

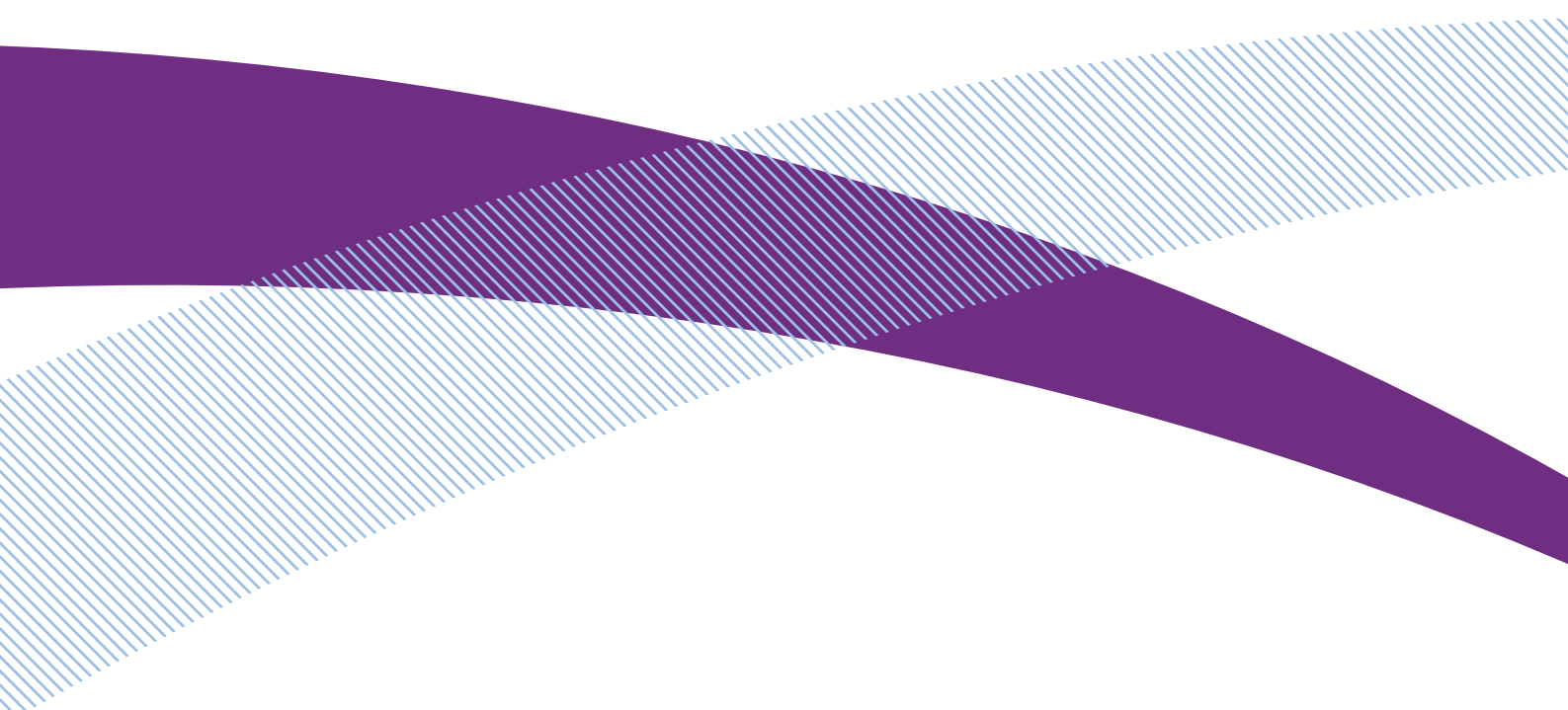


In association  
with



# **Storage, Replay and Disposal of Digital Evidential Images**

Publication No. 53/07





# Storage, Replay and Disposal of Digital Evidential Images

Publication No. 53/07

1.0

# Storage, Replay and Disposal of Digital Evidential Images

Publication No. 53/07

1.0

FIRST PUBLISHED NOVEMBER 2007

© CROWN COPYRIGHT 2007

For information on copyright see our website:  
<http://science.homeoffice.gov.uk/hosdb/terms>

Home Office Scientific Development Branch  
Sandridge  
St Albans  
AL4 9HQ  
United Kingdom

Telephone: +44 (0)1727 865051  
Fax: +44 (0)1727 816233  
E-mail: [hosdb@homeoffice.gsi.gov.uk](mailto:hosdb@homeoffice.gsi.gov.uk)  
Website: <http://science.homeoffice.gov.uk/hosdb/>

# Contents

1	Introduction .....	3
	1.1 Scope .....	3
	1.2 Purpose .....	3
	1.3 Related documents .....	3
	1.4 Types of archive .....	4
2	Overview .....	6
	2.1 New imaging applications .....	6
	2.2 Generic system outline.....	7
3	System considerations.....	10
	3.1 Storage capacity requirements .....	10
	3.2 Reliability and availability .....	11
	3.3 Ease of retrieval .....	12
	3.4 Managing metadata and indexing.....	12
	3.5 Security .....	13
	3.6 Data migration and media longevity.....	14
	3.7 National versus local solutions.....	14
4	Responsibilities .....	16
	4.1 The role of the IT department versus the Imaging department.....	16
5	Requirements template.....	18
	5.1 Overview of the process.....	18
Appendix A:	Definitions.....	21
Appendix B:	Calculation of storage volumes .....	23
	B.1 Introduction.....	23
	B.2 Definition of factors.....	23
	B.3 Storage requirements relating to short-term retention .....	24
	B.4 Storage requirements relating to long-term retention .....	24
	B.5 Example: Helmet cams .....	25
	B.5.1 Short-term storage: year 1 .....	25
	B.5.2 Short-term storage: year 10 .....	25
	B.5.3 Long-term storage: year 10.....	25
Appendix C:	Future storage technology .....	27
Appendix D:	Museum versus migration .....	32

Appendix E:	Media longevity issues .....	34
E.1	Longevity of physical storage media.....	34
E.1.1	Optical media .....	34
E.1.2	Magnetic media .....	37
E.1.3	Hard disk drives .....	38
E.2	Storage, handling and testing .....	40
E.2.1	Optical disks.....	40
E.2.2	Magnetic tape .....	44
E.3	International standards on image permanence .....	45
E.3.1	Introduction .....	45
E.3.2	Traditional photographic media .....	45
E.3.3	Enclosures .....	46
E.3.4	Media for electronic storage .....	46
Appendix F:	Requirements templates .....	48
F.1	Basic template.....	48
F.2	Advanced template .....	50

# 1 Introduction

## 1.1 Scope

This is the first of three technical documents that are being produced in support of the National Policing Improvement Agency (NPIA) ACPO (2007) Practice Advice on Police Use of Digital Images. It covers aspects relating to the storage, replay and eventual disposal of evidential digital images generated by the police, or transferred to them from a third party.

The term “evidential” should in this context be taken to include any image generated by, or transferred to the police, irrespective of the original intention in capturing it i.e. it is assumed initially that all images have the potential to be evidential.

Some of the issues raised are not specific to imaging data, and apply equally well to other forms of digital evidence. However, digital images (especially video) are exceptionally heavy users of storage space and also bring unique difficulties associated with the long-term maintenance of replay capabilities. That said, any discussion of digital image archiving inevitably has to be within the wider context of IT system design. This document is not attempting to cover the IT aspects, but goes as far as providing a template via which the needs of a police imaging unit might be communicated to IT specialists within forces.

The wider issues of transferring images between agencies of the Criminal Justice System, including the processes of revelation and disclosure, are for the present time excluded from the scope. These too, however, will have a bearing on the broader IT system design aspects, in particular on bandwidth requirements.

## 1.2 Purpose

The primary purpose of this document is to set out a generic framework for thinking about storage, replay and disposal of digital evidential images, and to encourage a long-term approach to managing the technology.

Additionally it provides:

- Guidance on specific technical issues such as the calculation of storage capacity needs; longevity of storage media; expected future trends etc. This should obviate the need for forces to conduct their own technical investigations, as well as ensuring consistency of approach.
- Templates for communicating requirements to the IT function.

## 1.3 Related documents

The following related documents should be noted:

- ACPO (2007) Practice Advice on Police Use of Digital Images.

- Home Office/ACPO: Digital Imaging Procedure (DIP) 2007.
- ACPO(2006): Guidance on the Management of Police Information (MOPI).
- “Information Systems Strategy for the Police Service” (ISS4PS).
- ACPO/ACPOS: ”Information Systems Community Security Policy”.
- “Police and Criminal Evidence Act” (PACE) Codes D, E and F.

The above documents have general applicability. Not listed are documents specific to individual police imaging applications.

Relevant definitions are provided in Appendix A.

## 1.4 Types of archive

Note that the 2002 version of the Home Office/ACPO Digital Imaging Procedure mandates the use of WORM (Write Once Ready Many times) media for the storage of master images. This approach has the major advantage of allowing the integrity of the master images to be assured via the same physical security arrangements that are used for other evidential exhibits. However, as the number and size of master images increases, and as technology has progressed, it is recognised that there are significant advantages in permitting secure server storage, the main ones being:

- Reduced physical space needs.
- Accessibility.
- Ease of searching.
- Reduced cost.
- Reduced likelihood of data loss due to degradation over time of physical media.
- Reduced risk of media obsolescence.
- Potential for integration with other forms of digital evidence (e.g. on same case).

These advantages can be gained *if, and only if, the server is maintained and provides an equivalent level of integrity for the images*. It is on this basis that the 2007 version of the DIP permits a range of approaches to the storage of master images, the basic options for which are set out in Table 1.

WORM media may still represent the best option for some applications, especially those requiring relatively modest storage capacity (i.e. stills as compared with video). There may also be situations in which a combination of approaches represents the best overall solution e.g.:

- Use of WORM for legacy images and use of secure servers for newly acquired images (i.e. the cost of transferring legacy images to the network is not warranted).



- Use of WORM for image masters, whereas working copies reside on a secure server.

The concerns relating to WORM media longevity are however significant and have prompted the SWGIT group in the USA to warn against their use for long-term archiving. Reference should be made to section 3.6 and Appendices E1, E2 and E3 for more guidance.

Table 1: Summary of archive options

Option for master image storage		Advantages	Disadvantages
WORM		Integrity assured via physical security. Likely to be in the original format.	Less convenient to search and access (though this may be alleviated by using a "juke box" arrangement). May require considerable physical space. Concerns over media longevity (especially HDD*) and availability of replay hardware and software.
Write protected HDD* or tape.			
Secure server**	Stand-alone PC	Easier to search and likely to be more space efficient than WORM. Gets round the problem of media longevity if managed properly.	Additional measures needed to ensure integrity, though less problematic than when using a network. Concerns over availability of replay hardware and software, though probably easier to manage migration to new formats.
	Stand-alone network	As stand-alone PC plus easier to share/distribute images.	As stand-alone PC with integrity issues exacerbated by network aspect.
	Force network	As stand-alone network but with facility to integrate with other case data. Will generally be subject to formal back-up procedures.	As stand-alone network, but likely also that there will be restrictions on how images may be put onto the network.
	National solution	Applicable only when there is a need to search and share data nationally, usually associated with identification (e.g. Fingerprints; ANPR; FIND etc).	

\* Refers to HDDs recovered from third party systems (as opposed to HDDs which are properly managed and suitably backed up within a secure server environment).  
**The use of this medium for storage of master images is not preferred.**

\*\* The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'RESTRICTED' under the Government Protective Marking Scheme (GPMS), in accordance with the ACPO Community Security Policy (CSP), as documented in an associated Accreditation Documentation Set (ADS) and as approved by either the local Force Information Security Officer and/or the National Accreditor for Police Information Systems.

## 2 Overview

### 2.1 New imaging applications

Digital imaging is a fast moving technology, driven primarily by commercial entertainment/multimedia markets. Performance continues to improve whilst costs decrease, leading to a steady stream of new applications and hence formats.

There is no doubt that the technology has the potential to offer great benefits to law enforcement, but police forces need to be wary of introducing new applications merely because they have the means to do so. It is easy to overlook the problems that a new application may bring with it, especially if full consideration is not given as to how the resultant images will be handled in the long-term. Questions that need to be asked include:

- What will be the evidential value and the limitations of the images? What arguments might be advanced by the defence?
- Will the introduction of this technology have the effect of raising the “evidential bar?” i.e. If there is the expectation that images should always exist, will the testimony of a police officer or other witness be given less weight when they do not?
- Have all of the costs associated with capturing and retrieving the imaging data been identified? For example, will there be a requirement to use specialist technical staff, or the need to replace equipment (such as when hard drives are seized from third party CCTV systems)?
- Has full consideration been given to image storage, migration, retrieval, replay, viewing and disposal, especially given the very long retention periods for serious cases?
- Are proper arrangements in place for image data access and security, as well as for the associated meta-data?
- Have the operating costs of the system been considered (for example the need to employ specialist technical staff such as an archiving officer), and have system maintenance and upgrade costs been included?
- Does this new application comply with legislation and precedence (e.g. Data Protection Act or specific to application) including any likely future changes?
- Where is the technology heading in the longer-term, especially given that it is not driven or controlled by the relatively small law enforcement market? How quickly will the hardware and/or software become obsolete? What will be the implications for the police user?
- Is there a need for a pilot implementation to evaluate the benefits and disadvantages? Have any such pilots been quality assured and their conclusions validated?

Police users clearly have an obligation to think these issues through fully, and only allow the introduction of new applications once the implications of doing so have been properly assessed. Some of the issues are application specific, but it is considered that those relating to storage, replay and disposal can, to a certain extent, be addressed via a generic framework.

## 2.2 Generic system outline

Figure 1 depicts the key elements of a police storage, replay and disposal system. Note that this is part of a larger system that includes the sharing of images across the Criminal Justice System.

Factors affecting the required storage capacity are indicated adjacent to the relevant parts of the system. These are developed into a calculation of the required storage capacity in Appendix B (see section 3.1). Each system component is numbered for ease of reference:

### 1 *Capture/point of transfer.*

This is the process by which the police either generate the image directly, or take possession of it from a third party. Note that the decision on what should or should not be seized by the police is outside of the scope of this particular document, although it obviously has a bearing upon the storage requirements. Note also that a large number of other factors relating to storage capacity needs are determined at this point.

### 2 *Download*

Download is the process by which the images and associated metadata are transferred from the point of capture to a storage medium (the “assessment store” #3). This is not a selective process i.e. everything that is captured must be stored for an initial period whilst an assessment is made as to whether it could have any evidential potential.

### 3 *Assessment store (short-term)*

This is the storage facility to which all images acquired by the police are initially downloaded. The store may or may not be physically separate from the “evidential” medium/long-term store (#6), and depending on the application, may or may not require comparable capacity.

### 4 *Review*

In the context of this discussion, “review” describes the police role of assessing the evidential potential of the images.

### 5 *Delete/overwrite*

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 to take place is at 31 days ( $T_S$ ).

### 6 *Evidential store (medium-long term)*

This is the repository for images that have potential evidential value i.e. all images retained beyond the 31 days ( $T_S$ ) and in certain public protection cases, until the

subject reaches 100 years of age. The retention period ( $T_1$ ) is not in reality a constant, but will vary in accordance with MOPI guidelines and review processes. However, assuming it is constant, #7 illustrates the way in which a new application can quickly commit the police service to a long-term storage obligation as the data aggregates from year to year, and disposal only starts to occur once the retention period has elapsed.

8 *Legacy images*

In planning the capacity of a new storage facility, account must be taken of legacy images (ie those images previously stored under some local system) which it is desired to include (either to safeguard them or to facilitate searching).

9 *Retrieval*

Retrieval is the process of accessing the image file from the store.

10 *Replay*

Replay is the process of successfully generating an image from the image file. This requires the availability of the necessary replay hardware and software.

11 *Viewing*

Viewing is the display of the image on a monitor or via hard copy. It is shown separately from “replay” as the two functions do not necessarily have to be physically collocated.

12 *Editing/Processing*

“Editing” describes the process of selecting, assembling and sequencing trimmed portions of raw material into a final viewable product. “Processing” generally involves adjusting the technical properties of the image and modifying the actual content to improve or change some aspect of it.

13 *Exhibit derived from working copy*

Where an image is edited or processed in some way to create a different version, and becomes the basis of a witness statement, then this variant image must be retained as an exhibit (as well as the original). Refer to ACPO(2007) Practice Advice on Police Use of Digital Images.

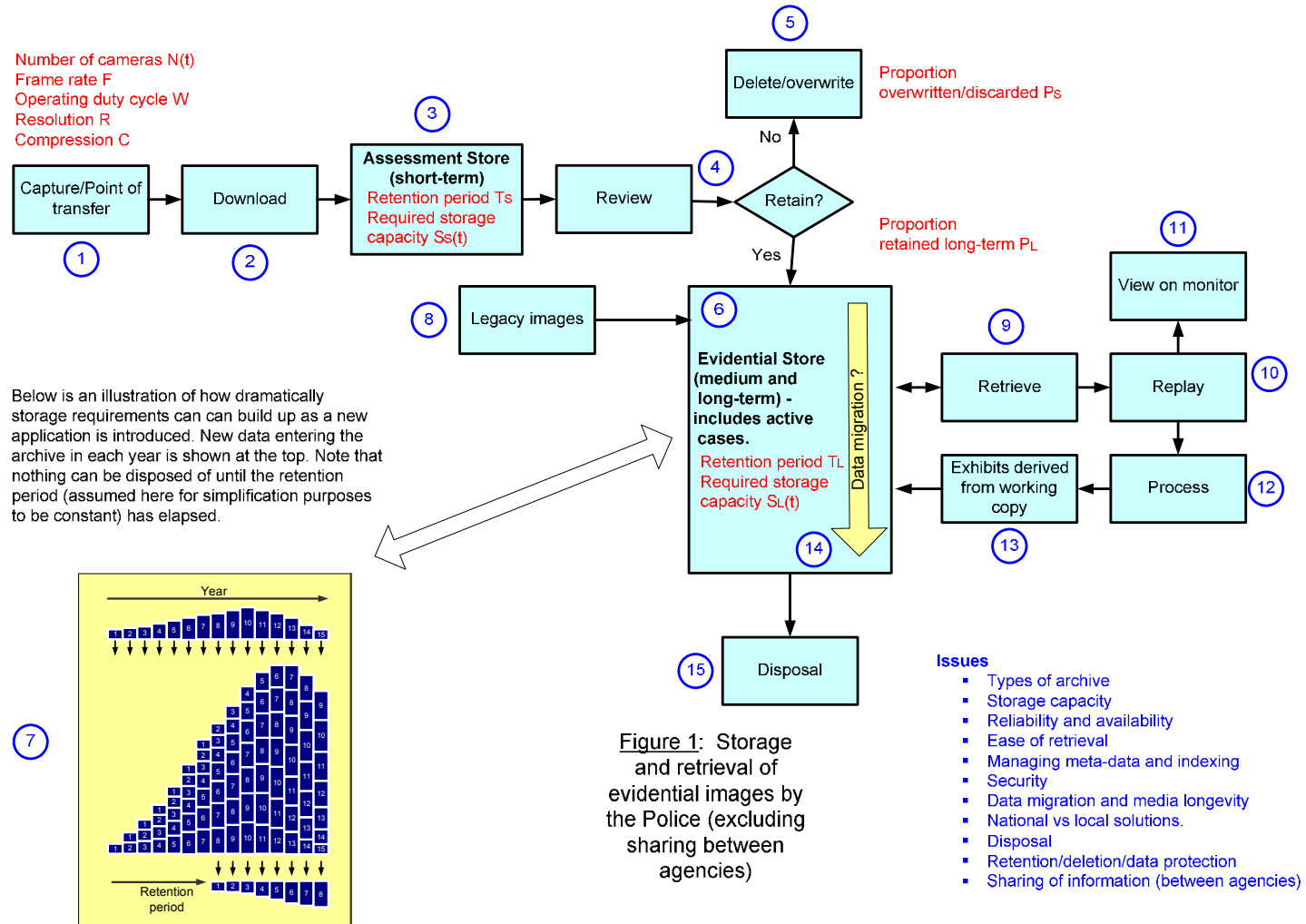
14 *Data migration*

For long-term storage there may be doubts regarding the future ability to replay images, due for example to the uncertain availability of replay hardware and software. One possible solution to this is to periodically migrate the master images to current formats (see also section 3.6). Assuming that data migration is part of the overall information management strategy, the costs for implementing this must be considered at the planning stage. Data migration should only be via formally approved processes, and on this basis there is no requirement to retain the (soon to be unplayable) original master.

15 *Disposal*

Having been retained for the necessary periods, images should be disposed of in a manner that prevents their restoration (see under “Definitions”).

## Storage, Replay and Disposal of Digital Evidential Images



**Figure 1: Storage and retrieval of evidential images by the Police (excluding sharing between agencies)**

## 3 System considerations

### 3.1 Storage capacity requirements

Storage capacity (as a function of time) is probably the most fundamental aspect of the system that needs to be considered – it is easy to embark on a new imaging application without fully understanding the implications for storage, and hence the ensuing costs.

Factors relating to storage capacity are shown in red in Figure 1. A large number of these are determined at the point of image capture. In particular, consideration needs to be given to “operating duty cycle” i.e. the fraction of the time that the camera is recording images. Those applications that run all of the time (i.e. do not operate “selective capture” – refer to ACPO (2007) Practice Advice on Police Use of Digital Images) are particularly storage intensive. The number of cameras, frame rate, resolution and compression are also factors at this point.

Appendix B provides a generic calculation for storage volumes, valid for both video and stills. A hypothetical worked example is given for body-worn cameras which illustrates the way in which a new application can quickly commit the police service to a long-term storage obligation as the data aggregates from year to year, and disposal only starts to occur once the retention period has elapsed. Understanding retention periods is therefore very key. Reference should be made to MOPI, but Table 2 provides a simple overview for the purpose of estimating storage capacity.

Table 2: Simplified overview of retention periods

<b>CPIA as a minimum to cover appeal – typically length of sentence + 6 months.</b>			
<b>Group 1</b>	<b>Group 2</b>	<b>Group 3</b>	<b>Group 4</b>
Certain public protection matters	Other sexual and violent offences.	All other offences.	Undetected crime; CRB disclosures; intelligence products; missing persons; victim/witness details.
Managed under MAPPA. Continue to retain, review every 10 years (in practice until offender reaches 100 years old or dies).	Use the National Retention Assessment – review every 10 years and follow risk based approach (possible escalation to Group 1). This could also require retention until offender is 100 years old.	Retain for 6 years.	Undetected crime: Serious specified offences retain for 50 years. Others 6.  CRB disclosures: Retain for 10 years.  Missing persons resolved 6 years; unresolved indefinitely.  Victim and witness details are as crime type.

Some further points need to be made:

- The police have traditionally stored evidence in accordance with defined retention periods, but under MOPI this is moving to more of a decision based approach.
- In principle some form of actuarial approach is needed to calculate storage requirements. This would be based on an assessment of the numbers of each type of crime (hence the retention periods) coupled with an assessment of the types of images (hence the typical file sizes) likely to be associated as evidence.
- The issue arises as to whether a safety margin should be included within the basic calculation. The recommendation is that a conservative approach should be taken when compiling a business case. However, in reality it is expected that the actual provision of capacity will always be on an expandable/incremental approach so as to avoid the premature or unnecessary outlay of expenditure.
- It may safely be assumed that storage costs will decrease significantly in the future, and therefore to calculate future storage requirements at present day values is unnecessarily pessimistic. Appendix C provides a view of future storage technology.
- The requirements of any legacy images (those already in existence) must be added to the calculations of Appendix B as indicated by #7 of Figure 1. Anecdotal evidence suggests that many forces have local image stores (on CD ROMS, standalone PCs etc) that may not even be visible to the Imaging department. Such local arrangements are unlikely to be safe in the longer-term, and it is strongly recommended that they are brought into a central repository.

## 3.2 Reliability and availability

Any server should be backed up as a matter of course. Depending on the risk assessment, there may be a case for a further level of redundancy to protect against the loss of master images. Consideration also needs to be given to anti-virus protection and power-down. **Note the definition of “secure server” given in section 1.4.**

Force IT systems are generally run as 24/7 operations with availability being set according to the criticality of the data (there are no national standards as such). This raises the issue of whether some images are more critical than others, and whether storage should be organised around this rather than simply according to application. For example, it may be necessary to ensure very high availability of images that relate to terrorist activities. Some forces take the view that such information must be held in dedicated areas in order to achieve this.

There is a particular point of vulnerability if, as in the case of the 7/7 investigation, large quantities of hard disk drives are seized and there is insufficient time to make copies.

### 3.3 Ease of retrieval

Consideration needs to be given as to how quickly it is required to recover images, for example from a cold case that is suddenly linked to a current investigation. This in turn may have implications for the way in which the evidential store is designed.

Obviously retrieval from a secure server is much easier than from a WORM based archive. The following are suggested as minimum retrieval performance requirements:

Table 3: Suggested minimum retrieval performance requirements

	<b>Routine</b>	<b>Urgent</b>
WORM based	12 hours	3 hours
Secure server	1 minute	10 seconds

Note that there may be some technologies that fall between these two eg a mechanical WORM based tower or “juke box”.

### 3.4 Managing metadata and indexing

Metadata is information relating to the image data. In this context we use the term to refer only to that which is automatically generated by the capture device or application (see Appendix A). This may include, but is not limited to:

- Time and date of image capture.
- Camera number/location.
- Software version.

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

All images must have an audit trail associated with them (see ACPO (2007) Practice Advice on Police Use of Digital Images). This will include the metadata and, if the images have been processed, a history log (this will be in electronic form if the processing software is capable of generating it automatically).

Indexing is the use of data (which may or may not be metadata) to facilitate efficient searching and retrieval of images. The indexation system should be developed within the context of local and regional force requirements. See also section 3.7 (National vs Local Applications).

By way of example, the following attributes might be used as the basis of indexation (separately or in combination):

- Operational name.
- Date of incident.
- MIR reference number.



- Victim's name.
- Offender name (if known).
- Case reference number.

Note: A common current practice for WORM based archives is to organize so as to facilitate disposal e.g. placing images into either a 7 year (volume crime) or 30 (serious crime) store. However, this aspect ceases to be important once the images are stored with appropriate metadata on a secure server.

### 3.5 Security

Security requirements should be assessed on the basis of risk.

For server based systems it is sufficient to state that they “should be implemented according to ACPO/ACPOS Community Security Policy”.

The ACPO/ACPOS Community Security Policy (CSP) was ratified in January 2003 and broadly sets down police standards for information security embracing confidentiality, integrity and availability. This policy explicitly cites standards of compliance namely the Manual of Protective Security, BS 7799 and CESG InfoSec standards.

Forces are measured in terms of their compliance with the CSP by way of considering the elements of defence in depth strategy namely policies/procedures, physical security, personnel security and technical security. Key tasks for achievement are identified under each of these headings. A force can legitimately claim compliance with the CSP when it has confidence that all of the elements have been considered, implemented where appropriate and any residual risk accepted at the highest level of management. There is an acknowledgement that this process continues to be the subject of systematic review due to changes that are likely to occur in the baseline standards.

Images are treated no differently in principle from any other form of information in respect of CSP and full cognizance must be taken of the relevant security standards and procedures defined by the CSP in designing imaging systems.

Storage systems that are based on the use of WORM media will generally afford the same level of physical security to the WORM as would be the case for any other evidential exhibit. (reference should be made to section 1.4).

Where a master image is transitioned to a non-WORM system this must be done via an approved and auditable process. The new master will then be designated and the old master disposed of unless it is an exhibit in its own right for some other reason (eg there are fingerprints on the medium).

**Note the definition of “secure server” given in section 1.4.**

### **3.6 Data migration and media longevity**

As noted in sections 1.4 and 2.2 there may be doubts regarding the long-term ability to replay images, due for example to the uncertain availability of replay hardware and software. One possible solution to this is to periodically migrate (ie back record convert) the images to current formats. Appendix D discusses this in more detail (the so-called “museum vs migration” option).

Media longevity may also be a factor for storage systems based on WORM media, similarly requiring migration of data. Refer to Appendix E1 which summarises what is currently known regarding this issue, and also to Appendix E2 which provides storage and handling advice. Appendix E3 summarises the standards work that is on-going in this area.

In considering a “safe” assumption for WORM media longevity and the claims of manufacturers, the following factors have to be taken into account:

- How has the manufacturer defined “failure” i.e. to what extent does the medium have to become unreadable before it is deemed to have failed? Is this an appropriate standard for evidential images?
- What level of confidence do we require? (i.e. what are the consequences of losing data?).
- What type and quality of media were used? How were they written, labelled, handled and stored? This is especially a problem for CDs/DVDs that have come from a third party.

It is assumed that database storage systems will have their storage media periodically upgraded as part of the on-going maintenance of the network.

There are no hard and fast rules on if and when image data should be migrated. It is essentially a risk mitigation activity, and the key point is to be able to justify the decisions that are made on this basis. The following priorities for data migration are suggested however:

1. Unsolved serious crime.
2. Storage media approaching end of safe life – serious crime.
3. Storage media approaching end of safe life – other crime.
4. Player technology becoming obsolete.

Note that data migration should only be via formally approved processes, in order to ensure that there is no question mark over the integrity and evidential content of the migrated images. On this basis there is no requirement to retain the (soon to be unplayable) original master.

### **3.7 National versus local solutions**

There are some applications (e.g. fingerprints; ANPR) where the storage solution is provided nationally rather than locally. This tends to be in areas associated with identification (hence the need for searching) and high mobility. Ultimately this decision should be determined from the business need, having taken into account any need for future-proofing.

In some cases, the master is nonetheless deemed to be held locally (fingerprints being one such example where the lifts are regarded as the

master, and a copy held on Ident1). It may be therefore that, by storing at both local and national level, we are making the storage problem bigger than it needs to be. Any decision to remove the requirement for retention of the local master, may only be made by the recognised ACPO Portfolio. Local (especially unofficial) storage systems that have the potential to undermine agreed national solutions should not be permitted.

## 4 Responsibilities

### 4.1 The role of the IT department versus the Imaging department

The provision of an archiving facility for digital evidential images should be seen as a matter for partnership working between the force IT department and the force Imaging department\*. This is a somewhat idealistic view, given that forces are not uniformly organised. Some for example have outsourced their IT, whilst others may not have an Imaging department as such. Nevertheless, the underlying principles of what follows remain sound.

Figure 2 illustrates the situation that exists to a greater or lesser extent in all forces. Generally there will be a range of imaging applications active within force. Some of these will be centrally managed, but others may be local and possibly not even visible to the central imaging function. Storage arrangements for these local applications will tend to be ad hoc (standalone PCs, CD ROMS in cupboards etc) and probably unsafe in the longer-term. Forces are strongly encouraged to identify a single “owner” of all images (normally the manager of the Imaging department) as the first step in providing a robust solution for image storage. This will be referred to as the “central model”.

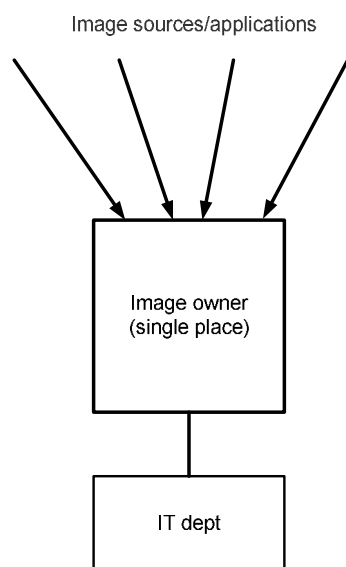


Figure 2: The central model

On this basis the relative responsibilities of the partners may be summarised as follows:

#### ***Imaging department\****

- Is the image owner (also the owners of all associated meta-data), hence responsible for policy relating to image capture and usage.

- Is responsible for ensuring that all local applications are brought under central control.
- Should be given the opportunity to contribute to all business cases for new imaging applications to ensure that they have been properly considered, as part of a coordinated procurement strategy.
- Is responsible for forecasting storage needs and defining requirements for implementation by the IT dept.
- Is governed by documents such as the ACPO (2007) Practice Advice on Police Use of Digital Images and the Home Office/ACPO Digital Imaging Procedure.
- Probably does not include IT specialists and will therefore lean heavily on advice from the force IT department.

### ***IT department***

- Is the owner of the IT infrastructure, including aspects such as reliability, security, and access control.
- Holds responsibilities that are much broader than the provision of IT for digital evidential images.
- Is governed by documents such as the ISS4PS, Core DM and local force information management strategy as defined by MOPI.
- Is responsible for guiding the formulation of, and responding to, the IT requirements of the Imaging department.
- Is accountable to the information compliance function (which may or may not be a separate group).
- Probably does not have imaging background, and may therefore be unfamiliar with some of the concepts and terminology.

The differing perspectives of the Imaging and IT departments, if not properly recognised, can lead to misunderstanding and conflict. Imaging departments are interested in viewing images, whilst IT departments are concerned with security. Some forces do not allow CD/DVD drive access to their network (for fear of viruses), making viewing of images inconvenient (although images can of course be put onto the network via the IT function). This is probably one of the main underlying reasons why most forces have seen a proliferation of standalone systems for imaging, the aim being to by-pass the force network.

*\* NB The term “Imaging department” is essentially used here to mean a central owner of the images (which may be a nominated individual). This does not impose a requirement on forces to create such a department as this may be inappropriate given the scale of their imaging operations.*

# 5 Requirements template

## 5.1 Overview of the process

It was stated earlier that the Imaging department is “responsible for forecasting storage needs and defining requirements for implementation by the IT dept”. This is by no means an easy task, especially if there are multiple imaging applications to be considered. The fact nevertheless remains that IT departments need good information if they are to come up with good solutions.

Figure 3 illustrates the recommended process:

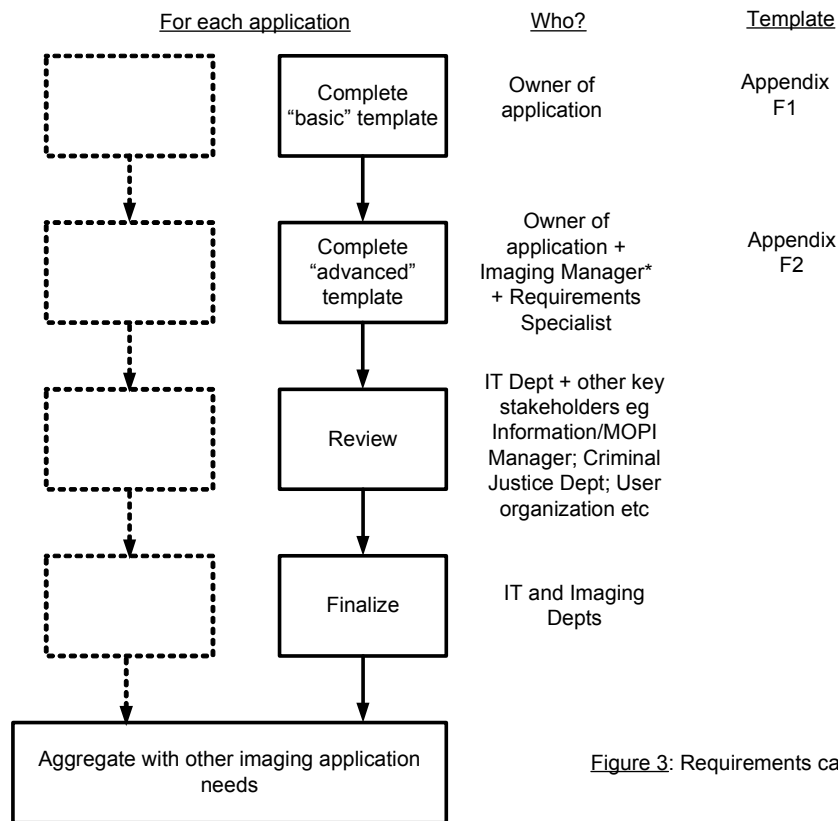


Figure 3: Requirements capture process

The local owner of each application (i.e. the person who is introducing it or knows most about it) completes a “basic” template (Appendix F1) that in effect registers the need for IT provision. This goes to the Imaging department (\* or “image owner” as described previously).

A more in-depth template (Appendix F2) is then completed. This is a much more difficult matter, so it is proposed that assistance is provided by a “requirements specialist” i.e. someone who has been specifically trained in this process. Typically there will need to be one or two such people in each force, and in many cases this may include the Imaging Manager.

## Storage, Replay and Disposal of Digital Evidential Images

The completed second template is then passed to the IT department and any other key stakeholders (eg Information/MOPI manager), prior to all relevant parties meeting to finalise the content.

The IT department will in most cases wish to aggregate this with the needs of other imaging applications and indeed with more general IT requirements in order to produce an optimum solution.

Circumstances will of course change (or predictions proven to be wrong!), so it is likely that the requirements will have to be validated or amended from time to time.

**IMPORTANT NOTE RELATING TO APPENDICES**

Various web site and other references are provided for information in the appendices which follow. The Home Office Scientific Development Branch does not vouch for the content of these references, nor should they be taken as representing the views of the Home Office.



## Appendix A: Definitions

### *Archiving*

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

### *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.

### *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.

### *Disposal (MOPI)*

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

### *History/technical log*

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

### *Indexing*

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

### *Metadata*

Information relating to the image data. In this context we mean only those data which are automatically generated by the capture device or application. 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.

### *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.

*Storage*

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

*SWGIT*

The Scientific Working Group on Imaging Technology (USA).

*WORM media*

Write Once Read Many times (e.g. CD ROM).

## Appendix B: Calculation of storage volumes

### B.1 Introduction

The aim is to provide a simple generic framework for estimating the storage capacity likely to be needed for evidential images, so that:

- The main factors affecting this are identified.
- We are able to gauge the likely scale of the future storage requirements.

The framework should be valid for both video and stills images. Recent discussions re helmet-cams is used as a worked example.

### B.2 Definition of factors

**N(t)**

is the number of cameras relating to the application in question at a particular point in time  $t$ . This number can relate to a force, region etc.

**F**

is the frame-rate/number of images captured per second by each camera while it is operating.

**W**

is the fraction of the time that each camera is operating.

**R**

relates to the number of pixels in each individual image (resolution).

**C**

is the level of compression that is applied to the image e.g.  $C = 0.1$  for a compression ratio of 10.

**T<sub>S</sub>**

is the short-term retention period, during which the evidential value of images is assessed.

**T<sub>L</sub>**

is the long-term retention period for those images that have evidential value.

**P<sub>S</sub>**

is the proportion of the images that is retained for the short period ( $T_S$ ) before being overwritten or discarded.

**$P_L$**

is the proportion of the images that is retained for a long period ( $T_L$ ) because of its evidential value.

**$S_S(t)$**

is the short-term storage requirement.

**$S_L(t)$**

is the long-term storage requirement.

**$S(t)$**

is the required storage for the images (excluding any associated information). It is equal to the sum of the short period storage requirement  $S_S(t)$  and the long period storage requirement  $S_L(t)$ .

$N(t)$ ,  $S_S(t)$ ,  $S_L(t)$  and  $S(t)$  vary with time. All of the other factors are assumed to be constants.

### **B.3 Storage requirements relating to short-term retention**

On the assumption that the short-term retention period is small compared with the rate at which the number of cameras  $N(t)$  is changing, the amount of data entering the store is approximately equal to the amount of data leaving the store, and the associated storage requirement is:

$$S_S(t) = N(t) * F * W * R * C * P_S * T_S \quad (\text{eqn 1})$$

### **B.4 Storage requirements relating to long-term retention**

This is more complicated because  $N(t)$  may vary considerably over the retention period, and the amount of data entering and leaving the store will be different. Generally we would expect at time  $t$  that:

$$\text{Data entering the store} = N(t) * F * W * R * C * P_L$$

$$\text{Data leaving the store} = N(t - T_L) * F * W * R * C * P_L$$

Hence the net change in storage requirement between times  $t_2$  and  $t_1$  is:

$$F * W * R * C * P_L \int [N(t) - N(t - T_L)] dt. \quad (\text{eqn 2})$$

The effect of the integral is to sum up the net flow of data into the store over the period between times  $t_1$  and  $t_2$ .

## B.5 Example: Helmet cams

### B.5.1 Short-term storage: year 1

Assume there are currently ~ 50 helmet-cams being deployed in the Plymouth area, full time across 3 x 8 hour shifts. They are recording at 25 frames per second at a resolution of 720 x 576 pixels. Format is MPEG4 with a compression ratio of 50:1. All images are routinely retained for 31 days before being overwritten.

$$N(t) = 50$$

$$F = 25 \text{ Hz}$$

$$W = 1$$

$$R = 720 \times 576$$

$$C = 0.02$$

$$PS = 1$$

$$TS = 31 \text{ days } (31 \times 24 \times 60 \times 60\text{s})$$

Hence  $S_s(t)$  is approximately 28 Terabytes

### B.5.2 Short-term storage: year 10

Suppose that the deployment of such cameras increases linearly within Devon and Cornwall so that by year 10 there are 500 cameras operating in the same way.

$N(t)$  is now 500, all other factors being the same.

Hence  $S_s(t)$  is approximately 280 Terabytes

### B.5.3 Long-term storage: year 10

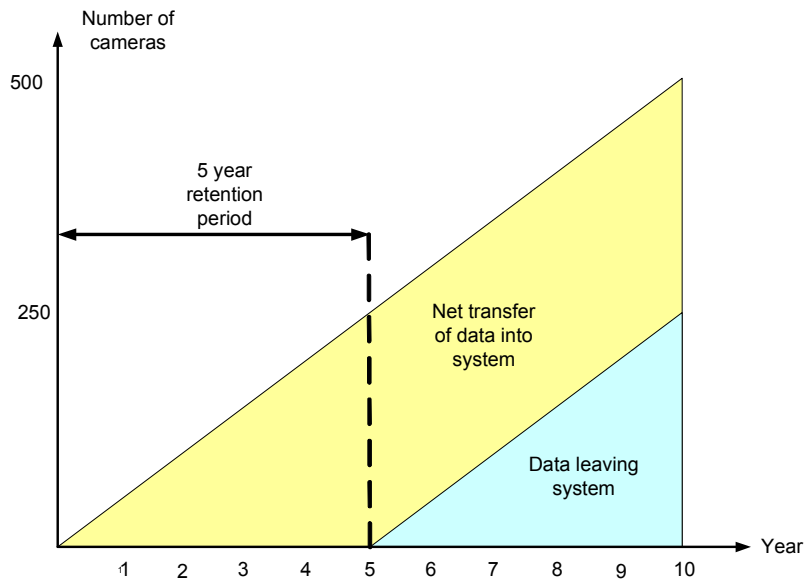
In addition to the short-term (31 day) storage, assume that 5% of images have to be retained for 5 years. ie  $P_L = 0.05$  and  $T_L = 5$  years.  $N(t) - N(t-T_L)$  is depicted in the following table:

End Yr	1	2	3	4	5	6	7	8	9	10
$N(t)$	50	100	150	200	250	300	350	400	450	500
$N(t-T_L)$	0	0	0	0	0	50	100	150	200	250
$N(t)-N(t-T_L)$	50	100	150	200	250	250	250	250	250	250

This shows that the *rate* at which the storage requirement increases will itself increase up until year 5 after which it is constant (the storage requirement itself will continue to increase thereafter at a steady rate).

The integral in (eqn 2) can be approximated by summing the bottom row of the table (this adds up to 2000 camera-years). On this basis, the long term storage requirement (assumed starting from zero) will, by the end of year 10, have grown such that  $S_L(t)$  is approximately 646 Terabytes.

The diagram below illustrates the situation. The larger triangle represents data entering storage. The smaller triangle represents data leaving storage (i.e. no longer required because the retention period has expired). The difference between the two represents the net transfer of data into the storage system.



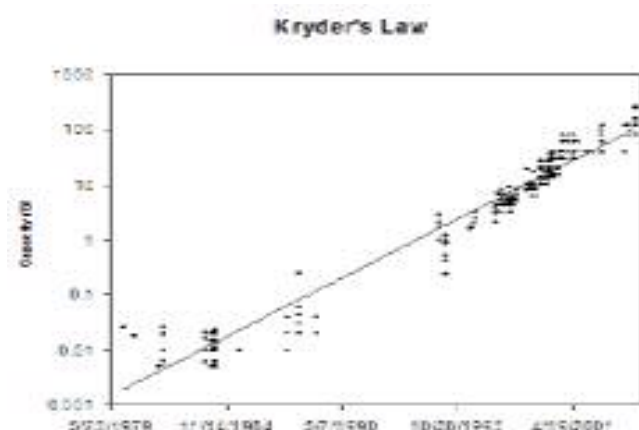
## Appendix C: Future storage technology

The future of storage technology can be split into two key areas:

- Portable storage media, for which the current (and speculative) trend indicates the growth of solid state media and optical media formats.
- Larger scale storage in the form of high capacity Hard Disk Drives (HDD), Solid State Disks (SSD) and in larger scale deployment Storage Area Networks (SAN).

Whilst a SAN is dependant on network technology the actual physical storage is undertaken by individual drives. The current most common device is the HDD. Advances in HDD technology can be predicted with Kryder's "law":

**Kryder's law** states that hard drives (HD) are benefitting from an exponential increase in the density (bits per unit area) of information they are able to store. Kryder's law is essentially Moore's "law" for storage.<sup>1</sup>



Extending the trend-line indicates firstly that in 2006 we appear to be on track with the 2001 predictions assumptions, and secondly that in 2012 HDD storage capacity should be around 5 terabytes per drive and by 2017, 50 terabytes. The prediction for 2012 is in part validated by the Seagate research indications. The prediction for 2017 is solely based on Kryder's law.

P C hard disk capacity (in GB). The plot is logarithmic in the y-axis so the fit line corresponds to exponential growth.

There is a further cost based law<sup>2</sup> that indicates that the cost of storage halves every 12 months whilst the capacity doubles although there is very little supporting information for this premise other than 'Moore's law'<sup>3</sup> and its associated progress.

<sup>1</sup> [http://en.wikipedia.org/wiki/Kryder%27s\\_law](http://en.wikipedia.org/wiki/Kryder%27s_law) – last accessed Aug 2007

<sup>2</sup> [http://en.wikipedia.org/wiki/Kryder%27s\\_law#External\\_links](http://en.wikipedia.org/wiki/Kryder%27s_law#External_links) – last accessed Aug 2007

<sup>3</sup> [http://en.wikipedia.org/wiki/Moores\\_law](http://en.wikipedia.org/wiki/Moores_law) – last accessed Aug 2007

SSD technology is certain to be a growth area over the next 10 years. [Storagesearch.com](http://www.storagesearch.com) indicate the 3 most common trends for the past 7 years as:

- **Network storage** (SAN / Server technology)
- **Backup media** (migration away from tape based backup)
- **Semiconductor storage** (development of Flash media)

And they predict the next 7 years main trends as:

- **Compliance and security** (integrating and securing SANs and operating platforms)
- **Reliability** (linked to reliance on SAN and RAID/server style storage)
- **Solid state disks** (growth and dependence on SSD technology) <sup>4</sup>

The following tables display emergent or established development areas. The main area of advance is the optical market – this appears to be the main format for portable storage media. **The performance figures are obviously liable to change and should be taken as indicative only:**

Generic	Optical
Format Name	<b>BLURAY</b>
Capacity	50 GB (46.6 GiB) (Dual Layer)
Physical Size	12 cm, single sided diameter
Transfer Rate	54 Mbit/s (1.5x)
ETA	Available now.
Notes	About 23 hours of standard-definition (SD) and 9 hours of HD video can be stored on a 50 GB disc
Reference	<a href="http://news.sel.sony.com/en/press_room/b2b/media_app_systems/release/24099.html">http://news.sel.sony.com/en/press_room/b2b/media_app_systems/release/24099.html</a>

Generic Type	Optical
Format Name	<b>HD DVD</b>
Capacity	30 GB (Dual Layer)
Physical Size	12 cm, single sided diameter
Transfer Rate	36.55 Mbit/s
ETA	Available now.
Notes	Over 8 hours HD from 30GB disk
Reference	<a href="http://www.thelookandsoundofperfect.com/">http://www.thelookandsoundofperfect.com/</a>

<sup>4</sup> <http://www.storagesearch.com/news11.html> - last accessed Aug 2007 - **STORAGE search** tracks the top 1,000 storage companies from birth to death and related storage technologies and markets. It's published by **ACSL**



Generic Type	Magnetic
Format Name	<b>Hard Disk Drive (current technology)</b>
Capacity	120 GB (Typical) – 1TB (Maximum)
Physical Size	3.5"
Transfer Rate	From 133Mbit/s (PATA, SATA) to 3000Mbit/s (eSATA II). UWSCSI is ~320Mbit/s.
ETA	Available now.
Notes	
Reference	

Generic Type	Optical
Format Name	<b>Versatile Multilayer disk</b>
Capacity	5 GB per layer (up to 10 layers)
Physical Size	12cm diameter
Transfer Rate	40 Mbit/s
ETA	?
Notes	1-and 2-layered version announced. Experimental 4-layer versions some way ahead.
Reference	<a href="http://www.nmeinc.com/">http://www.nmeinc.com/</a>

Generic Type	Optical
Format Name	<b>Enhanced Versatile Disk</b>
Capacity	Not Known
Physical Size	12 cm
Transfer Rate	Not Known
ETA	Not Known
Notes	EVD is not likely to be a major focus of future industry deployment efforts
Reference	<a href="http://en.wikipedia.org/wiki/Enhanced_Versatile_Disk">http://en.wikipedia.org/wiki/Enhanced_Versatile_Disk</a>

Generic Type	Optical
Format Name	<b>Forward Versatile Disk</b>
Capacity	5.4GB of storage per layer (Up to 3 layers)
Physical Size	12 cm, single sided diameter
Transfer Rate	
ETA	Available now?
Notes	Red laser technology - an offshoot of DVD. 135 minutes of 1080i video on a 3-layer disc
Reference	<a href="http://www.eol.itri.org.tw/En/Research/research_4_a1.asp">http://www.eol.itri.org.tw/En/Research/research_4_a1.asp</a>

Generic Type	Solid state
Format Name	<b>Solid State Disk</b>
Capacity	Up to 64Gb
Physical Size	2.5", 3.5"
Transfer Rate	USB 2.0 (480 Mbit/s)
ETA	Available now.
Notes	
Reference	<a href="http://www.storagesearch.com/bitmicro-art3.html">http://www.storagesearch.com/bitmicro-art3.html</a>

Generic Type	Optical
Format Name	<b>Holographic Versatile Disk</b>
Capacity	3.9 Terabytes
Physical Size	12 cm diameter
Transfer Rate	1 Gigabit/second
ETA	
Notes	Optware is expected to release a 200GB disc, and Maxell with a capacity of 300GB and transfer rate of 160 MBit/s.
Reference	<a href="http://www.hvd-forum.org">http://www.hvd-forum.org</a>

Generic Type	Magnetic
Format Name	<b>Hard Disk Drive (IDE Future)</b>
Capacity	7.5 Terabyte
Physical Size	3.5"
Transfer Rate	Not Known
ETA	Not Known
Notes	Seagate Announced research in 2006
Reference	

This table is chronological where release data is available. Most of these technologies appear to have versioning releases or they are an improvement on current technology. As the technology improves the currently available format may not accurately reflect the capabilities and capacities of the final version.

Other notable areas of work include Super Slim Laser Technology<sup>5</sup> (SSLT) and biological storage types<sup>6</sup>

SSLT is an interesting enhancement to the lasers used in the reading and writing of optical storage media. The impact of this enhancement has not been measured but anecdotally it is expected to improve the potential of optical media types by some 1000%.

Biological storage is mooted as being a possible longer term storage platform. Current research is investigating the use of protein and molecular based memory, although at this time there is very little qualitative information available about these methods and capabilities.

---

<sup>5</sup> <http://www.pinktentacle.com/2006/06/super-sharp-lasers-to-boost-disc-capacity-tenfold/> - last accessed Aug 2007

<sup>6</sup> [http://www.doc.ic.ac.uk/~nd/surprise\\_97/journal/vol1/ary/#how](http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol1/ary/#how) – last accessed Aug 2007

## Appendix D: Museum versus migration

The considerations for devising a coherent archival strategy appear to focus on three main points:

1. Media longevity
2. Format evolution
3. Technology evolution

A fundamental issue to address is: ‘what is important, the original item or the content of the original item?’ If the archive value is in the physical medium then the clear option is a museum type approach (ensuring the artefact is maintained in conditions conducive to longevity). If the value is in the content (which is generally the situation we are considering) then other archive options have to be considered.

A second key issue is the length of time that the artefact (in this case image) needs to be archived for. If this exceeds the safe life-time for the medium (see section 3.6) re-proving (re-writing and validation of the new version) will need to be considered within the artefact’s archive lifespan.

The next issue is that of the longevity of the media format. Current trends indicate that there is a major shift in the common media of choice roughly every 12 years (and this mean time between format change is decreasing). If the data is unreadable because there is no comprehension of the data format then preservation of the physical media has been valueless.

The third question is that of available technology. Even though the artefact has been successfully preserved and there is a good local knowledge of the anticipated data format (perhaps it is still in use), the data is only accessible if there is an extraction tool to remove it from the storage medium into a presentable form. Consideration therefore has to be given to providing a suite of legacy media reading equipment to ensure data is accessed regardless of format.<sup>1</sup>

These pointers indicate that a migration route would offer the best preservation of critical data. The main concerns with this route are that of cost and time. Depending on the size of the archive and the format of the data (some migration methodology could be automated) the impact in time and new media to commit the old data could well become costly. Also the archival process requires managing and as such an archivist is needed to ensure that migration routes are adhered too, and frequent technology audits are undertaken to ensure format and technology selection represents the best choice for the content (and subsequent content usage).

---

<sup>1</sup> Consider the case of the BBC Domesday Book, developed as a snapshot of the nation in 1986. The data lasted for less than 20 years as it was committed to a storage system only the BBC used. Once the infrastructure broke down the data was valueless – until recent success after much effort to recover the data by BBC researchers. <http://www.atsf.co.uk/dottext/domesday.html#whtd> – last accessed Aug 2007.

Another consideration is that of format change. If data is being trans-coded from one format to another it becomes imperative to ensure that each migration is both lossless and adds no superfluous or spurious data to the original content.

A final consideration is that of audit trail – it becomes evidentially imperative to be able to prove the lineage of the master copy of any evidence. Any re-versioning of content must be via formally approved processes and have a clear and established audit trail. On this basis there is no requirement to retain the original (soon to be unplayable) original master.

## Appendix E: Media longevity issues

### E.1 Longevity of physical storage media

This research was split into two main areas, optical media (e.g CD, DVD etc) and magnetic tape.

A number of organisations were contacted, including the BBC, The National Archive, The Digital Preservation Coalition, JISC (Preservations), The British Library and the Library Of Congress (The National Digital Information Infrastructure and Preservation Program). Much of the work being undertaken by these organisations focuses more on the content of the media rather than the physical properties of the media itself, the main argument being that there is little point maintaining some media source for 30 years if there is no replay system to extract the content of the media source. All parties advocated the migration route and some information and contacts were collated that might be of interest to other research areas (e.g. “migration” versus “museum”).

In addition International Standards now cover some of these issues. These standards cover test methods, specifications and care and handling advice. In addition to being kept up to date through a regular revision schedule they contain an accumulation of international expertise on these issues as they are arrived at through a consensus from “manufacturers, vendors and users, consumer groups, testing laboratories, governments, engineering professions and research organizations”.<sup>1</sup>

One of the largest problems with establishing ageing data for media formats was reported as the validity of accelerated ageing processes. Some of the optical media formats are still relatively young when compared to other mature media formats such as magnetic tape. However, some of these procedures are now the subject of International Standards.<sup>2,3,4</sup>

#### E.1.1 Optical media

In addition to International Standards one source of useful information was the cdrfaq website<sup>5</sup>. cdrfaq.org is a creative commons based community website that collates information from across a large users group (predominantly from the Usenet newsgroup comp.publish.cdrom) The resultant information is heavily peer reviewed offering a valuable open source resource.

Optical disk storage media have been used for professional data storage since their appearance in the early 1990s. This started with the recordable CD format (CD-R)

---

<sup>1</sup> See <http://www.iso.org/iso/en/stdsdevelopment/whowhenhow/how.html>, last accessed July 2007.

<sup>2</sup> BS ISO 18924:2000, “Imaging materials. Test methods for Arrhenius type predictions”, ISBN 0 580 36425 9

<sup>3</sup> BS ISO 18921:2002 “Imaging materials. Compact discs (CD-ROM). Method for estimating the life expectancy based on the effects of temperature and relative humidity”. ISBN 0 580 40028 X.

<sup>4</sup> BS ISO 18927:2002, “Imaging materials. Recordable compact disc systems. Method for estimating the life expectancy based on the effects of temperature and relative humidity”, ISBN 0 580 39106 X

<sup>5</sup> <http://www.cdrfaq.org/faq.html> – Last accessed July 2007

and latterly moved to the larger capacity recordable DVD formats. It is unlikely to stop here with newer high density media giving more favourable cost per GByte storage ratios.

It soon became apparent that the finite lifetime of the stored data was an issue. For example, it is noted that “A CD-ROM of good manufacture should last several years or even decades”.<sup>3</sup> A similar figure is given for CD-R media.<sup>4</sup> Most studies covered the life expectancy of the storage media in isolation. It is noted that the different media behave differently which is not surprising as they contain different reflecting layers, substrates and dye systems.

However, the problem is more complex than this as the storage of data and subsequent replay has to be treated as a system. The system can be considered to consist of the following elements:

1. The optical disk writer (the “burner”).
2. The optical medium.
3. The storage conditions and handling of the media.
4. The optical disk player.

Only items 2 and 3 in the above list are standardised and, as 1 and 4 are not, the data quality and overall life expectancy is to a certain extent unpredictable. As a result some testing of individual systems is necessary to ensure data integrity. One particular variable of note in this system is the race for ever faster read and write speeds. Recordable disks optimised for higher speed writing may have less image retaining dye and the effect on longevity is not publicly known. A particular disk brand will probably have a write speed that optimises performance that can only be found by testing.

It should also be noted that although optical media are subject to some standards these cover only the data and physical format. Longevity is not covered so it is up to the user to put in place procedures to maximise this. Error measurement in particular is a key metric to ensure longevity. A disk with a high error rate may register as readable upon verification immediately after being written but fail within a relatively short space of time.

Various manufacturers’ studies indicate that the life expectancy of well manufactured optical discs is in excess of 50 years under typical ambient room conditions.<sup>3</sup> However, it should be noted that the rapid rate of technology change in this market may effectively render a storage medium unreadable before the end of life point of the media is reached. As an example, many tape drive formats and the 8 and 5¼ inch floppy drives are no longer available. Unless the hardware and software to read these media were suitably archived too, or migration strategies put in place, this data would now be unavailable.

There are a number of different optical media types, these have been split into factory pressed media and user burnable.

### **Factory pressed media**

By some estimates, pressed CD-ROMs may only last for 10 to 25 years, because the aluminium reflective layer starts to corrode after a while, a phenomenon known as “disk rot”.

### **User burnable**

Methods for testing lifetime viability are still in their infancy. An International Standard, presently under periodic revision covers accelerated testing but only for the effects of temperature and relative humidity.

### **Recordable CDs (CD-R)**

These disks can be recorded and not erased and re-written, commonly known as WORM (Write Once Read Many). They contain a dye layer and a reflective surface. The dye layers can use one of three different technologies. These are cyanine, phthalocyanine and azo. While various claims are made for the relative permanence of these technologies it is believed that of the 3 cyanine technology has the lower life expectancy. Unfortunately, colour of the disk is not a good indication – both cyanine and azo technologies can give similar disk colours.

The manufacturers claim 75 years (cyanine dye, used in "green" discs), 100 years (phthalocyanine dye, used in "gold" discs), or even 200 years ("advanced" phthalocyanine dye, used in "platinum" discs) once the disc has been written. That said, because of the popularity of CD-R there is a wide choice of manufacturers and brands. Unfortunately associated with this is a wide variation in disk quality, many of which may not be of adequate quality for long term use.<sup>6</sup> Predicted lifetimes cover a wide range from 25 to over 250 years which vary with the manufacturer and the disk type.

The type of metal used in the reflective layer is a further variable with CD-R disks. Aluminium is not used in CD-R as it can interact with the dye layer. Silver too can lose reflectivity due to atmospheric pollutants such as sulphur dioxide. Silver alloys are therefore used to inhibit this effect.

While manufacturers of gold disks consider these to give the best permanence performance there is a problem in that the adhesion of gold to the polycarbonate substrate is believed to be inferior to silver in some circumstances. In general in terms of stability, aluminium < silver / silver alloy < gold.

### **CD-RW**

CD-RWs (write once read many times) are expected to last about 25 years under ideal conditions. Repeated rewrites will reduce this time. The shelf life of an unrecorded disc has been estimated at between 5 and 10 years.

---

<sup>6</sup> M Mizen, "The Role of Product Testing in Digital Fulfillment", IS&T's International Symposium on Technologies for Digital Fulfillment, 2007.



There is a standards document called the orange books <sup>7</sup>, but it does not explicitly state a longevity criteria, more so a set of criteria governing the whole CD family of media.

## E.1.2 Magnetic media

Some of the information for magnetic tape media was established through conversations with various organisations, predominantly ‘Imation’<sup>8</sup> who are a significant manufacturer of storage media. Additional information came from international standards.

### **3590, 3590E data cartridges [wide width tape – 1 inch+]**

Imation warranty data tapes for 30 years (long length usage 400 full file read while write passes, short length – 120,000+ read forward passes). This is linked to storing the data in a controlled environment, with temperature and humidity being the main two factors.

The main problem is changes to environment. The tape is more forgiving of a constant  $\pm$  few degrees temperature or Relative Humidity percentage points deviation from the specified values than frequent changes in conditions.

### **‘DAT’ style [small width tape – 4mm, 8mm etc]**

Warranty period is set as less; 2 years (or 5000 read/write passes) as usage is more likely to be in ‘normal’ office conditions as opposed to a controlled archive environment. There is a physical difference in the tape construction, but the larger impact is considered to be the usage environment.

### **General advice**

The migration route was indicated as the preferred archive strategy. This was proposed as it offers the best navigation of improvements / enhancements / revisions to data format, tape format and replay technology to ensure data is available when required in a usable format.

If migration is being considered it was suggested that data be re-proven to latest technology every second or third format generation review. This was indicated as being a cost considerate strategy, whilst ensuring that data is stored in accessible state.

Other sources have anecdotally (and independently) indicated that as a basic benchmark, 5 to 10 years is considered to be a general usable lifespan for magnetic tape if kept in the correct environment. Magnetic tape contained in compact or video cassettes or the data cartridges described above is prone to damage from external contaminants and effects<sup>9</sup>. Smoke dust and airborne debris can prejudice both the reading and writing of magnetic tape. Airborne pollutants from vehicle exhausts and cleaning materials can have chemical effects. Finally, magnetic fields from sources such as motors and magnetic latches can also degrade the stored data.

---

<sup>7</sup> <http://www.ip.philips.com/services/?module=IpsLicenseProgram&command=View&id=21&part=2> - last accessed Aug 2007.

<sup>8</sup> [www.imation.com](http://www.imation.com) – last accessed Aug 2007.

<sup>9</sup> BS ISO 18933:2006 Imaging materials, Magnetic tape, Care and handling practices for extended usage.

### E.1.3 Hard disk drives

Magnetic hard disk drives (HDDs) are an attractive technology due to maturity, mass market availability with continued cost per gigabyte reductions and capacity growth. They are also surprisingly robust. As an example, almost no data was lost when a library at Stanford University was flooded, submerging the disk drives.<sup>10</sup>

The major hard disk manufacturers design their drives to have 100 percent data recovery after five years and possibly ten. Two manufacturers were contacted – Seagate and Western Digital, but as with the tape manufacturers were unable to provide much more in terms of specific usage beyond general warranty information. Their verbal advice was to treat an HDD like all magnetic data storage types and reprove (re-write to re-assert the magnetic charge) the data every 5 to 7 years.

Questions on the subject of differences between a stored ‘spinning’ hard disk (powered but not accessed frequently if ever) and a stored un-powered hard disk were not addressable by the manufacturers due to a lack of investigational data. It seems one of the difficulties with the line of questioning is that as the technology develops it becomes more difficult to predict an accurate longevity span for the anticipated conditions. It should be recognized that magnetic hard drives used for long term storage should therefore not be left inactive for several years as no experience exists regarding idle-storage.

Other data sources offered interesting strategies to HDD based data storage. For example, a conference paper describes a tool for use by librarians to assist in the management of HDD based archival storage.<sup>10</sup> Many of the strategic points have been covered in the previous discussion (e.g. museum versus migration) however some technological suggestions based around linked HDDs are offered.

The broad measurement of the technical quality of an HDD is determined at manufacture as the device’s ‘mean time before failure’ (MTBF<sup>11 12</sup>). This allows some probabilistic analysis of a data storage system – it should be noted however that this is limited to an active (i.e. powered) HDD array rather than an individual stored HDD. There are also some known flaws in the mathematical assumptions made in this predictive process.

Another measurement metric is power up cycles or spin up cycles (also called CSS, or "on/off cycles") which is sometimes offered by HDD manufacturers. Again as this is a relatively new measure the correlation to real world storage examples is difficult to ascertain. However it may be a useful means to estimate the remaining life expectancy of a drive. The significant problem with this measure is that information is required about the state and usage history of a (seized) drive that could be impossible to ascertain.

---

<sup>10</sup>D S H Rosenthal, M Roussopoulos, T J Giuli, P Maniatis, M Baker, “Using Hard Disks for Digital Preservation”, Proc. IS&T’s Archiving conference, pp 249 – 253 (2004).

<sup>11</sup> <http://en.wikipedia.org/wiki/MTBF> - last accessed Aug 2007.

<sup>12</sup> <http://web.archive.org/web/20001202154100/http://www.storage.ibm.com/storage/oem/tech/mtbf.htm> last accessed Aug 2007

One way to mitigate the effect of hard drive failure is to configure a number of drives as a RAID (Redundant Array of Independent Disks). Although the RAID system was not designed specifically for data archiving it does enhance reliability and is therefore commonly implemented in systems requiring high availability. This is because if one of the drives in the array fails all the data on that disk can be reconstructed with data from other disks in the RAID.

The level of failure the system will tolerate, and the speed of recovery from such failures is a product of the RAID levels. RAID level 1 is effectively two drives mirrored which is two copies of the data on different physical drives. As a result, if one disk fails the data is available on the other drive. Higher level RAID arrays use increasingly complex systems to ensure data integrity with more efficient use of storage space.

MAID (Massive Array of Idle Disks) is a lower power version of RAID and uses several hard disk drives mounted in racks. The hard disk drives are normally not spinning when not in active use but can be on-line in a few seconds. These hard disk drives can be configured just like a RAID system with the data recorded on more than one hard disk drive. MAID is comparable to RAID in cost for the same total capacity but the hard disk drives will last longer because they are normally idle. Since they are normally idle, they use much less power than a RAID system.

The downside to both RAID and MAID technologies (in addition to the obvious increase in cost per gigabyte) is that in their most common implementation the disks are all located in close proximity. As a result they do not provide protection against real threats such as attack, human error or disaster.<sup>10</sup>

## **E.2 Storage, handling and testing**

### **E.2.1 Optical disks**

#### **Writing the disk**

This is the most sensitive part of the process. Anything that can degrade the writing beam from laser to recording layer can reduce performance and therefore the effective longevity. There are a number of practical steps that can be taken to maximise performance.

- 1 If the blank disks are kept in a cool environment to maximise lifetime, allow to warm up in the work area but within the sealed media case. An acclimatisation time of 24 hours is recommended.<sup>1</sup> It is important to avoid condensation on the disk.
- 2 Test the supply of blank disks. This important step is often omitted and is the subject of a separate section within this appendix.
- 3 Work in a clean dust free environment.
- 4 A visual inspection of the disk will help to detect any damage, abnormalities or contaminants on the surface of the disk. This inspection is extremely important before recording to a disk. It is performed best while holding the disk by the edge, tilting the disk while viewing the surface at various angles of light reflected from a defused light source. This method can highlight issues that may not be detected by an initial inspection.
- 5 Blow the blank media clean using pressurised clean air.
- 6 Avoid interruptions to the data flow between computer and disk writer. Common causes of this are a fragmented file structure on the computer (defragment the computer hard drive before writing) or automatic activities such as screen savers, mail replication etc (disable such activities before starting to write the optical disk).
- 7 Verify the written disk. This is a process whereby the recorded file is read back from the optical disk and checked against the original data.

For a higher level of data security it is advisable to create multiple copies. This can be done to various levels with a master copy stored under optimal conditions, a working copy in use and a safety copy stored at a different location to the master. These copies should be made on different batches of disks.

#### **Disk storage**

The recording layer in optical disks can be damaged by light, heat, moisture and a combination of these. Prolonged exposure to moisture allows water to become absorbed into the disk where it may react with the disk components causing failure.

---

<sup>1</sup> BS ISO 18921:2002 Imaging materials. Compact discs (CD-ROM). Method for estimating the life expectancy based on the effects of temperature and relative humidity. ISBN 0 580 40028 X.

Extended exposure to humidity above 65 % RH will promote fungal growth on the disks.

International standards make the following environmental recommendations for the storage of optical disks.<sup>2</sup>

1. Useful life will be increased by storing disks at low temperature and low relative humidity, since chemical degradation is reduced at these conditions. However, storage of disks below -10°C and below 10 % RH is not recommended so use of a freezer is not a good idea.
2. The average relative humidity of an extended-term storage environment shall be maintained between 20% RH and 50% RH. Note that this is a lower RH than many UK environments.
3. Cycling of relative humidity shall not be greater than  $\pm 10$  %. This implies some level of humidity control.
4. The maximum temperature for extended periods shall not exceed 25°C, and a temperature below 23°C is preferable. The peak temperature shall not exceed 32°C.

The US National Institute of Standards and Technology (NIST) recommend a temperature range of between 4°C and 20°C for extended storage.<sup>3</sup>

In addition, disks should be stored in a dark environment to reduce the risk from light fading.

Optical disks can also be affected by airborne pollutants such as ammonia, chlorine, sulphides, peroxides, ozone, oxides of nitrogen, smoke and acidic gases.<sup>2</sup> These cause chemical reactions that are harmful to optical disks. As a result ammonia and chlorine-based cleaners should not be used in optical disk storage areas. The polycarbonate substrates are sensitive to these reactive gases causing crazing on the disk. These pollutants also accelerate the degradation of the metal layer.

Magnetic fields are a concern only for magneto-optical disks. The maximum permissible fields specified for magneto-optic disks (48 000 A/m or 600 Oersteds at the recording layer) are higher than for magnetic tape<sup>4</sup> because the optical material must be heated in the presence of the magnetic field for changes to occur. External magnetic fields are most frequently observed near motors and transformers. A separation of a few metres from the source will usually provide sufficient protection. External fields of a more unanticipated nature may be produced by some headphones and microphones or by cabinet latches.<sup>2</sup>

Optical disks shall not be stored in the same storage vault as reflection prints due to possible interactions caused by off-gassing that attacks the disks.

There is no compelling evidence that disk storage orientation matters. Horizontal or vertical storage seems to make little difference.

Further information on storage environments can be found in the relevant ISO standard.<sup>2</sup>

---

<sup>2</sup> BS ISO 18925:2002 Imaging materials. Optical disk media. Storage practices. ISBN 0 580 39217 1.

<sup>3</sup> F R Byers, "Information Technology: Care and Handling of CDs and DVDs — A Guide for Librarians and Archivists", NIST Special Publication 500-252 (2003).

<sup>4</sup> BS ISO 18923:2000 Imaging materials. Polyester-base magnetic tape. Storage practices, ISBN 0 580 36266 3

### **Storage cases**

Optical disks should be kept in chemically inert storage containers such as the relevant jewel or Amaray cases. They are then correctly supported by the hub and the surfaces of the disk are kept from contact with the inside of the case. This minimises the possibility of damage from surface contact. It should be noted that CD and DVD jewel cases are of different design because of a different hub structure. The cases are commonly differentiated by a “Compact Disc” or “DVD” logo in one corner of the case. Stable materials such as polypropylene are recommended. Potentially harmful enclosures include cardboard, paper and highly plasticized materials and should not be used.

Sleeves made of polypropylene or polyester will not harm disks but give little mechanical protection. Take care to avoid surface abrasion when inserting or removing disks from such sleeves. Do not use smooth plastic sleeves in contact with disk surfaces for extended term storage. Any adhesion may delaminate the disk when it is removed.

For long-term disk storage any paper label or insert is removed from inside the case. Paper can retain moisture in the case and may release harmful pollutants.

Do not leave optical disks in the computer drive. Temperatures within a disk reader can exceed 40°C and repeated thermal cycling can warp the disk.

### **Disk cleaning**

1. Blow the disk clean using pressurised clean air. For heavier contamination rinse with distilled water or a water based lens cleaning solution. For severe contamination isopropyl alcohol may be used. Finally, wipe the disk with a lint free cloth. Avoid using paper cleaning products or abrasive cleaners.
2. Never wipe a disk around the circumference. Instead use radial strokes from the centre to the outside of the disk. This is because the disk is written in coaxial tracks parallel to the circumference and wiping in this direction risks damaging long sections of sequential data.

### **Disk handling**

Do not touch the recording area of an optical disk.

When taking a disk out of the jewel case use the following procedure.

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

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

1. Open the jewel case and put it down on a flat surface.
2. Place the disk on the jewel case labelling side up with the central hub over the retaining mechanism.

3. Push the central area of the disk onto the location mechanism. Do not touch data area of the disk.

Optical disks can develop an electrostatic charge, particularly at low humidity levels. The disks then attract dust particles which can interfere with the reading and writing processes. Operations should be conducted in a clean, dust free environment particularly if the humidity is low.

### Disk testing

The only way to know the condition of a collection of disks is to test them. By this we mean not just see if they are still readable. Modern day disk readers contain sophisticated error correction systems that will hide the effect of disk degeneration until it is too late. At that point any subsequent copies are highly likely to be irreversibly flawed, if the disk can be read at all.

There is one useful tip for data recovery. As disk readers vary in capability a disk that is unreadable in one unit may well be (just) readable in another. Try a number of disk readers. If you find one that works, copy the data on the disk quickly!

A key parameter of disk quality is the Block Error Rate (BLER) which can be considered to be a high level estimate of the performance of the system.<sup>1</sup> BLER is defined as the number of erroneous blocks of data read from the disk per second measured at a particular point in the system during playback under set conditions.<sup>5</sup> As an example of acceptable BLER figures, music CDs can have a rate of 220.<sup>6</sup> However, for data disks the acceptable level may be as low as 50.<sup>7</sup> It should be noted that the standard for testing CD ROM and CD R disks uses this higher level which may be unacceptable for data disks.<sup>1,8</sup>

Unfortunately BLER is not the whole story and disks with a BLER below 50 can still fail due to other mechanisms. However, it is probably the best single metric for recordable CD systems.

There is an ISO standard on optical media testing.<sup>9</sup> However, the systems needed are expensive. A more cost effective solution may be to use CD and DVD writing software that reports BLER. Nero CD-DVD Speed and Plextor Plextools are amongst those that are believed to report this metric.<sup>10</sup>

---

<sup>5</sup> BS EN 60908:1999 Audio recording. Compact disc digital audio system.

<sup>6</sup> ISO/IEC 10149:1995 Information technology -- Data interchange on read-only 120 mm optical data disks (CD-ROM)

<sup>7</sup> K Bradley, "Risks Associated with the Use of Recordable CDs and DVDs as Reliable Storage Media in Archival Collections - Strategies and Alternatives", UNESCO (2006).

<sup>8</sup> BS ISO 18927:2002 Imaging materials — Recordable compact disc systems — Method for estimating the life expectancy based on the effects of temperature and relative humidity.

<sup>9</sup> BS ISO 12142:2001 Electronic imaging. Media error monitoring and reporting techniques for verification of stored data on optical digital data disks. ISBN 0 580 38766 6

<sup>10</sup> M Mizzen, "The Role of Product Testing in Digital Fulfillment", IS&T's International Symposium on Technologies for Digital Fulfillment, 2007.

### **Disk labelling**

It is a common fallacy that only the recording (non-labelling) side of the disk is subject to damage. The label side of a CD-R disk commonly has only a thin lacquer layer on top of the metal coating that is crucial to reflect the reading laser. Some solvents used in marker pens such as xylene and toluene can penetrate and compromise this lacquer coating. As a result it is best to avoid solvent based marker pens. Water or alcohol based markers should be OK. Best practice is to only use a marker on the clear inner hub or the “mirror band” of the disk as this is not a recording area.

Adhesive labels should not be used. In addition to contributing to disk imbalance they have been shown to increase the rate of BLER accumulation on storage. Laser etch engraving however appears to be safe however.<sup>11</sup> While there is no scientific evidence that inkjet printing onto specially coated layers affects disk life, its safety is not proven so should be avoided.

### **E.2.2 Magnetic tape**

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

Magnetic tape intended for extended use should be handled at stable temperatures between 18°C and 25°C and stable relative humidities of between 15% and 50% RH.

Magnetic fields are a concern for magnetic tape use and storage. The maximum permissible steady state (DC) fields are 4 000 A/m (50 Oersteds) and a peak intensity varying (AC) field of 800 A/m (10 Oersteds). External magnetic fields are most frequently observed near motors and transformers. A separation of a few metres from the source will usually provide sufficient protection. External fields of a more unanticipated nature may be produced by some headphones and microphones or by cabinet latches and magnetised tools.

---

<sup>11</sup> M Youket, N Olson, “Compact Disc Service Life Studies by the Library of Congress”, Proc. IS&T’s Archiving conference, pp 99 – 104, (2007).



## E.3 International standards on image permanence

### E.3.1 Introduction

This document gives an overview of relevant international standards on the permanence of images stored on both electronic storage and photographic hard copy media. These standards were developed under the auspices of the photography technical committee of the International Standards Organisation. The intention is to give readers a guide to the standards that are publicly available as a valuable resource.

Because of the extended lifetime of many of the media covered here accelerated ageing methods are commonly employed. The Arrhenius method in particular is commonly employed for accelerated ageing and is itself the subject of an ISO standard for this application.<sup>1</sup>

### E.3.2 Traditional photographic media

There are a number of standards that cover the image permanence issues of traditional photographic media from a number of perspectives that should be of particular interest for evidence preservation.

ISO 18911 is a general document on the keeping of films. It provides recommendations concerning the “storage conditions, storage facilities, handling and inspection for all processed safety photographic films in roll, strip, aperture-card or sheet format, regardless of size.”<sup>2</sup>

ISO 18901 establishes the specifications for photographic films intended for the storage of records.<sup>3</sup> It applies to black-and-white films coated on acetate or polyester bases processed to produce a silver image by negative or reversal processing. It should be noted that silver containing microfilm has a separate specification.<sup>4</sup>

For print media ISO 18929 establishes the specifications for silver-containing monochrome prints intended for dark storage and also applies to prints that have been toned to improve the permanence of the silver image.<sup>5</sup>

Issues pertaining specifically to colour films and papers are dealt with under ISO 18909.<sup>6</sup> This standard contains test methods for long term dark storage stability so is particularly pertinent to stored images.

<sup>1</sup> BS ISO 18924:2000, “Imaging materials. Test methods for Arrhenius type predictions”, ISBN 0 580 36425 9

<sup>2</sup> ISO 18911:2000, “Imaging materials -- Processed safety photographic films -- Storage practices”.

<sup>3</sup> ISO 18901:2002, “Imaging materials -- Processed silver-gelatin type black-and-white films -- Specifications for stability”.

<sup>4</sup> ISO 18919:1999, “Imaging materials -- Thermally processed silver microfilm -- Specifications for stability”.

<sup>5</sup> ISO 18929:2003, “Imaging materials -- Wet-processed silver-gelatin type black-and-white photographic reflection prints -- Specifications for dark storage”.

<sup>6</sup> ISO 18909, “Photography — Processed photographic colour films and paper prints — Methods for measuring image stability”.

### **E.3.3 Enclosures**

In addition to the standards specifying stability requirements and storage conditions of the images themselves, there are a small number of standards that specify the enclosure materials used for storage. The first of these is ISO 18902.<sup>7</sup> This standard deals with the materials used in filing enclosures, containers, albums and frames as well as the construction of folders, sleeves, slide mounts etc.

The second covers multiple media archives.<sup>8</sup> This standard was necessary because in the real world users are frequently faced with the task of storing many types of material together. The content can consist of processed film and prints plus digital storage media such as magnetic tape and optical disks. As a result it may not be practical or realistic for the user to provide a number of different storage environments that are optimized for each material.

### **E.3.4 Media for electronic storage**

There are a number of international standards that cover this increasingly important area of image storage.

The first of these covers the storage of magnetic media used in video, audio and computer tape.<sup>9</sup> An additional document covers the care and handling of such storage media covering topics such as contamination routes, handling, environment, inspection, cleaning, maintenance, transportation and staff training.<sup>10</sup>

There are a number of interesting standards on optical media. ISO 18921 covers life expectancy test methods of CD-ROM media.<sup>11</sup> It suggests that a suitable acclimatisation time for a disk removed from cold storage is 24 hours. ISO 18927 covers the same ground for CD-R<sup>12</sup> and ISO 18926 same for magneto-optical disks.<sup>13</sup>

The life expectancy test methods above are interesting but probably more pertinent to the practitioner is ISO 18925 which covers the storage practices for optical media in general.<sup>14</sup> This document makes the following recommendations.

Useful life will be increased by storing disks at low temperature and low relative humidity, since chemical degradation is reduced at these conditions. However, storage of disks below -10°C and below 10 % RH is not recommended so use of a freezer is not a good idea.

---

<sup>7</sup> ISO 18902:2001, "Imaging materials -- Processed photographic films, plates and papers -- Filing enclosures and storage containers".

<sup>8</sup> ISO 18934:2006, "Imaging materials — Multiple media archives — Storage environment".

<sup>9</sup> ISO 18923:2000, "Imaging materials. Polyester-base magnetic tape. Storage practices".

<sup>10</sup> BS ISO 18933:2006 Imaging materials, Magnetic tape, Care and handling practices for extended usage.

<sup>11</sup> BS ISO 18921:2002 Imaging materials. Compact discs (CD-ROM). Method for estimating the life expectancy based on the effects of temperature and relative humidity. ISBN 0 580 40028 X.

<sup>12</sup> BS ISO 18927:2002 Imaging materials — Recordable compact disc systems — Method for estimating the life expectancy based on the effects of temperature and relative humidity.

<sup>13</sup> BS ISO 18926:2006 Imaging materials — Information stored on magneto-optical (MO) discs — Method for estimating the life expectancy based on the effects of temperature and relative humidity.

<sup>14</sup> BS ISO 18925:2002 Imaging materials. Optical disk media. Storage practices. ISBN 0 580 39217 1.

The average relative humidity of an extended-term storage environment shall be maintained between 20 % RH and 50 % RH. Note that this is a lower RH than many UK environments.

Cycling of relative humidity shall not be greater than  $\pm 10$  %. This implies some level of humidity control.

The maximum temperature for extended periods should not exceed 25°C, and a temperature below 23°C is preferable. The peak temperature shall not exceed 32°C.

Ammonia and chlorine-based cleaners should not be used in optical disk storage areas. These cause chemical reactions that are harmful to optical disks.

There is an ISO standard on optical media testing.<sup>15</sup> However, the systems needed are expensive.

---

<sup>15</sup> BS ISO 12142:2001 Electronic imaging. Media error monitoring and reporting techniques for verification of stored data on optical digital data disks. ISBN 0 580 38766 6

## Appendix F: Requirements templates

### F.1 Basic template

The following is a basic template for communicating imaging needs to the IT function (refer to section 5):

<b>Digital Imaging Archive/Storage Requirements Gathering</b>	
<b>Date</b>	
<b>Sponsor/ Senior stakeholder:</b>	
<b>Dept.</b>	
<b>Contact name</b>	<b>Tel. Number</b>
<b>1. Use of images</b> (i.e. video, stills images, combination. Give an overview of the problem and/or describe the business need.)	
<b>2. End to end process</b> (Describe start to end process, any common themes and exceptions)	
<b>3. Internal customers</b> (Where do your images come from and go to?)	
<b>4. Other agencies?</b> (Are there customers outside your force that you wish to communicate with?)	
<b>5. Equipment used</b> (What equipment do you use in all of the processes?)	

<b>6. Where are images currently stored?</b>
<b>7. How are they secured/protectively marked?</b>
<b>8. How are they archived/disposed of?</b>
<b>9. What information is kept with images?</b>
<b>10. Volumes</b> (How much material do you deal with on a monthly basis?)
<b>11. Search/retrieval</b> (How do you locate, access and retrieve the material you keep?)
<b>12. SOPs</b> (Do you have any existing procedures that need to be maintained?)
<b>13. What are the current bottlenecks/problems?</b>
<b>14. Ideas for improvement</b>

## **F.2 Advanced template**

ACPO (2007) Practice Advice on Police Use of Digital Images, combined with this HOSDB technical document encourage, a close relationship between image owners, users and ICT departments.

A robust relationship between those disciplines will serve to efficiently address the constantly emerging technical challenges of the fast moving digital imaging environment, so that the technology can be thoroughly researched, meaningfully deployed and fully exploited.

Whilst the front end image capture systems have in many cases been used for some time and are now well embedded, the further data handling issues, specifically in relation to storage and archiving in networked systems or centrally managed repositories, have been developed to a lesser degree.

A number of forces will therefore be addressing the need for network, storage and archiving capacity at a time when a large number of legacy images already exist, a large number of image users are apparent and/or new technology emerges ready for introduction.

It is recommended that at an early stage imaging owners, technology users and ICT departments commence the dialogue about their individual requirements in order that the any future efforts are suitably captured and defined.

A basic requirements template can assist with this initial task that will be carried out by an image user and a member of ICT. This, however, needs to be expanded into a more mature exercise and the Digital Imaging Archive/Storage Requirements Gathering Questionnaire template can be used. It is envisaged that the process of completion will include major stakeholders, ICT, MOPI and other legal and procedural functions. This process should be managed and supported by a force Digital Champion.

This template does not offer an exhaustive list and should be supplemented by force specific considerations, but may lead to a requirements catalogue that far exceeds the suggestions made here.

**Digital Imaging Archive/Storage Requirements Gathering**

**Questionnaire template**

**Date:**

**Force Imaging champion/Senior stakeholder:**

**Department:**

**Tel. number:**

1. Use of images- are they video, stills, a mixture? Give a problem description and/or define the business need.

*Image capture and volume*

2. How are the images captured? i.e. camera type, scans, conventional methods, CCTV etc.
3. What equipment is used at capture stage/point of transfer?
4. How many capture devices are there? (refer to generic calculation of storage volumes Appendix B)
5. Is the image material generated by a third party?
6. Who are the users contributing to the system?
7. Where are the users located?
8. How often are images acquired in a given time period? (refer to generic calculation of storage volumes Appendix B)
9. What media is used? (refer to generic calculation of storage volumes Appendix B)
10. What file types are produced? (refer to generic calculation of storage volumes Appendix B)
11. How much of the initial material captured needs to be maintained? (refer to generic calculation of storage volumes Appendix B)
12. Does the original image capture quality need to be maintained throughout?

*Transfer*

13. Have you got internal/external customers, who need to transfer images to you? IT departments need to assess this for the network capability, connectivity and security.
14. What restrictions/constraints exist that may prohibit the transfer of images?
15. Do you need to transfer images from the repository/network to internal/external customers? IT departments need to assess this for the network capability, connectivity and security.

16. How is the material protectively marked (GPMS)? Consult with the Force Security Officer.
17. How will the image material be secured during electronic transfer? IT departments need to consider privacy, integrity and availability.
18. The system needs to offer legal and statutory compliance within the CJX. (i.e. RIPA, MOPI, Data protection, CPIA, FOIA) and other government directives.

*Users*

19. Who needs to access the material from an administrative, user or any other workflow point of view? Consider access rights and restrictions.
20. Once a decision has been made to upload and centrally hold image material, who needs to upload, index and search the material and from what location(s)?
21. Who governs and administers the material not selected for loading?
22. How many users will the system need to support at any time? IT needs to consider the network size and licences needed for daily workflow.
23. What part of the workflow functionality can be automated, i.e. updates, notifications, work requests?
24. What security restrictions need to apply to different users in terms of access rights and restrictions?
25. Does the image repository need to link with other applications/ networks for data mining or information sharing purposes?
26. Are there existing local standard operating procedures internally or with other parties in the CJX?

*Assessment store*

27. What information is kept with images (metadata and supporting information, i.e. admin data)?
28. Do you have legacy images you wish to convert? Define the volume.

*Evidential store*

29. How are images currently archived?
30. Will you seek to carry out any back record conversion?
31. Do separate archiving categories apply? Consider whether highly sensitive material needs to be kept separate from the main database.
32. What proportion of images has to be accessible at all times? Are there different timescales applicable for the availability?

*Other considerations*

33. What management data does the system need to deliver?
34. What report forms and other documents does the system need to be able to produce?



35. Does the system need to accommodate customisation, i.e. logos, headers?
36. Who will be the designated owner of the system?
37. What are the current bottlenecks/problems in the handling of the images?  
Suggestions for improvements.

*Consider what other departments and stakeholders need to assess the information given or can contribute to it. These might include:*

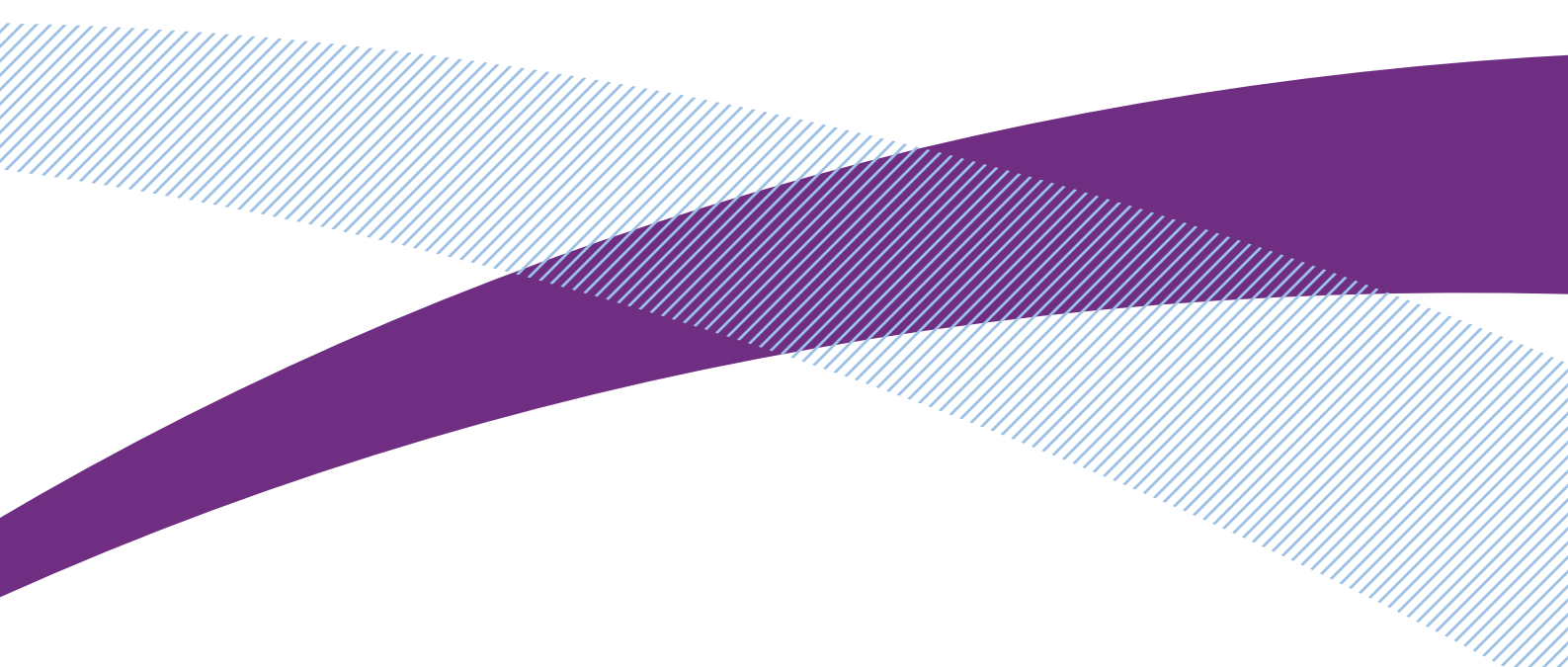
- *Force Security Manager*
- *MOPI Manager*
- *Data Protection*
- *SSM*





This is an official document.

If found please return to the nearest police station and inform them how and when it was found. Its unauthorised possession, use, retention, alteration, destruction or transfer to another person may be an offence under the Official Secrets Act.



Home Office Scientific Development Branch  
Sandridge  
St Albans  
AL4 9HQ  
United Kingdom

Telephone: +44 (0)1727 865051  
Fax: +44 (0)1727 816233  
E-mail: [hosdb@homeoffice.gsi.gov.uk](mailto:hosdb@homeoffice.gsi.gov.uk)  
Website: <http://science.homeoffice.gov.uk/hosdb/>