Digital Images.**

1.1.1 MANAGING POLICE INFORMATION FOR POLICE PURPOSES

ACPO (2005) Code of Practice on the Management of Police Information states that all information, including intelligence and personal data obtained for police purposes is referred to as police information. Images are a form of police information.

Policing purposes are defined as:

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice;
- Any duty or responsibility of the police arising from common or statute law.

1.1.2 INFORMATION MANAGEMENT STRATEGY

Digital images should be specifically included in any planning for information technology (IT) systems and investment. Management of digital images should, therefore, be a part of the Information Management Strategy (IMS).

According to ***ACPO (2006) Guidance on the Management of Police Information,*** the IMS sets out the following:

- Who is responsible for police information held within the force;
- The purposes for collecting and holding information;
- Which business areas will be holding information within the force, and the standards that will apply within those areas;
- The safeguards that will be applied to police information held within different business areas;
- The relationship between police information held within different business areas;
- Which processes ensure police information is audited for accuracy and relevance to the policing purposes;

- What controls are applied to ensure the integrity and security of police information held by the force;
- The training that will be established to support the management of police information;
- The dedicated resources that will be allocated to support the delivery of the IMS and their relationship to other business areas;
- Arrangements for receiving records and monitoring record keeping;
- How the force will comply with national and local security policy and standards.

1.1.3 MANAGING IMAGING REQUIREMENTS WITHIN FORCE

Imaging applications should have some central management in police forces. In larger police forces this might be an imaging department which has oversight of all applications. In smaller forces this function may be carried out by a manager or force lead for imaging. The diversification of imaging applications requires that information relating to applications is held and managed centrally. The force imaging function should be closely allied with the force IT department. The requirements of all new applications should be discussed at inception stage so that issues of continuity of evidence and storage are considered at an early stage. Managing imaging applications centrally enables police forces to develop standard operating procedures (SOPs) that are based on local and national good practice. For further information on the partnership role between imaging and IT functions see, ***HOSDB (2007) Storage, Replay and Disposal of Digital Evidential Images,*** **Section 4.** See:
http://www.scienceandresearch.homeoffice.gov.uk/hosdb/publications/

1.1.4 USING THE DIGITAL IMAGING PROCEDURE

DIP v2.0 describes the process required to ensure that a master copy is defined as such or is created at the earliest opportunity and that only working copies are subject to any editing and processing techniques. It also describes the ways in which images can be stored, either on removable media or as part of a secure server. See: **http://www.scienceandresearch.homeoffice.gov.uk/hosdb/publications/**

1.1.5 COMPLIANCE WITH THE HUMAN RIGHTS ACT 1998

The Human Rights Act 1998 (HRA) underpins all other legislation and policy relating to the management of police information and gives effect to the European Convention on Human Rights (ECHR) in domestic law. The ECHR contains a number of fundamental rights which relate to the management of police information. The HRA requires UK legislation to be compatible with the ECHR and makes it unlawful for a public authority, including a police force, to act in a way that is incompatible.

Article 6 of the ECHR is the right to a fair trial. All images generated by the police or provided to the police by third parties have the potential to be used as evidence in criminal proceedings. This means that the use of police images is subject to legal safeguards in the same way as other police information. Safeguards relating to Article 6 rights might, for example, include developing full audit trails which document any editing and processing applied to an image, ensuring that the master copy of an image is stored correctly, and maintaining full disclosure schedules.

Article 8 ECHR is the right to respect for private and family life, home and correspondence. Article 8 includes both a negative obligation not to interfere with an individual's private life and a positive obligation to protect individuals against interference from other individuals. This affects the way in which digital images are captured, recorded and used. The European Court of Human Rights in *Peck v United Kingdom* (2003) 36 EHRR 41, paragraph 57, stated that:

> 'Private life' is a broad term not susceptible to exhaustive definition… The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world… There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'.

The judgment in this case suggests that CCTV recordings of an individual in a public place might, in some circumstances, be regarded as recording a private situation. The mere fact of an individual being in a public place is not sufficient to render the acts carried out as being public beyond those who may be passing by at the time.

Interference with the right to private and family life, such as sharing information about an individual, must be justified by one of the exceptions laid out in Article 8(2) and should be:

- In accordance with the law – this requirement should be satisfied if a legal power exists (as outlined above) and the processing of the information is in accordance with the Data Protection Act 1998 (DPA) and statute law;
- Necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others;
- Proportionate.

1.2 CRIMINAL JUSTICE DISCLOSURE

The Criminal Procedure and Investigations Act 1996 (as amended) (CPIA) introduced the statutory test for disclosure of unused material to the defence in a criminal case, see **4.1.4 Extent of Inspection of Unused Material – Images.** The duty to record and retain all information, including unused information, begins at the start of an investigation.

This disclosure regime refers to any prosecution material which has not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused, or of assisting the case for the accused. The Act provides that material need not be disclosed if the court, on an application by the prosecutor, concludes it is not in the public interest to disclose it and orders accordingly (sometimes referred to as public interest immunity or PII). Full information on the statutory regime for criminal justice disclosure can be found in ***Attorney General (2005) Attorney General's Guidelines on Disclosure*** and ***Crown Prosecution Service (2005) The Prosecution Team Disclosure Manual.***

The duties of the police under the statutory disclosure regime are part of the obligation for investigators to pursue all reasonable lines of enquiry whether these point towards or away from the suspect. For further information about criminal investigations, see ***ACPO (2005) Practice Advice on Core Investigative Doctrine.***

Deletion of any police generated images, or third-party images in police possession, prior to their respective retention periods (see **5 Retention, Storage and Disposal of Images**) may amount to a breach of the Act if they are not available for disclosure. In practice this means that police generated images should be accompanied by a full audit trail, from the point of capture of the image until they are passed to the CPS and throughout the whole management process. For further information about the amount of imaging material which should be downloaded, see **3.1.2 Selective Retrieval.**

1.3 DATA PROTECTION ACT 1998

The Data Protection Act 1998 (DPA) implemented the Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) into UK law. The Directive is intended to protect the rights of individuals when information about them is processed by organisations including the police. The Act contains a framework for decision making in the management of police information which is personal or sensitive personal data, whether processed on computer, CCTV, Automatic Number Plate Recognition (ANPR), stills camera or any other device. The Information Commissioner is the guardian of the Act and has enforcement powers where it is suspected that provisions of the Act have been contravened.

If the information is personal data then the DPA will apply. Slightly different provisions exist in the DPA depending on whether the information is sensitive personal data or not.

CCTV recording is covered by the DPA when the information relates to a living individual who can be identified. In judging this it should be established if the person was the focus of the information and whether the information tells something significant about them. If a CCTV system is used to record automatically without focusing upon an individual, the DPA is unlikely to apply unless information can be cross-referenced against other data which can identify the person.

CCTV systems used in large shops, railway stations, town centres and other places where large numbers of people gather are designed to focus on particular people or identify criminal activity and are covered by the DPA.

In the DPA, ‘processing’ has a broad meaning encompassing obtaining, recording, holding data and carrying out various operations in respect of it. When the term processing is used in this practice advice in reference to editing and processing digital images, it has a different meaning (see **3.1 Definitions of Editing and Processing**).

DPA applies eight principles to personal data, which should be observed when retaining and processing data. For further details see ***ACPO (2006) Data Protection Manual of Guidance, Part 1: Standards.***

All queries and requests relating to digital images which fall within the DPA should be directed to the force Data Protection Officer.

1.3.1 PERSONAL DATA

Personal data is defined in the DPA as information which relates to a living individual who can be identified from that data or other information held or likely to be held. It also includes any expression of opinion about the individual and any indications of the intentions of any person in respect of that individual. Data is not only personal if it is retrievable by a person's name or because a person's name is mentioned in a document. The definition of personal data is not limited to circumstances where a name can be attributed to a particular image by the person processing the image. If images of distinguishable individuals' features are processed and an individual can be identified from those images, they will amount to personal data. For example, a vehicle registration mark (VRM) processed by the police will be regarded as personal data on the basis that police forces have the capacity to identify vehicle keepers from that information. Data falls outside of the DPA if it is anonymous or depersonalised, but if there is a key or password to decrypt the data, the key or password is classed as personal data.

In considering whether data is personal, consideration should be given to two issues:

- Whether it is significantly biographical (eg, whether it has affected the subject's privacy in personal, family, business or professional life);
- Whether the data subject is the focus of attention.

In general, personal data should be kept confidential, but there are a number of exceptions to this general rule which are outlined in the DPA. These include Schedule 2 Public Functions which contain an exception when processing information for the purposes of prevention or detection of crime, apprehension or prosecution of offenders.

1.3.2 SENSITIVE PERSONAL DATA

A sub-category of personal data is sensitive personal data. According to the DPA sensitive personal data is information that relates to an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious or other similar beliefs;
- Membership of a trade union;
- Physical or mental health or condition;
- Sexual life;
- Alleged or committed criminal offences;
- Proceedings for any offence committed or alleged to have been committed;
- Disposal or sentence concerning any alleged or committed offences.

1.3.3 SUBJECT ACCESS REQUEST

The processes for dealing with subject access requests are covered in detail in a number of documents. These include ***ACPO (2006) Data Protection Manual of Guidance, Part 1: Standards, ACPO (2005) Guidance for the Provision/Viewing of Images Captured by Safety Cameras*** and ***Information Commissioner (2000) CCTV Code of Practice,*** (currently being updated).

1.4 SHARING INFORMATION FROM DIGITAL IMAGES

Under section 10 of the DPA an individual is entitled to serve notice on a data controller requiring the organisation not to begin, or to cease, processing personal data relating to that individual if that processing is likely to cause substantial, unwarranted damage or distress to that individual or another person. Before sharing information with the general public, the purpose for sharing must be considered.

1.4.1 SHARING IMAGES TO ESTABLISH IDENTITY

There will be circumstances where it is necessary to share digital images with the general public, usually through the media, in order to establish the identity or the whereabouts of a person. This image sharing might be to identify offenders, victims and witnesses, missing persons or remains of a deceased person. When it is decided that the public's assistance is needed in the identification process, the wishes of the victim of an incident, if practicable, should be taken into account. Where consent is used as the basis for sharing images, this should amount to a genuine free choice for the individual. In many circumstances consent will not be the most appropriate basis for sharing images as sharing will take place within the exception for the purposes of prevention or detection of crime, apprehension or prosecution of offenders. These principles apply to all images and not only to digitally generated ones.

Checklist 1 Sharing Digital Images to Establish Identity

The following general principles should be considered:

- There should be a purpose for sharing the images that is within the DPA;
- Third parties should not be identifiable;
- Faces, VRM and other identifying features of third parties should be fully obscured;
- Known subjects (usually victims or witnesses) should be shown the images which are intended to be shared;
- Any editing and processing carried out to assist with the identification process should be included within the audit trail;
- Images shared with known subjects, witnesses and the media should be maintained as a new and additional master copy.

Images should only be used if the use is compatible with the purpose for which the image was originally captured. For example, it would be an incompatible use if images from equipment installed to prevent or detect crime were disclosed to the media merely for entertainment purposes.

For further information on sharing information with the media, see ***ACPO (n.d.) Media Advisory Group Guidance Notes.***

1.4.2 CONSENT TO SHARE WHEN THE IDENTITY OF A PERSON IS KNOWN

Where images are shared which identify a particular individual and that individual is known, that person's consent should be sought before the information is shared. The European Court of Human Rights in *Peck v United Kingdom* (2003) 36 EHRR 41 has suggested that CCTV recordings of an individual in a public place are not sufficient to exclude it from being regarded as a private situation.

The mere fact of an individual being in a public place is not sufficient to render the acts carried out as being public beyond those who may be passing by at the time. It was suggested in the above case that if an individual in an image is not present for a public event or is a public figure, and the sharing of the image means that it is viewed more widely than the individual could have foreseen, then that person's consent should be obtained prior to the image being shared with the media or general public. If consent is not obtained, identity of such a subject should be fully obscured on the released image.

In circumstances where an individual's image is publicised in order to enforce a civil order, such as an Anti-Social Behaviour Order (ASBO), or to locate a person with a criminal conviction or absconder from prison, permission does not need to be sought from the subject. When considering publicity, the ECHR rights of the public, including victims and offenders, should be taken into account. Any publicity should be proportionate, legal and necessary.

1.4.3 RECEIVING DIGITAL IMAGES FROM THIRD PARTIES

Upon receipt, digital images from third parties should be treated in the same way as police captured images. In practice this requires that the principles of ***DIP v2.0*** are followed and a master copy is made as soon as possible. Generally, there should be no need to retain personal equipment such as mobile phones or personal data assistants (PDAs) from third parties who have presented material in their capacity, for example, as a witness. In circumstances where equipment is seized from a potential offender, the advice outlined by ***ACPO/NHTCU (2004) Good Practice Guide for Computer Based Electronic Evidence v3.0*** should be applied.

When images need to be retrieved from third parties such as CCTV schemes or retailers, it is preferable for the images to be downloaded by the system owner or administrator and then given to the officer. If the retrieval has to be carried out by the officer, they should be provided with specialist advice about retrieval methods. If the capture system presents significant difficulties for retrieval of images, the deployment of specialist retrieval officers should be considered. Specialist image retrieval officers or receiving officers being given third-party images should ensure that an audit trail is started at the point of receipt. For further information on audit trails, see **2.5 Starting an Audit Trail.**

Checklist 2 Receiving Digital Images from Third Parties

Officers or imaging practitioners should ensure that they:

- Establish the 'point of transfer' as part of the audit trail;
- Seek information from the third party relating to details of the capture and storage of the image;
- Consider the need to seize the sim card, memory card or other storage medium;
- Provide electronic facilities for digital submissions for cases involving significant public interest and the potential for a high volume of third-party images;
- Record details of the equipment used to capture the image;
- Record details of the third party and their relationship to the incident, eg, witness, victim.

1.4.4 COPYRIGHT AND APPLYING THE GOVERNMENT PROTECTIVE MARKING SCHEME

Images generated by the police and released outside of the prosecution services should be clearly copyrighted to the chief constable or relevant community safety partnership. Copyright statements should not obscure any part of the image or associated metadata.

The principles of the Government Protective Marking Scheme (GPMS) should be applied, as appropriate, to all images generated from police capture devices and third-party images at the point of transfer. Protective marking labels or authentication techniques applied should not obscure any part of the image or associated metadata. Storage media, including network storage, should be clearly marked or protected according to the classification applied to the images. Classification status should also be included as part of the audit trail. For further information about applying the GPMS, see ***ACPO (2001) Handling of Protectively Marked Material: A Guide for Police Personnel*** and ***ACPO/ACPOS (2006) Information Systems Community Security Policy.***

1.5 FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 (FOIA) creates a general right of individual access to all types of recorded information held by public authorities, including all information, not just documents, but excluding personal and sensitive personal data. Personal information is governed by the principles of the DPA rather than the FOIA.

The FOIA applies to all public authorities, including police forces, central and local government, the National Health Service (NHS), educational bodies and the armed forces. The FOIA places a requirement on public authorities, including the police, to produce and maintain a publication scheme – a document which details the classes of information that an organisation will routinely make available under the FOIA. Public authorities are also required to process requests for information held by them within twenty working days of receipt. This includes responding to a request. In the majority of cases the authority has to confirm whether or not the information is held and then provide it, if it is held, unless it is subject to an exemption.

There are a number of qualified exemptions relevant to the police, including information relating to national security (section 24), investigations and proceedings conducted by a public authority (section 30) and law enforcement (section 31). The purpose of the exemptions is to assist the Police Service in protecting information that, if released, may have a negative impact on its ability to fulfil its core functions of law enforcement, crime prevention and the protection of life. Unless one or more of these exemptions applies, individuals making applications have two rights under the Act: (i) to be told whether or not the authority holds the information applied for, and (ii) to have that information communicated to them in an intelligible form. The regulatory and enforcement authority for the Act is the Information Commissioner.

For more detailed information about the application of the FOIA to the Police Service, see ***ACPO and Hampshire Constabulary (2007) Manual of Guidance: Freedom of Information – Version 4.***

MANAGEMENT ISSUES

- Developing an information strategy which includes all aspects of police images.
- Producing a publication scheme for the purposes of freedom of information which includes digital images.
- Establishing systems for receiving third-party images.
- Ensuring that digital images are managed in accordance with the DPA.

Section 2

CAPTURING IMAGES

This section examines some of the police applications of digital imaging as an evidence resource (including third-party images that are given to the police for use as evidence). This section should be read in conjunction with *DIP v2.0* and any other application specific guidance or standards documents.

CONTENTS

2.1 CONSIDERATIONS AT CAPTURE STAGE

Capture is the process of recording as a still image or video sequence. Within a policing context this includes automatic capture, capture by imaging practitioners and capture by police officers. Prior to image capture the following steps should be taken:

- Obtain relevant authorisation or display fair processing notices as necessary;
- Check image metadata or embedded data (this may include time and date, camera number and location, software version, operator's name, user defined fields, information provided by manufacturer);
- Start an audit trail before capture or as soon as possible afterwards;
- Check equipment.

For further checks prior to capture, see ***DIP v2.0*** at:
http://www.scienceandresearch.homeoffice.gov.uk/hosdb/publications/

2.1.1 THIRD-PARTY IMAGES

At the point of transfer the responsibility for the handling of third-party images transfers to the police. The point of transfer will depend on the nature of images being transferred and the recording format and equipment used by the third party. At the point of transfer the police audit trail should begin and ***DIP v2.0*** applies. This audit trail should include attempts to obtain information relating to the capture of the image. See **2.5 Starting an Audit Trail.**

2.2 SOURCES OF POLICE GENERATED DIGITAL IMAGES

Some digital images are not captured by the police but are provided by third parties such as members of the public, eg, via mobile phone devices or PDAs, or as part of non-police capture systems, for example, small business CCTV. Use of private capture equipment owned by police officers or police staff should be minimal and should be restricted to use as a last resort. Any images captured on privately owned equipment should be treated as third-party images that have been submitted by members of the public, see **1.4.3 Receiving Digital Images from Third Parties.**

The following alphabetical list details some of the sources of digital imaging as used by the Police Service for the purposes of evidence collection. It excludes details of covert use of digital imaging and any applications which are reconstructions or interpretations, rather than involving the capture of an original image. This list is not exhaustive.

2.2.1 AUTOMATIC NUMBER PLATE RECOGNITION

Automatic Number Plate Recognition (ANPR) is the automatic image capture and recognition of vehicle registration numberplates and the checking of those details against a number of databases.

ANPR readers can be deployed in a number of ways:

- Dedicated fixed sites (key strategic sites such as ports and major road networks);
- Portable units;
- Linked into CCTV systems (police and/or local authority);
- Mobile units (in the form of dedicated vans and in-car systems);
- Other agencies and commercial companies using ANPR (eg, garage forecourts, shopping centres);
- Hand-held devices.

Each ANPR camera is capable of capturing many images of vehicles per hour, and matching numberplates against numerous databases or 'hot lists' very quickly. There are two types of ANPR generated data: read data and hit data. Read data contains all the numberplates captured for the duration of that deployment. Hit data identifies those numberplates that have hit against a particular database or hot list as being of interest. Individual ANPR systems link to an in-force central server known as the Back Office Facility (BOF). The in-force BOFs store the time, date, location and direction of travel of the vehicle together with an image of the numberplate, known as a 'plate patch'. In some cases an image of the vehicle is also stored.

The BOFs will link to the National ANPR Data Centre (NADC). This will enable investigators to search on a national basis. The BOFs and the NADC contain large quantities of data, and tools are being developed to interrogate this data. The six basic analytical functions are:

- Vehicle or crime pattern;
- Geographical;
- Location/time;
- Sequential pattern;
- Convoy;
- Post-incident.

For further information on ANPR, see ***ACPO (2007) ANPR Strategy for the Police Service (2007-2010)*** and ***ACPO (2007) ANPR Standards Issue 3.***

2.2.2 BODY-WORN VIDEO DEVICES

These devices are deployed in a variety of ways including as protective vest mounted, headsets and on police dogs for search activities. They are generally used as selective capture cameras and are deployed as evidence gathering tools for specific types of incidents such as public disorder or domestic abuse. Officers using body-worn devices should, where practicable, inform members of the public that they are recording. This is particularly relevant when recording information on private property. Armbands or badges can also be worn to inform members of the public that recording might be taking place; these are fair processing notices for the purposes of data protection. Use of body-worn video devices is overt recording and is, therefore, not usually subject to authorities under the Regulation of Investigatory Powers Act 2000 (RIPA). Deployment of body-worn video devices should, however, be supervised and directed, and officers should avoid recording general policing and activities of no further interest. For further information see **3.1.1 Selective Capture** and ***Police and Crime Standards Directorate (2007) Guidance for the Police Use of Body-Worn Video Devices.***

2.2.3 IN-VEHICLE CAMERA SYSTEMS

In-vehicle camera systems have a number of applications, from recording aerial images of pursuits and poor driving to showing the route of a vehicle involved in a collision through the view of the driver involved in the incident.

For further information on in-vehicle camera systems, see ***ACPO (2004) Code of Practice for Operational Use of Road Policing Enforcement Technology.***

2.2.4 CLOSED-CIRCUIT TELEVISION

Closed-circuit television (CCTV) systems record in a wide range of formats. These recordings can be provided by third parties or generated by police CCTV systems, such as those used in custody suites and mobile CCTV units. The operational requirements should determine the type of system used, for example, some systems will need to capture detail such as the appearance of people or vehicle registration numbers. Other issues for consideration include:

- The quality of recorded images (which will usually be inferior to those on live display);
- Effects of compression on the quality of the images (especially the recorded images);
- Accuracy of time and date information;
- Ensuring the system provides the facilities to enable the video evidence to be exported and shared within the criminal justice system;
- Processes for maintaining systems;
- Intended purpose of capture of the CCTV system if it is owned and maintained by a third party and the images captured are not intended predominantly for criminal justice purposes.

CCTV systems used in police custody suites should be used appropriately and according to set criteria for capture of images and siting of cameras. For further information see ***ACPO (2006) Guidance on the Safer Detention and Handling of Persons in Police Custody.***

For further information about capture requirements, see ***HOSDB (2007) CCTV Operational Requirements Manual, Information Commissioner (2000) CCTV Code of Practice*** (currently being updated) and ***ACPO/Home Office (2007) National CCTV Strategy.***

2.2.5 COVERT SURVEILLANCE

Specific procedures which are stipulated for the evidential handling, use and appropriate disclosure of digital images obtained through the use of covert techniques, including directed and intrusive surveillance, are not covered in this practice advice. The general principles outlined in this practice advice should, however, be adopted when using covertly obtained digital images. For further information on these issues, see ***ACPO/HMRC/SOCA (forthcoming) Guidance on the Use and Management of Surveillance Techniques, ACPO/SOCA/HMRC (forthcoming) Guidance on the Use and Management of Undercover Techniques*** and ***ACPO/HMRC/SOCA (forthcoming) Guidance on the Lawful and Effective Use of Covert Techniques – The Legal Framework and Covert Operational Management.***

2.2.6 CRIME SCENE PHOTOGRAPHS

Digital crime scene photography at capture stage is similar to conventional film techniques except that additional metadata is captured with the image and in some cases the compressed image may be unsuitable for evidential purposes. Crime scene photography includes any image taken at the scene, for example, capture of the scene itself using video, thereby allowing the viewer to see damage to property or non-intimate injuries to a victim.

Considerations at capture stage include:

- Ensuring equipment generates correct metadata;
- Using an appropriate file format to capture different scenes without compromising the image quality;
- Obtaining advice from specialist photography, where appropriate;
- Linking views and sequences of a crime scene.

See National Training Centre Initial Crime Scene Investigator's Course for further information on capture in crime scene photography.

2.2.7 FACIAL RECOGNITION SYSTEMS

The most common use of facial recognition is for investigative purposes rather than definitively proving identity. Facial recognition systems are not sources of images but are an application of digital images. Suspect images are compared with a database of reference images and the software will order the database to reflect its scoring of the likelihood of a match. Usually, the suspect images have to be pre-vetted to ensure they are of a suitable quality to be used with the software, and the results obtained need to be interpreted with care. Any use of this application depends on the quality of the initial capture of the image.

Facial recognition software, which is designed to automatically compare faces, is based on algorithms. One issue with using such software is that it does not necessarily differentiate on obvious physical characteristics, using instead more mathematically abstract criteria.

Use of facial recognition requires consideration of the following:

- The findings of the software need to be interpreted with care;
- Typical software is very sensitive to lighting conditions and head pose, although systems are becoming more robust in this respect;
- Most algorithms are insensitive to skin colour and gender;
- The software was developed for use with fairly good quality images, not those typically extracted from CCTV sequences.

Under section 12 of the DPA individuals have certain rights to prevent automated decision taking where a decision, which significantly affects them, is based solely on automated processing. ***Information Commissioner (2000) CCTV Code of Practice*** (currently being updated) states that if an automatic facial recognition system is used, procedures should be established to ensure that the match is also verified by a human operator, who will assess the match and determine what action, if any, should be taken. This will help to ensure compliance with the DPA, particularly the first principle (lawful processing) and seventh principle (unauthorised or unlawful processing). The result of the assessment by the human operator should be recorded whether or not they determine there is a match.

The distinction between facial recognition and facial mapping is that recognition is performed by using automated software, whereas mapping is a manual process used to prove or disprove identity. It may be the case that the automated recognition system would provide a set of possible matches, but the human expert would make the final decision as to whether any of these possibilities were indeed a correct match. For further information see ***ACPO (2003) National Working Practices in Facial Imaging*** and ***HOSDB (2006) Briefing Note on Facial Mapping for Video Evidence Analysis Users' Group.***

2.2.8 FINGERMARKS

In capturing arrestee, latent and lifted fingerprints, operators should use appropriate capture systems to obtain the detail necessary for fingerprint experts to assess images for identification purposes, including examination, comparison and verification tasks. The visual identification of ridge characteristics can be affected by the pixels per inch (PPI) present in electronically captured images, although image quality also depends on a number of other factors including the optical transfer function of the capture device.

Considerations at capture stage include:

- PPI resolution;
- Levels of greyscale and use of colour imaging;
- Storing and transmission without compression, with lossless compression or using an approved technique;
- Ensuring developed or lifted fingerprint images are accurate replicas (pixel for pixel value) of the latent image;
- Compatibility with any automated fingerprint recognition software used nationally or locally (including Livescan);
- Audit trails that document capture details of latent fingerprints and subsequent developed or lifted fingerprints.

See ***ACPO (2006) National Fingerprint Manual – Issue 1*** **[CD-Rom].**

2.2.9 IDENTIFICATION

Video identification parades typically reduce police time taken to arrange conventional identity parades, and reduce distress caused to victims by enabling them to look at a series of digital images or mug shots. They are also more flexible than identity parades as the line-up can be viewed in venues other than a police station. The benefits of this are the faster identification of suspects and a reduced risk of an identification parade being abandoned. Video identification applications providing a bank of digital images of possible volunteers for line-ups include Video Identity Parade Electronically Recorded (VIPER) and Profile Matching (PROMAT). A central video database is maintained in both applications.

The capture of clear images of arrestees is central to the use of any identification process. The following issues require consideration at capture stage:

- Correct pose including full head, neck and shoulders, face fully visible;
- Iris and pupil of the eyes should be clearly seen, where possible;
- Neutral facial expression with both eyes open and mouth closed;
- Lighting should uniformly illuminate the subject’s face and the background;
- Background should be plain, smooth and flat.

Further details about the quality of the capture are available from:
http://www.npia.police.uk/en/7771.htm

2.2.10 INVESTIGATIVE INTERVIEWING

Visually-recorded interviews might be appropriate in suspect interviews as well as those with vulnerable, intimidated or child witnesses. As a visually-recorded interview might replace the first stage of a vulnerable or intimidated witness’s evidence in court, the same rules apply as if the evidence had been given in court. The quality of the visual and audio recording will, in part, determine whether it can be used as evidence in chief.

For further information about the processes of recording investigative interviews, see ***Home Office (2007) Achieving Best Evidence in Criminal Proceedings: Guidance on Interviewing Victims and Witnesses, and Using Special Measures, Appendix O, Technical Specifications.***

Issues for consideration at capture stage include:

- The preferred method is that hand-held equipment should be used only in exceptional circumstances;
- Interviews should be conducted in fixed interview suites except in rare circumstances when portable equipment can be used;
- In any circumstances where portable equipment is used, the reasons for this should be recorded by the investigating officer;
- Equipment must be operated and maintained by properly trained staff;
- Equipment operators should remain in control of recording equipment at all times during the interview process.

For further information about the equipment specifications of capturing interviews, see ***Criminal Justice System (2004) Visual Recording of Evidence Within the Criminal Justice System – Equipment Specification.***

2.2.11 PUBLIC ORDER EVIDENCE AND INTELLIGENCE GATHERING

Digital recording has two main applications in public order policing, firstly as an evidence gathering function and secondly as an intelligence function prior to any disorder occurring. Both applications involve overt capture of images and these methods are deployed as part of the Police Support Unit (PSU) response.

Evidence gathering teams are deployed to gather digital evidence of the most serious incidents occurring at the time, with a commentary where practicable. These teams are usually deployed with protection officers, who also manage communication with the incident commander to facilitate their most effective use.

Issues for consideration at capture stage include:

- Early deployment, eg, at a planned demonstration prior to any disturbance;
- Siting evidence gatherers as close as possible to any disorder;
- Ensuring the safety of evidence gatherers and equipment;
- Recording suspects and possible witnesses;
- Confirming the location of the PSU by recording landmarks.

Forward intelligence teams (FITs) are deployed both as an intelligence function and to reduce the potential for disorder through recognition of nominals. They are also uniformed officers who gather intelligence, including digital images, which are used to assist the planning of resource deployment. FITs are deployed to capture images prior to disturbances. They should withdraw during incidents and be replaced with evidence gathering teams.

For further information on public order applications, see ***ACPO (2004) Public Order Standards, Tactics and Training Manual.***

2.2.12 ROAD SAFETY CAMERAS

There are many types of recording device used in road safety, including speed checking equipment and cameras sited at traffic lights to capture vehicles contravening signals. These can be fixed site cameras or mobile units, automated or requiring operators. Fixed site approved speed cameras operate in conjunction with an approved second independent method of speed measurement. This secondary check is required in order to provide a further check on the accuracy of the device. No secondary check is required for red light cameras as two images are captured and provide sufficient check on the movement of the vehicle.

Police forces, highway authorities and other members of casualty reduction partnerships assess the location of suitable capture sites according to the following factors:

- A recognised collision problem;
- The causes of the collisions, or a major factor in the severity of injuries, must be illegal excess speed or red light running;
- A review of the site and surrounding roads indicating enforcement is the best available option with the sole intent being to reduce casualty figures by influencing driver behaviour;
- Any possible effects on residents living close to camera sites.

Camera equipment should be type approved and used only for the function for which it was approved, eg, attended actively operated equipment should not be used in an unattended or attended automatic mode.

Safety cameras are not intended to be hidden and, therefore, equipment should not create a road safety problem. Road signs and general visibility should not be obscured or diminished by the equipment. Camera housing should not be obscured by signs or foliage. Mobile safety cameras can operate from up to ten different capture sites, moving at regular intervals.

Under section 12 of the DPA individuals have certain rights to prevent automated decision taking where a decision, which significantly affects them, is based solely on automated processing. One example of automated decision making includes issuing a court summons to a person recorded as a vehicle keeper with the Driver and Vehicle Licensing Authority (DVLA) on the basis of a safety camera reading, without any further investigation or intervention.

For further information on safety cameras, see ***ACPO (2004) Code of Practice for Operational Use of Road Policing Enforcement Technology.***

2.3 CAPTURE QUALITY FOR PURPOSES OF THE DPA

All digital images processed by the police should be as clear as possible so that they are effective for the purpose(s) for which they are intended. The third data protection principle in the DPA, that data be adequate, requires that the police should record all factual and descriptive information relating to digital images in a format which assists interoperability and transfer between different police information systems.

All police officers, imaging operators and third parties involved in the capture (referred to as 'process' for purposes of the DPA) of digital images should be familiar with relevant national and local guidance (SOPs) related to the particular application of digital imaging with which they work, and the purpose(s) for which the images are being processed.

Any agreement or contract with a third party responsible for capturing digital images on the part of the police should emphasise that images can only be captured (referred to as processed for purpose of DPA) to achieve the purpose(s) for which it has been installed.

2.4 FAIR PROCESSING NOTICES

In order to capture (process) fairly, the following information, at least, should be provided, either verbally or in writing, to the individuals at the point of obtaining their images:

- Identity of the data controller;
- Identity of any representative the data controller has nominated for the purposes of the Act;
- The purpose(s) for which images are captured;
- Any information which is necessary, having regard to the specific circumstances in which the images are captured, to enable processing in respect of the individual to be fair.

For example, fair processing notices can be signs in public places where CCTV (including custody suite CCTV) or road safety cameras are in operation.

For further information about fair processing notices, see ***ACPO (2006) Data Protection: Manual of Guidance, Part 1: Standards.***

2.5 STARTING AN AUDIT TRAIL

A full audit trail (including a maintenance log) should be established and maintained at the point of image capture, or at the point of retrieval or seizure if it is generated by a third party. The audit trail should be of sufficient detail to allow replication of all processing by a comparably trained person. The audit trail should document the working processes from the initial master copy, to the working copy and to the end product. The development of the audit trail is essential for the disclosure process and will form part of the disclosure schedule. The audit trail should be developed by, or shared with, the exhibits and disclosure officer(s) from the beginning of the investigation process.

For some routine processes (converting and copying), the full audit trail is not essential, provided that the content of the image is not critically affected. See **4.1.1 Completing the Audit Trail** and **4.1.2 Special Considerations in Cases Involving Video Image Exhibits.**

2.5.1 NAMING THE MASTER AND WORKING COPIES AND VERSION CONTROL WHEN USING IT-BASED SECURE STORAGE

The master copy (and any subsequent working copies) should be named appropriately as soon as it is practicable to do so. This is of particular importance when using a secure network to store different versions of an image. Systems should be developed to ensure that the master image is properly stored and is retrievable before making and using working copies.

2.6 CREATING A MAINTENANCE LOG

The correct functioning of the capture equipment is a significant part of demonstrating the integrity of an image. In capture equipment in which images are generated by the police, all relevant information about the capture system should be recorded and checked as part of a maintenance log which, if required, may be produced for criminal justice purposes.

Checklist 3 Possible Elements of a Maintenance Log

Maintenance staff or imaging operators should consider including the following information, where relevant to the application:

- Manufacturers' specification of the application(s);
- Dates of routine maintenance inspections;
- Accuracy of metadata and details of any errors;
- Supply levels of recording media and power;
- Software checks to ensure replay of the captured image is possible;
- Scheme of checks is available for the imaging operator prior to capture.

MANAGEMENT ISSUES

- Assessing compliance with ***DIP v2.0.***
- Ensuring all capture and retrieval equipment is appropriately maintained with completed maintenance logs.
- Developing SOPs for all capture applications.

Section 3

EDITING AND PROCESSING

This section defines and summarises the functions of editing and processing images. It should be read in conjunction with *DIP v2.0* and with the understanding that editing and processing techniques should only be applied to a working copy of the image.

CONTENTS

3.1 DEFINITIONS OF EDITING AND PROCESSING

Editing can be described as the process of selecting, assembling and sequencing trimmed portions of raw material into a final viewable product. As used in this document, the term includes deletion, but not 'selective capture', see **3.1.1 Selective Capture.**

Processing images generally involves adjusting the technical properties of the image and modifying the actual content to improve or change some quality of the image. The use of the term processing in this section should not be confused with the wider definition of processing data within the DPA, which includes obtaining, processing, recording, holding or carrying out any operation or set of operations on the data.

A number of editing and processing functions have routinely been carried out in relation to conventional, wet film processing. It is, therefore, not necessary to apply any additional safeguards to those digital imaging actions that mimic these previously accepted conventional techniques. For this reason traditional techniques have been excluded from this section.

3.1.1 SELECTIVE CAPTURE

This involves the decision to switch on and off video recording devices, for example, when using body-worn video and in-vehicle cameras, and should not be confused with other editing processes. Selective capture does not include the deletion of images, only the decision to start and cease capture. Any use of selective capture should aim to record incidents in their entirety. Where there is a break in recording this should be explained as part of the audit trail, and as part of the audio recording (if this function is available).

In circumstances where selective capture is used, and it is appropriate, the operator should verbally provide the following information at the beginning of the recording:

- Name of the operator;
- Location;
- Time, if not correct on the recording device;
- Reason for beginning to record.

(If it is not possible to verbally provide information, details should be included as part of the audit trail or as part of the case papers.)

Where possible and practicable, operators should consider providing a running commentary during the recording of any incident. At the cessation of recording, operators should verbally (or otherwise) provide the following information:

- Reason for ceasing the recording;
- Time, if not correct, on the recording device;
- Incident identifier such as a case number or name of arrestee.

The information about the decision to capture, and any related metadata should form part of the audit trail. Metadata is often automatically generated by the capture device and may include the time and date of image capture, camera number and/or location and software version. Those using selective capture techniques should ensure that no editing takes place at the point of downloading the images.

3.1.2 SELECTIVE RETRIEVAL

When an incident of interest is identified on a capture system and this data is required to be downloaded, this process is referred to as selective retrieval. This method might be used in relation to a number of capture applications, eg, CCTV systems, body-worn videos and other third-party applications such as images from mobile phones and other devices which capture images. In some circumstances, mostly dependent upon the complexity of the capture system and the need to maintain the integrity of the data, retrieval may be carried out by specialist image retrieval officers or imaging practitioners. However, the decision about the quantity of data to download (eg, video either side of the incident, which camera views are relevant) should be made by the investigating officer in consultation with the retrieval officer or imaging practitioner. This decision should be reviewed as the case progresses and further information becomes available. Care should be taken to note systems which may over-record, and therefore lose data, when carrying out reviews of selective retrieval strategies.

When deciding on the volume of data to be downloaded to fully cover the captured incident and any surrounding circumstances, the following factors should be taken into consideration:

- Parameters fixed by the capture retention system, eg, some might only capture for a twenty-four-hour period at a time or might overwrite images;
- Expedient retrieval to secure material from non-police generated images;
- Type or nature of offence or incident;
- Gravity of offence or incident;
- Context of offence or incident;
- Capture coverage of the area in which the offence or incident took place, including possible entrance and exit routes, image quality and anticipation of possible defence tactics.

If retrieval is taking place from a CCTV system, the capture process should not be stopped while data is being downloaded.

For further information see ***HOSDB (2006) Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems No. 21/06.***

3.1.3 RECOVERY OF CORRUPTED IMAGE FILES

In situations where image files have suffered data corruption and require recovery through an approved IT process, any recovered image or image sequence, partial or complete, should be included as part of the audit trail. The audit trail should include an assessment of what data might have been lost or altered by the image file recovery process.

Note: The image recovery process may retrieve images that are not considered to relate to the case in question. Where this happens, a record should be included as part of the audit trail. For further information on audit trails, see **4.1.1 Completing the Audit Trail.**

3.1.4 PURPOSE OF EDITING AND PROCESSING

Much pictorial information, conventional and digital, is routinely used by investigators and finally presented to the courts. At times it is necessary to edit or process this information to reduce the volume, achieve better quality images and/or separate that which is relevant from that which is not.

Editing and processing of images should only take place with justifiable cause and in such a manner that it does not detract from the ability of the prosecution and defence to present their case and for the courts to arrive at a verdict. Any editing and processing should be carried out with the intention of assisting the investigative process and presenting the evidence to the courts in the clearest possible manner.

Imaging practitioners should ensure that the editing and processing methods they are employing are appropriate for use in a criminal justice context, and that software tools are valid and reliable. Misapplication of editing and processing techniques may change the context of an image, suppress pertinent information originally contained in it, or introduce misleading information that was not originally present.

The guidelines to safeguard the evidential integrity of images, contained in ***DIP v2.0,*** continue to apply.

Note: Editing and processing should only ever be applied to working copies and not to master copies.

3.2 EDITING

Editing can be divided into two main types.

3.2.1 CONVERTING AND COPYING

This includes certain routine processes where there is no intention to change the appearance of the image, examples include, printing, photocopying, monitor display, format or media conversion and scanning.

On occasions it may be desirable to compress image files to ease transmission and/or storage. Assuming that this will not result in any relevant degradation to the image (taking into account the evidential content and how this will be used in court), it may be regarded as a routine process. Issues resulting from compression should be judged by taking into account the evidential content of the image and how this will be used in court. For example, the introduction of artefacts could be critical in respect of a fingerprint image but of no consequence to a less detailed image. There are preferred schemes for compression which are dependent upon standards applied to particular capture applications.

The following faults might arise as an unintended consequence when applying the techniques of converting and copying:

- Distortion (eg, colour distortion, loss of contrast and resolution) when printing and photocopying or when displaying on a monitor;
- Loss of image quality or metadata when undergoing format or media conversion;
- Loss of image quality or introduction of artefacts when applying lossy compression.

The risks relating to distortion can be mitigated by appropriate calibration and maintenance of all printing, photocopying and display equipment, as well as ensuring that such equipment is of the appropriate specification and all operators are trained to the required local standards.

Issues relating to format conversion may be unavoidable in certain circumstances (eg, when processing evidence from proprietary CCTV systems), but they can be addressed by following ***HOSDB (2006) Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems No. 21/06.***

3.2.2 SELECTION, ASSEMBLY AND SEQUENCING

Generally, this can be taken to include the following:

- Editing, including deletion, in time (eg, cutting a sequence) or space (eg, region of interest, cropping);
- Highlighting regions of interest, eg, selecting or discarding part of an image, selecting specific images within a sequence;
- Obscuration to preserve privacy, eg, pixilation of faces;
- Stitching or compilation;
- Presentation, eg, adding captions or breaks into video, incorporating images within other information (creating a storyboard).

The principal issue relating to selection, whether in time or in space, is that of loss of context. There is the danger that the omission of images or part of an image could materially affect the interpretation of what is finally presented in court. Annotation is a good example of this, where the captions in themselves might obscure some of the image content. When editing, practitioners should consult investigators and, where necessary, the CPS to ensure that all appropriate content is preserved.

3.3 PROCESSING

Processing can be divided into three main types.

3.3.1 ENHANCEMENT

Enhancement relates to any process that serves to improve the overall image quality and includes:

- Brightness adjustments;
- Contrast adjustments;
- Colour cast removal (colour correction is assumed to be routine processing);
- Noise removal;
- Edge enhancement;
- Histogram stretching.

Enhancement can be a compromise, ie, certain parts of the image are being enhanced to the detriment of other image areas. For example, the effect of edge enhancement is to broaden edges, which can in turn lead to loss of nearby fine structure. When enhancing, careful consideration needs to be given to what is being lost from the image, how this might affect the evidence and how this is presented. Enhancement should not generally be applied to selective portions of an image unless these regions and the enhancements within them are clearly identified; this is of particular significance in enhancing fingermarks. However, it is permissible to enhance the whole of a cropped image.

3.3.2 RESTORATION

Restoration refers to the reversal of mechanisms in the capture process, eg, motion blurring or functions that have caused image deterioration. The intent behind restoration techniques is to return the image to an undeteriorated state. Such tools are usually validated by mathematical modelling.

Restoration does not add information and, therefore, excludes interpolation (estimation of missing information). This falls into the category of reconstruction.

The following are examples of restoration techniques:

- Blur removal from an image, eg, defocus and motion blur;
- Greyscale linearisation adjusts the brightness among objects to reproduce the different brightness values in the scene;
- Colour balancing is the adjustment of the colour components to reproduce the colour to that of the original;
- Warping;
- Geometric restoration removes geometric distortion of an image, eg, fish eye lens.

The risk associated with restoration techniques is that depending on how well the function has been mathematically modelled, the restored image may still differ from the original in an evidentially significant way. Therefore, the limitations of the restoration process have to be understood, taken into account and communicated when presented.

3.3.3 RECONSTRUCTION

This is the production of visual aids to assist the understanding of juries, or to provide information to them in a more acceptable form (for example, to sanitise an otherwise graphic or disturbing crime scene), or to support the hypothesis of an expert witness. Though the images that form the input may be classed as evidential, the outputs from reconstructions are not true images but are graphical interpretations and should not be presented as true images. For that reason care should be exercised in determining the extent to which a reconstruction is made to appear realistic.

3.3.4 USE OF EXTERNAL CONTRACTORS

Any contractor generating a reconstruction on behalf of the police should be able to justify the approach they have taken, and explain the individual steps in producing the generated model or depiction. All externally produced enhancements or reconstructions should be accompanied by corresponding history logs and should be fully incorporated into the audit trail. Any work carried out by a contractor should be supervised by force imaging specialists to ensure that it meets the requirements as set out in this document. Reconstruction is not the focus of this document, neither are the many available products used for forensic reconstruction purposes.

3.4 PRINCIPLES OF USING EDITING AND PROCESSING TECHNIQUES

Checklist 4 Considerations when Undertaking Editing and Processing Techniques

Imaging practitioners should:

- Ensure that the original image is preserved as a master in accordance with ***DIP v2.0;***
- Apply techniques only to the working copy of the image;
- Note that when an image is altered and becomes the basis of a witness statement, eg, as part of an identification process, the altered image becomes a new and additional master copy;
- Ensure continuity and security of evidence in accordance with ***DIP v2.0;***
- Preserve the metadata of the master copy and, wherever practicable, in respect of the working copies;
- Carry out techniques which are consistent with their skills, experience and accreditation;
- Ensure that history logs (often electronically generated by software applications) are included as part of the audit trail;
- Accompany all imagery with a full audit trail;
- Ensure that when applying a technique, the effect does not undermine the evidential content of the image;
- Use software and hardware supplied by their police force that is supported by SOPs.

3.5 SPECIALIST ROLES FOR IMAGING PRACTITIONERS

Only competent, suitably trained and authorised personnel should carry out any of the editing and processing functions (these may be specialist imaging staff or other application users). Editing and processing carried out by non-imaging practitioners should be sanctioned and supervised by the relevant imaging departments or imaging practitioners. The Council for the Registration of Forensic Practitioners (CRFP) distinguish between roles relating to the use and further editing and/or processing of images. Police forces can use these distinctions as an example and as a guide.

- **Generalist** – will have a basic knowledge of imaging and will know how to use the technology without the background knowledge of how the technology works. A generalist will carry out basic elements of image processing which are applicable to all imaging sub-specialities (refer to CRFP definitions for further information).

- **Specialist** – will work with specific software and hardware in order to process or edit images. Specialists will produce exhibits in their own right, as well as work with other investigators' products and develop evidential statements resulting from the editing and processing tasks carried out. A specialist will carry out primary and advanced processing, and technical analysis (refer to CRFP for further information).

- **Expert** – will be able to interpret images and analyse data to identify anomalies and alterations. An expert will carry out all types of processing and technical analysis, as well as interpretation that will require the expression of an opinion (refer to CRFP for further information).

For further information about CRFP definitions see:
http://www.crfp.org.uk/

Table 1 relates the above training levels to the previously discussed types of editing and processing.

Table 1 Suggested Remit for Imaging Roles

	Generalist Basic image processing	**Specialist** Primary and advanced image processing	**Expert** Technical analysis, interpretation and all other image processing
Reconstruction	✗	✗	Only if accepted expert in reconstruction
Restoration Enhancement Selection, Assembly, Sequencing	✗	✓ Working to SOPs and works with investigator; does not provide interpretation	✓ Working to SOPs and works with investigator; provides interpretation
Conversion/ Copying	✓ Working to SOPs	✓	✓

3.6 PREPARING DIGITAL IMAGES AS EVIDENCE IN COURT

When presenting evidence in court, the practitioner should be able to explain:

- What purpose (eg, within the DPA) and justification exists to process and edit images;
- Why a particular tool was selected;
- How the tool was applied;
- How the end product was achieved.

It is not expected, however, that practitioners are able to explain the construction of the software or hardware itself. Where necessary, the manufacturers should be contacted to access technical specialists.

The software and hardware applications in any one area should be described in local SOPs that should be made available for inspection if required.

MANAGEMENT ISSUES

- Providing SOPs for all software and hardware used for editing and processing.
- Ensuring that software and hardware is suitably calibrated and maintained to the manufacturers' specifications to achieve the set objective.
- Ensuring that any editing or processing not carried out by imaging practitioners is sanctioned and supervised by the imaging department.

Section 4

CASE PREPARATION, DISCLOSURE AND REVELATION TO THE CROWN PROSECUTION SERVICE

This section describes the case preparation and disclosure of unused material relating to evidential digital images, and provides information for consideration when revealing exhibit images to the CPS and preparing for court. It should be read in conjunction with the *Attorney General (2005) Attorney General's Guidelines on Disclosure, Crown Prosecution Service (2005) The Prosecution Team Disclosure Manual* and the Code of Practice on Disclosure, (issued under section 23(1) of the Criminal Procedure and Investigations Act (1996).

CONTENTS

4.1 CASE PREPARATION CONSIDERATIONS IN DIGITAL IMAGE EVIDENCE

In each police investigation an exhibits officer and a disclosure officer should be appointed. These roles might be performed by the same individual, who might also be the investigating officer. In large or complex cases a number of exhibits and disclosure officers might be appointed. A lead disclosure officer should, however, be the focus for enquiries, and be responsible for ensuring that the investigator's disclosure responsibilities are complied with. In complex cases the exhibits officer and the disclosure officer should have ready access to imaging specialists or experts who might be required to respond to more detailed enquiries.

Checklist 5 Considerations in Cases Involving Digital Image Exhibits

Officers should:

- Ensure that all exhibit images have been reviewed (and unused images captured or seized and retained from the beginning of an investigation are included as part of the disclosure process);
- Ensure that viewing logs have been completed, as applicable;
- Check the audit trail for completeness and submit it with the exhibit;
- Assess and schedule material, including images and their metadata (when required);
- Inform the prosecutor of the date of the start of the investigation as different disclosure regimes apply;
- Apply GPMS to exhibit images;
- Ensure that unused material is retained and stored appropriately and is catalogued, including whether or not it has been fully viewed;
- Review unused material, including images, once a defence statement has been received.

4.1.1 COMPLETING THE AUDIT TRAIL

The responsibility for the development of an audit trail rests with any personnel who have had contact with the digital exhibit material. This may include image retrieval officers, police officers or staff, image capture operators, imaging practitioners and specialists, disclosure officers, exhibits officers, investigating officers, data protection officers and others.

Some parts of the audit trail will be part of a technical log or history log and will be generated by software applied to the image as part of any editing and processing. The audit trail should include sufficient information to enable a comparatively trained practitioner to replicate the steps to achieve the same results from the master copy. The level of detail listed in **Checklist 6** should not be required for every image or video sequence. However, a relevant audit trail should be developed for all exhibits. Information should be compiled for exhibits as required by the circumstances of each case. Further information should always be available subject to a request for more detailed information.

Checklist 6 Compiling an Audit Trail for Digital Images

Imaging practitioners and officers should include the following information (with date and time of action) when available and if appropriate:

- Details of the case;
- GPMS classification of the image (and any special handling instructions, if relevant) and the name of the person who classified the image;
- Where the image is third-party generated, information about point of transfer including whether the image is the master copy, 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 (see **2.6 Creating a Maintenance Log**);
- Identity of the capture operative including third parties and retrieval image officers, where applicable;
- 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 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.

4.1.2 SPECIAL CONSIDERATIONS IN CASES INVOLVING VIDEO IMAGE EXHIBITS

Video images such as CCTV sequences or material from body-worn video devices require accurate viewing logs to be completed to accompany each evidential sequence or exhibit that has been retrieved. Viewing officers should include the following points when compiling viewing logs as part of case preparation:

- Date of viewing;
- Reason for viewing;
- Identifier number of media and/or file and action number;
- Type of media viewed, eg, MiniDV, DVD;
- Format of proprietary files;
- Software used with version number, if applicable;
- Location of camera and any other camera coverage;
- Name of person giving authorisation for viewing;
- Name of person viewing data;
- Time of sequence;
- Outcome and description of sequence;
- Signature of person viewing data.

Checklist 7 Specific Considerations in Cases Involving Video Image Exhibits

Investigating and exhibits officers should consider the following:

- Make and model of the capture system;
- Whether the image was generated as part of a multiplex system;
- Whether other video sequences from a multiplex system have been retrieved and retained;
- Whether there is or has been coverage of the vicinity or area and if it has not been retrieved and retained, the reasons for this;
- Whether the capture system metadata was correct and if not, any discrepancies which have been noted;
- Viewing logs relating to the imagery;
- Information about other viewing logs relating to unused material, including a description of other imagery.

4.1.3 DEVELOPING THE DISCLOSURE SCHEDULE FOR UNUSED IMAGES

The established procedure of developing a disclosure schedule (MG6 forms) records all relevant information, including digital image evidence relating to a case. These should be completed by the disclosure officer, who should ensure that unused images are included as part of the schedule. Overtly captured digital images should form part of the information recorded on the non-sensitive disclosure schedule.

The schedule should provide a brief description of what is contained in the image or video sequence and any significant processing applied to it. A more detailed description of processes should only be provided if the image becomes an exhibit or is requested by the defence to form part of the defence case. The description of the unused image on the schedule should enable the prosecutor to make an informed decision about defence disclosure. For example, if an image has been substantially cropped, or only a selective area has been enhanced, it may be necessary for the schedule to state this so that the defence may be made aware of the availability of the uncropped and unadjusted images.

Checklist 8 Completing a Disclosure Schedule Containing Unused Digital Images

Disclosure officers should consider including:

- Information about the application used to capture the image, including whether the image was police generated or third-party generated;
- Information about any digital image material which might reasonably be considered to undermine the prosecution case or assist the case for the accused;
- Purpose of capture or seizure;
- Brief description of what is portrayed by the image and any significant processing applied to the image, eg, cropping;
- Reference to the availability of an audit trail relating to the image, if required;
- Replay software or equipment required;
- Details of any software used to examine unused digital material (including the extent and manner of the examination) and the reason for using the software;
- Any access by the defence to the image(s) and whether this was supervised or in the form of a copy.

4.1.4 EXTENT OF INSPECTION OF UNUSED MATERIAL – IMAGES

Unused material is material that may be relevant to the investigation and has been retained but does not form part of the case for the prosecution against the accused. The principles of disclosure apply to digital images and computer-based electronic evidence in the same way as any other material obtained in the course of an investigation. It is a matter for the investigator to decide which material it is reasonable to enquire into, and in what manner. The receipt of a defence case statement should be a key point in reviewing which material is relevant and which is unused.

Where the viewing officers cannot inspect, view or listen to all the material, the duty to inspect extends to what is reasonable and proportionate in the circumstances of the case. In cases involving a large volume of imagery the investigating officer and the disclosure officer should decide on criteria for prioritising viewing of material. In some cases this decision will be recorded as part of a policy log. In circumstances where it is not practical to view all images or sequences, material should be clearly labelled as unviewed. Any unviewed material should be described by general category and the extent and manner of any inspection or viewing of the material should be recorded with a justification for not having viewed it as part of the investigation. This should form part of the schedule supplied by the disclosure officer. All retained images should be stored as master copies in a retrievable format that allows for replay and viewing, if required.

In circumstances where the defence request to view specific unviewed material, the disclosure officer should ensure that the material is viewed and a viewing log or description of the material has been completed prior to allowing defence access. In cases involving a large volume of material which cannot reasonably be viewed fully, supervised viewing should be considered in order to facilitate defence access.

4.2 REVELATION TO THE CROWN PROSECUTION SERVICE

Existing local service level agreements and protocols should include revelation of all investigative material, including that associated with digital images. Any revelation of digital images to the CPS should be made in a format which is retrievable and viewable. There should also be early discussion about defence viewing, and the most appropriate medium to use when requiring court personnel or magistrates and juries to view material. See **4.3 Transfer of Digital Images to the Crown Prosecution Service.**

Checklist 9 Considerations for File Preparation at Revelation Stage

Officers responsible for file preparation should:

- Ensure that the master copy of the exhibit is kept in suitable and secure conditions by the police, and is made available to the court, if required;
- Liaise with the relevant CPS prosecutor at an early meeting to discuss any issues relating to the capture system or processing carried out, where relevant;
- Provide the CPS with full information accompanying any evidential digital images (exhibits) – this might include audit trails, maintenance logs, viewing logs and disclosure schedules;
- List and describe any unused and/or unviewed material clearly;
- Ensure that viewing logs used for video 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 GPMS marking and the most appropriate method of transferring the imagery to the CPS.
- 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.

4.2.1 DEFENCE ACCESS TO DIGITAL IMAGE MATERIAL

Access to, and disclosure of, digital images which become exhibits should be recorded in the audit trail and case papers when disclosed at police interview stage. At post-charge stage, access should only be allowed after agreement from the CPS. Any access to exhibits and unused material, including copies, should be restricted to those people who have a legitimate role in viewing the image. All access to the images should be documented as part of the audit trail that accompanies each image, and then recorded.

All requests for disclosure of unused images should be recorded. Defence requests should be specific about exactly which images are required for viewing. For example, in the case of unused CCTV video sequences, the defence should be asked to specify the viewing period and the camera positions required. If disclosure of an unused image is facilitated, the following should be documented:

- The date and time at which disclosure was made;
- The identification of any third party to whom disclosure was made;
- The reason for disclosure;
- The extent of the information to which access was allowed, or which was disclosed.

Where the investigating officer and CPS prosecutor decide to allow inspection of images, adequate facilities should be made available where the defence can carry out their examination. Where necessary, there should also be a facility available for the defence representative to show images to the defendant in private. The defence and any forensic experts should not be allowed direct access to a master unused exhibit. There may be occasions when it is appropriate for the investigating officer to allow a defence forensic expert supervised access in order to facilitate the disclosure process, particularly when the defence statement indicates that such an examination is appropriate. In some circumstances supervised access might substantially reduce the cost of decoding or copying material. The investigator should agree this with the prosecutor in advance. In multiple accused cases, the prosecution team should seek to agree an acceptable lead expert to act on behalf of all accused.

If the relevant digital images are third-party images, it may be appropriate to ask owners of data if any breach of confidentiality will occur if the data is disclosed to the accused. Where the disclosure officer or investigator have concerns about differential disclosure of confidential information between co-accused, they should bring these concerns to the attention of the prosecutor. The prosecutor should seek agreement with the defence, and, where appropriate, the court, as to how disclosure may be made.

In situations where the defence is supplied with a copy of an image (working copy), consideration should be given to its potential impact if made public. In some circumstances it might be necessary to employ additional safeguarding techniques to monitor information.

4.2.2 COPYING DISCLOSABLE MATERIAL

Once decisions have been made about the duty to disclose, copies of images might be requested from both the prosecution and the defence. The nature of the material contained within the image should be considered prior to any agreement to copy part or all of it.

Checklist 10 Copying Images

Officers responsible for copying material for disclosure should consider:

- Whether it is appropriate for a copy of the image to be made (some digital images may require that supervised viewing is made available on request);
- The cost of copying, see ***ACPO (2005) Guidance on Charging for Police Services;***
- Making a copy of the master and working copies of digital images;
- Including the audit trail with each image, when required, to enable a comparatively trained practitioner to replicate the steps to achieve the same results from the master copy;
- Ensuring that duties under the DPA are fully complied with and that identities of people other than the accused are fully protected;
- Securing images, for example, using authentication techniques, as necessary;
- Applying the GPMS and copyright, as appropriate;
- Using a unique identifier on the copied material;
- Limiting the number of copies made and recording copy identifiers and recipients as part of the audit trail.

4.3 TRANSFER OF DIGITAL IMAGES TO THE CROWN PROSECUTION SERVICE

It is preferred that, whenever possible, information or data is provided to the CPS in its native format as transferring onto a different format or media will not create exact copies and some loss of the original image quality will occur.

Any conversion to a different format from the native or original format should include consideration and assessment of the quality of the image and whether conversion will significantly reduce the quality.

Efforts should be made to use standard formats for image capture and storage which should be readily available to the CPS and court system. In circumstances where the local CPS branches are unable to readily view material in its original or native format, arrangements should be made to facilitate viewing or convert it into another format. Local protocols, including service level agreements, should be developed to ensure that prosecutors are able to view images quickly in order to make prosecution decisions.

MANAGEMENT ISSUES

- Ensuring that all exhibits and disclosure officers have access to imaging specialists who are able to describe processes and techniques.
- Carrying out regular dip sampling of digital images, as part of the existing quality assurance processes, to ensure that they are accompanied by a full audit trail.
- Working with the CPS locally to ensure the most cost effective and efficient transfer of images for use as part of the criminal prosecution process.

Section 5

RETENTION, STORAGE AND DISPOSAL OF IMAGES

This section describes the decision-making process for retaining and disposing of police information, including associated images. It should be read in conjunction with *ACPO (2006) Guidance on the Management of Police Information, ACPO (2005) Code of Practice on the Management of Police Information* and *HOSDB (2007) Storage, Replay and Disposal of Digital Evidential Images.*

CONTENTS

5.1 RETENTION PRINCIPLES

ACPO has introduced retention and review periods for information and these are outlined in ***ACPO (2006) Guidance on the Management of Police Information*** (MOPI). The following principles relating to digital images are based on information from that document.

5.1.1 STATUS OF VISUAL IMAGES AS PART OF A RECORD AND PERSON RECORD

Any images associated with a police investigation are included as being part of a record for the purposes of MOPI when recorded for a policing purpose. Original exhibits relating to investigations do not necessarily have to be retained, although when they are not retained consideration should be given to retaining a visual image of the exhibit.

Visual images are not necessarily included as part of a person record but may be linked to it. The person record is the minimum information which should be retained if the national retention criteria apply. For further information on recording police information, review, retention and disposal, see ***ACPO (2006) Guidance on the Management of Police Information,*** **Section 4 Recording Police Information** and **Section 7 Review, Retention and Disposal.**

5.1.2 AUTOMATIC AND STATUTORY RETENTION OF IMAGES

Retention refers to the continued storage of, and controlled access to, information held for a policing purpose, which has been justified through the evaluation and review process. Some images will automatically be retained within national information networks. The Code of Practice issued under Part 2 of the CPIA includes a requirement to retain all material relevant to an investigation, at least until proceedings are completed and for the length of a custodial sentence or until discharge from hospital or at least six months from the date of conviction. All material should also be retained in circumstances where an appeal against conviction is in progress or if the Criminal Cases Review is considering an application. The CPIA retention timescales represent a minimum requirement for the retention of police information.

5.1.3 RETENTION OF IMAGES RELATING TO UNDETECTED CRIME

Images associated with undetected crime should be retained according to MOPI principles. For example, records, including associated evidential images, relating to undetected specified offences, as defined in the Criminal Justice Act 2003, should be retained for a period of fifty years from the date that they were reported to the police. 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, for example, eye witness identifications. See **5.1.4 Retention of Images Relating to Detected Crime** and ***HOSDB (2007) Storage, Replay and Disposal of Digital Evidential Images.***

5.1.4 RETENTION OF IMAGES RELATING TO DETECTED CRIME

Decisions relating to retention of images beyond timescales set by the CPIA Code of Practice should be taken locally by the information or records management team. These decisions should be taken as part of the initial review process and according to the principles set out by MOPI. This requires that an evaluation process is applied to images to determine whether they should be stored and then archived as part of a person record. In deciding to retain an image as part of a record, consideration should be given to:

- Adopting a risk focused approach based upon the principles of protecting the public and increasing the ability of the police to build up a composite picture of offending and offenders;
- Assessing the importance of the visual information and its status in evidential terms;
- Evaluating any possible future uses that the image might have for investigators, eg, images showing the demeanour of a witness or offender, or demonstrating changes in the appearance of an offender might have value for future investigations; use as bad character evidence or use by the civil court system;
- Checking whether the information is sufficiently covered elsewhere and if retention of the image would cause unnecessary duplication.

5.2 STORAGE AND ARCHIVING

The terms 'storage' and 'archiving' tend to be used interchangeably. For the purposes of this document, storage refers to the long or short-term holding of imaging data that has the potential to be used as evidence. Archiving refers to the long-term retention of evidential imaging data in a system that allows ease of retrieval.

Any system developed for storage and archiving should also have an assessment store into which all images are initially downloaded and assessed in terms of their relevance to any inquiry. Any images or sequences should be disposed of once they have been assessed as having no value or potential to be used as evidence. In some situations it may be possible for this assessment to be made on the basis of a class of images. For example, all crime scene images are evidential and should be retained past the point of the initial assessment. A useful timeframe for an initial assessment review to take place is at thirty-one days. For further information see ***Information Commissioner (2000) CCTV Code of Practice*** (currently being updated).

5.2.1 ACCESSING STORED AND ARCHIVED IMAGES

Storage and archiving systems (whether based upon write once read many times (WORM), standalone networks, force networks or national networks) should be developed with minimum and maximum timescales for retrieval included as part of the user requirement. Any systems based either on storing visual images with person records or storing images from applications together, eg, all CCTV images, should provide users with reasonable retrieval timescales according to their urgency and potential uses. Some images which might assist in urgent policing matters should be stored in a manner which allows for immediate retrieval and replay.

Indexing systems employed for retrieving images might use the following information as a basis for indexation (separately or in combination):

- Operational name;
- Date of incident;
- Major incident reference;
- Victim's name;
- Offender's name (if known);
- Case number reference.

See ***HOSDB (2007) Storage, Replay and Disposal of Digital Evidential Images*** for a discussion of the advantages and disadvantages of different storage and archiving solutions, and a diagram showing the process of storage and archiving of digital images. See: **http://www.scienceandresearch.homeoffice.gov.uk/hosdb/publications/**

5.2.2 VIEWING

Storage and archive media should be assessed for their capacity for future viewing. This assessment is only likely to be relevant to images stored in the medium to long term. The shorter retention periods of five to six years should usually not affect replay or viewing as the removable media or media player should not degenerate or become obsolete in the short term (although software for replay might require special consideration for future replay). Images stored on removable media should be maintained as per the manufacturers' instructions to provide the best prospect of future replay.

Forces should also consider developing migration strategies for any evidential images which need to be retained for longer periods of time and which are stored on media which might degenerate or become obsolete. For more information about longevity of WORM media, migration and types of storage, see ***HOSDB (2007) Storage, Replay and Disposal of Digital Evidential Images.***

5.3 DISPOSAL

5.3.1 REVIEW OF RETAINED IMAGES LINKED TO A PERSON RECORD

MOPI requires that all police information is reviewed in order to ensure that it is still necessary for a policing purpose, and is adequate and up to date. MOPI also states that any review process should be documented for audit purposes. The review should focus upon the person record and any other information, such as images, which are linked to it. Any images linked to the person record should also be reviewed for their potential to be viewed at the time of the next review, and their necessity to be stored for a further retention period. Any necessary steps should be taken to migrate evidence which might deteriorate before the next review.

Reviews of police information should all be undertaken according to the timescales set by MOPI, and should determine whether the records are necessary according to the framework set by the National Retention Assessment Criteria. All reviews should ensure that person records and any linked information are:

- Necessary;
- Adequate;
- Accurate and up to date;
- Not excessive;
- DPA compliant.

For a full explanation of the review processes and the National Retention Assessment Criteria, see ***ACPO (2006) Guidance on the Management of Police Information.***

5.3.2 DISPOSAL OF DATA AND AUDIT TRAIL

Once an image has been identified as disposable, through either the review system or as part of an automatic process, it should be disposed of with the person record and any other linked information. 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, except in circumstances where information is judged to be extremely sensitive.

In addition, any audit record which holds any personal details and is linked to the information or image should also be subject to disposal. The local IMS should include details of the disposal schedule.

The disposal schedule should be maintained to include the following information:

- Date of decision;
- Number of records;
- Whether the records were considered inadequate or no longer necessary for a policing purpose.

Information should be disposed of in accordance with ***ACPO/ACPOS (2006) Information Systems Community Security Policy.***

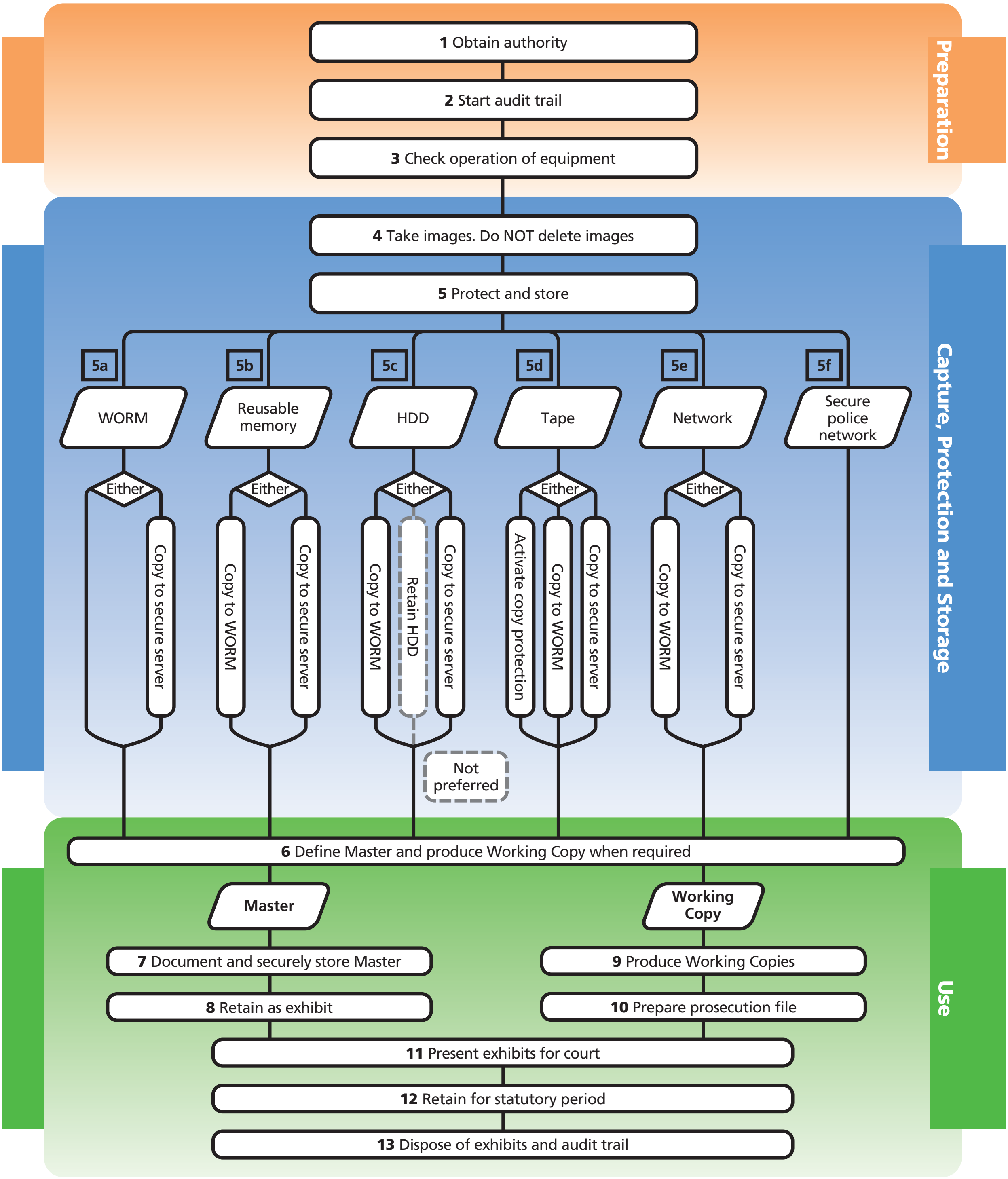
MANAGEMENT ISSUES

- Ensuring that IT storage systems provide the necessary review functions for the purposes of implementing MOPI for images.
- Developing strategies, which are shared by force imaging leads or functions, IT departments and information or records departments, for the review of all retained images.
- Developing and reviewing storage and migration strategies which incorporate developments in technology.

APPENDIX 1
DIGITAL IMAGING PROCEDURE

DIGITAL IMAGING PROCEDURE VERSION 2.0 (NOVEMBER 2007)

Capture and presentation of images from digital still and video recordings.



Reproduced by kind permission of the HOSDB.
© Crown copyright 2007.

APPENDIX 2
GLOSSARY

GLOSSARY

This glossary provides a quick reference to terminology, acronyms and abbreviations used in this practice advice.

ACPO
Association of Chief Police Officers

ACPOS
Association of Chief Police Officers in Scotland

ANPR
Automatic Number Plate Recognition is the automatic image capture and recognition of vehicle registration numberplates and the checking of those details against a number of databases.

Archiving
The long-term retention of evidential imaging data in a system that allows ease of retrieval.

ASBO
Anti-Social Behaviour Order

Audit Trail
The formal record of everything that has happened to an image from capture/point of transfer to disposal. This forms part of the disclosure schedule.

BOF
Back Office Facility – Individual ANPR systems link to an in-force central server known as the Back Office Facility. The in-force BOFs store the time, date, location and direction of travel of the vehicle, together with an image of the numberplate known as a ‘plate patch’. In some cases an image of the vehicle is also stored.

CCTV
Closed-Circuit Television

Colour Balancing
The adjustment of the colour components to reproduce the colour to that of the original.

CPIA
Criminal Procedure and Investigations Act 1996

CPS
Crown Prosecution Service

CRFP
Council for the Registration of Forensic Practitioners

Deletion
The apparent removal of information from a storage medium. In this context deletion differs from disposal in that it is not necessarily a proven means of preventing restoration. Deletion is an insufficient process for removing evidential records.

Digital Images
Digital images include any image (moving or still) captured digitally and stored electronically.

DIP
Digital Imaging Procedure

Disposal (MOPI)
The removal of information from all police systems justified through the review process to the extent that it cannot be restored.

DPA
Data Protection Act 1998

DVLA
Driver and Vehicle Licensing Authority

ECHR
European Convention on Human Rights

Editing
The process of selecting, assembling and sequencing trimmed portions of raw material into a final viewable product. As used in this document the term includes deletion, but not 'selective capture'.

Enhancement
Relates to any process that serves to improve the overall image quality.

FIT
Forward Intelligence Team

FOIA
Freedom of Information Act 2000

Geometric Restoration
Removes geometric distortion of an image, eg, fish eye lens.

GPMS
Government Protective Marking Scheme

Greyscale Linearisation
Adjusts the brightness among objects to reproduce the different brightness values in the scene.

HDD
Hard Disk Drive.

History/Technical Log
A sub-set of the audit trail, normally generated automatically by software applications being used for editing and processing.

HOSDB
Home Office Scientific Development Branch

HRA
Human Rights Act 1998

IMS
Information Management Strategy

Indexing
The use of data (which may or may not be metadata) to facilitate the location and hence retrieval of archived images.

IT
Information Technology

Lossless Compression
Data compression that allows the exact original data to be reconstructed from the compressed data.

Lossy Compression
A method where compressing data and then decompressing it retrieves data that may be different from the original, but is close enough to be useful in some way.

Metadata
Information relating to the image data. In this context only those data which are automatically generated by the capture device or application are meant. This may include:

- Time and date
- Camera number/location
- Software version.

Metadata is sometimes stored with the image file (often leading to a proprietary format) and sometimes separately. Metadata can be considered as part of the audit trail.

MOPI
Management of Police Information

NADC
National ANPR Data Centre

NHS
National Health Service

NHTCU
National Hi-Tech Crime Unit

NPIA
National Policing Improvement Agency

PDA
Personal Data Assistants

PII
Public Interest Immunity

PPI
Pixels Per Inch

Processing
Processing images generally involves adjusting the technical properties of the image and modifying the actual content to improve or change some quality of the image. The use of the term processing in this practice advice should not be confused with the wider definition of processing data with the DPA.

PROMAT
Profile Matching

PSU
Police Support Unit

Retention (adapted from MOPI)
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, Replay and Viewing
Retrieval is the process of accessing image data files; replay is the ability to convert these data files into a viewable format; viewing is the presentation on a monitor. These distinctions are made in this context as it may be possible to access a file, yet be unable to replay and hence view it.

RIPA
Regulation of Investigatory Powers Act 2000

Selective Retrieval
An incident of interest that is identified on a capture system and is required to be downloaded is referred to as selective retrieval.

SOP
Standard Operating Procedure

Storage
The long or short-term holding of imaging data that has the potential to be used as evidence.

UK
United Kingdom

VIPER
Video Identity Parade Electronically Recorded

VRM
Vehicle Registration Mark

WORM
Write Once Read Many Times (eg, CD-Rom).

APPENDIX 3 REFERENCES

REFERENCES

ACPO (2001) *Handling of Protectively Marked Material: A Guide for Police Personnel.* London: ACPO.

ACPO (2003) *National Working Practices in Facial Imaging.* London: ACPO.

ACPO (2004) *Code of Practice for Operational Use of Road Policing Enforcement Technology.* London: ACPO.

ACPO (2004) *Public Order Standards, Tactics and Training Manual.* London: ACPO.

ACPO (2005) *Code of Practice on the Management of Police Information.* Wyboston: NCPE. Available from **http://www.police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/** [Accessed 18 October 2007].

ACPO (2005) *Guidance for the Provision/Viewing of Images Captured by Safety Cameras.* London: ACPO.

ACPO (2005) *Guidance on Charging for Police Services.* London: ACPO.

ACPO (2005) *Practice Advice on Core Investigative Doctrine.* Wyboston: NCPE.

ACPO (2006) *Data Protection Manual of Guidance, Part 1: Standards.* London: ACPO.

ACPO (2006) *Guidance on the Management of Police Information.* Wyboston: NCPE.

ACPO (2006) *Guidance on the Safer Detention and Handling of Persons in Police Custody.* Wyboston: NCPE.

ACPO (2006) *National Fingerprint Manual – Issue 1* [CD-Rom]. Wyboston: NCPE.

ACPO (2007) *ANPR Standards Issue 3.* London: ACPO.

ACPO (2007) *ANPR Strategy for the Police Service (2007-2010).* London: ACPO.

ACPO (n.d.) *Media Advisory Group Guidance Notes.* London: ACPO.

ACPO/ACPOS (2006) *Information Systems Community Security Policy.* London: ACPO.

ACPO and Hampshire Constabulary (2007) *Manual of Guidance: Freedom of Information, Version 4.* London: ACPO.

ACPO/HMRC/SOCA (forthcoming) *Guidance on the Lawful and Effective Use of Covert Techniques – The Legal Framework and Covert Operational Management.*
London: NPIA.

ACPO/HMRC/SOCA (forthcoming) *Guidance on the Use and Management of Surveillance Techniques.* London: NPIA.

ACPO/Home Office (2007) *National CCTV Strategy*. London: Home Office.

ACPO/Home Office (2007) *Digital Imaging Procedure v2.0*. St Albans: HOSDB.

ACPO/NHTCU (2004) *Good Practice Guide for Computer Based Electronic Evidence v3.0*.
London: ACPO.

ACPO/SOCA/HMRC (forthcoming) *Guidance on the Use and Management of Undercover Techniques*. London: NPIA.

Attorney General (2005) *Attorney General's Guidelines on Disclosure*. London:
The Attorney General's Office.
Available from **http://www.attorneygeneral.gov.uk/** [Accessed 18 October 2007].

Criminal Justice System (2004) *Visual Recording of Evidence Within the Criminal Justice System – Equipment Specification*. London: Home Office.

Crown Prosecution Service (2005) *The Prosecution Team Disclosure Manual*. London: CPS.

Home Office (2007) *Achieving Best Evidence in Criminal Proceedings: Guidance on Interviewing Victims and Witnesses, and Using Special Measures.*
London: Home Office.

Home Office Scientific Development Branch (2006) *Briefing Note on Facial Mapping for Video Evidence Analysis Users' Group*. St Albans: HOSDB.

Home Office Scientific Development Branch (2006) *Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems*. Publication No. 21/06.
St Albans: HOSDB. Available from
http://www.scienceandresearch.homeoffice.gov.uk/hosdb/publications/
[Accessed 18 October 2007].

Home Office Scientific Development Branch (2007) *CCTV Operational Requirements Manual*. Publication No. 55/06. St Albans: HOSDB.
Available from **http://www.scienceandresearch.homeoffice.gov.uk/hosdb/publications/**
[Accessed 18 October 2007].

Home Office Scientific Development Branch (2007) *Storage, Replay and Disposal of Digital Evidential Images*. Publication No. 53/07. St Albans: HOSDB.

Home Office Scientific Development Branch (forthcoming) *Guide to Technical Standards for Police Imaging Applications*. St Albans: HOSDB.

Information Commissioner (2000) *CCTV Code of Practice*. Wilmslow: ICO.
Available from **http://www.ico.gov.uk/** [Accessed 18 October 2007].

Police and Crime Standards Directorate (2007) *Guidance for the Police Use of Body-Worn Video Devices*. London: Home Office.