Digital imaging guidelines (Taking, downloading and securing images)

Introduction

It is critical in law enforcement that a digital image (photograph) can be verified in court as an authenticated copy of the original digital image.

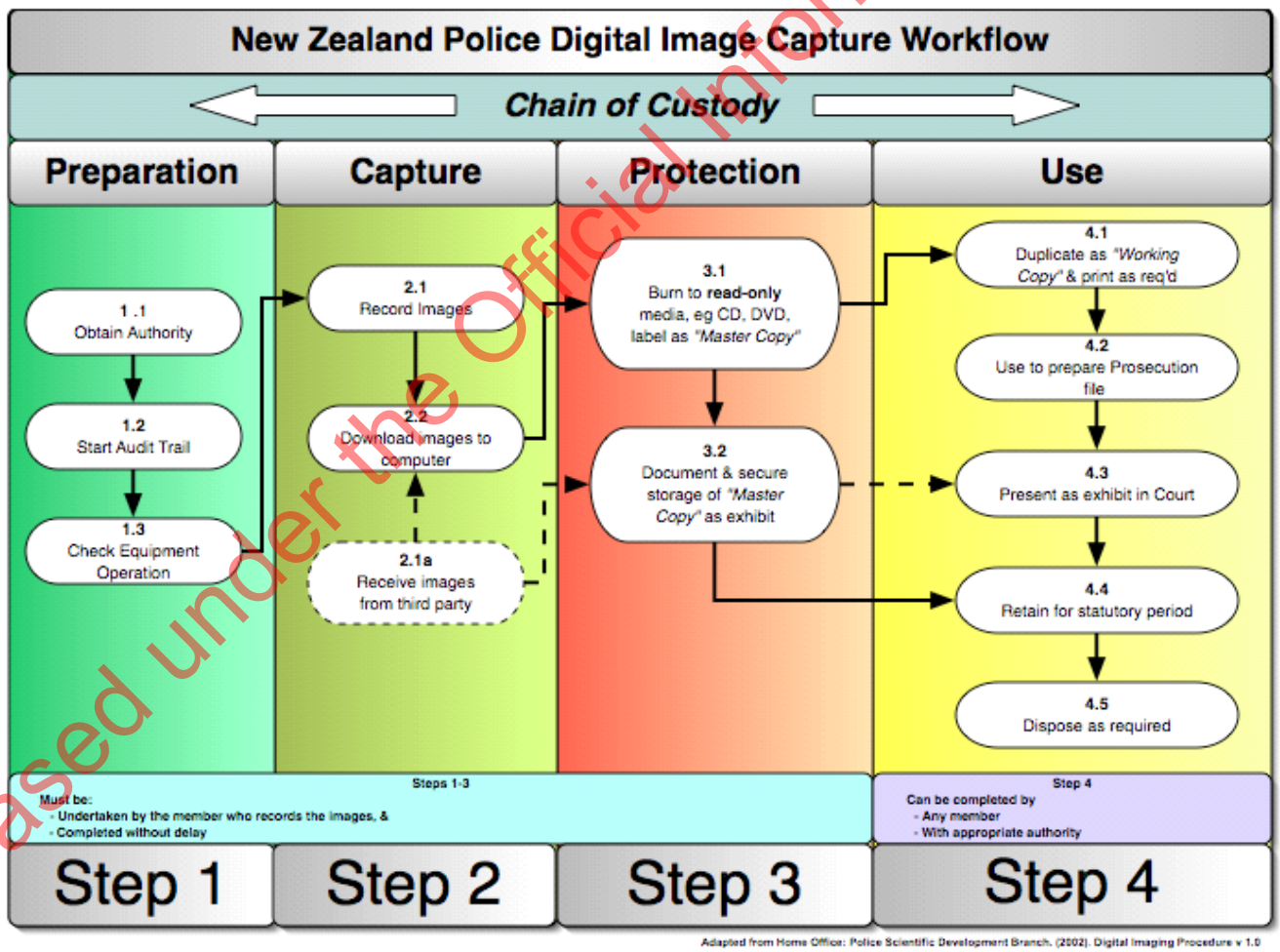
Frontline employees must follow the guidance in this section and in Taking and storing images for evidential purposes using iPhones / mobility devices which:

- simply outline the digital imaging process to:
  - ensure any images they take will be accepted by courts as reliable evidence
  - minimise the risk of legal challenges around whether the image could have been compromised
- supplement more detailed guidelines (the Australasian Digital Imaging Guidelines) used by Police forensic photographers.

Refer also to your local standard operating procedures.

Diagram of digital imaging process

This diagram provides an overview of the Police digital imaging process.



Preparing to take digital images

Follow these steps.

Step	Action

Released under the Official Information Act 1982

1	Consider first if it is necessary for the photographs to be taken. Remember that the images will be subject to disclosure.
2	If you are not trained in photography, consider whether you should use a forensic imaging specialist. See When should a forensic photographer be deployed. **Note**: Although mobility devices have onboard cameras, the images are not considered suitable for technical forensic photography. Mobility devices have some limited suitability for general photography such as stolen property and wilful damage.
3	If you decide to capture the images yourself, ensure: • you've read and understood these Police digital imaging guidelines, and • you are trained in or know how to use all the equipment used in the digital imaging process. If using an iPhone or mobility device see also Taking and storing images for evidential purposes using iPhones / mobility devices.
4	Before starting photography, check the camera and other equipment to ensure: • the camera is functioning properly and according to the manufacturer's guidelines • time and date information is set correctly. This will appear in the meta-data as an attachment to the image file.
5	Start an audit trail by recording in your notebook details of the digital images. You **must** include date, time and location. You **can** also include file number range, camera make, model and serial number.
6	Capture images on camera as required.

Downloading captured images to computer

After capturing your images on camera, download **all** images relating to your case to a **Police computer** using an external card-reader or camera software.

Do **not**:
- change file formats or alter the images in any way
- delete any images from your camera unless you have authority to do so.

Deleting images

Local standard operating procedures contain details of:
- who can authorise the deletion of images
- circumstances in which images can be deleted (usually only for technical reasons).

Be aware that deletion of images will cause a discontinuation of image numbering and may raise issues in court.

Images captured on mobility devices

- All images must be emailed to a Police email address using the full resolution (Actual Size) option. Depending on composition, several images can be sent at one time.
- Images should be immediately placed in a 'Read Only' folder to ensure ongoing integrity of the original images. Copies can then be forwarded.
- Once downloaded, images **must** be deleted from the mobility device.
- Video files, once emailed, are blocked until released following email confirmation of suitability.

For more information see Security of cameras and memory cards below for information about recovering deleted images.

Released under the Official Information Act 1982

Downloading images received from a third party

Digital cameras

- Secure the memory card as an exhibit. For minor offences, the cards can be returned after downloading.
- Take care if downloading a memory card onto a Police computer as the Endpoint Encryption software, if activated, will delete all images on the card. It is therefore advisable to forward the memory card to a Police Forensic Imaging Section for safe downloading.

USB flashdrives

- Secure the flashdrive as an exhibit. For minor offences, the flashdrive can be returned after downloading.
- DO NOT attempt to download onto a Police computer - the Endpoint Encryption software will delete all data on the flashdrive. Forward the flashdrive to a Police Forensic Imaging Section for safe downloading.
- With regard to video files, ensure **all** files are downloaded as the necessary playback software may be contained in a different file from the video file.

Mobile phones

- Both images and text data can be downloaded in a number of ways, i.e: email, text message, bluetooth and memory card. Seek assistance from a Police Forensic Imaging Section.
- In some cases photography of the phone screen may be the only option for image and data retrieval and this should be carried out by the Forensic Imaging Section.
- If the mobile phone is secured as an exhibit, ensure any passwords are also recorded. Consider securing the phone charger as well.

CD/DVD media

- Ensure these are correctly labelled and packaged.

Recovered stolen cameras, USB drives and mobile phones

- These devices will often contain images or data leading to an offender or complainant, even if the memory card has been deleted or formatted.
- Police Forensic Imaging Sections can assist with the recovery of deleted images and data. For serious offences contact the High Tech Crime Group.

Securing digital images after downloading to a computer

Follow these steps to document and secure images after they have been downloaded to a computer.

Step	Action
1	Save or burn the images in their original format to a secure server and folder or 'read-only' media, i.e. CD-R or DVD. **Warning**: Do not use re-writable media or multi-session recording functions. (Consider copying the original file into the station server (in the case file, if one exists) before burning it onto the 'read only' media).
2	Verify the media (CD-R or DVD) using the media verification function. This ensures a "like-for-like" copy has been made.
3	Label the CD-R or DVD as 'Master Copy' and include on the label the Police file number or any other identifier that relates to the images.
4	Record the details of the master copy on the POL268 or local image database. **Note**: If recorded on a local image database, the job reference number must be recorded on the master copy's label.
5	Print a copy of the images and attach the prints to the CD-R or DVD to the Police file.
6	Delete images or re-format memory card as required. (Refer also to Security of cameras and memory cards).

Released under the Official Information Act 1982

7	Store the master copy CD or DVD as an exhibit in the Exhibit Store with the POL268 or according to your local standard operating procedures.

Retention of the master copy
Keep master copies of images for the statutory period in accordance with the Retention and disposal of Police records chapter.

Before disposing of the master copy attach the CD-R or DVD and a printed copy to the Police file for filing. Then dispose of master copy in accordance with the Retention and disposal of Police records chapter.

Using the images

Make a working copy of the digital images by copying from the computer file. Attach an appropriately labelled CD-R or DVD along with a printed copy to the Police file.

Use the working copy to produce prints as required and to prepare the prosecution file and court booklets. Adjust, crop or enhance images as required. Refer to Photographic evidence in court for further information about preparing photographic evidence for court.

Presenting images as exhibits
Present the images to court as a print from your working copy, unless the court has requested the master copy. The person taking the images must validate the images for the court.

Disclosure
Digital images are subject to disclosure.

Security of cameras and memory cards

It is relatively straightforward to delete images on a memory card. However, this action merely gives instructions to the camera to write over deleted files.

Re-formatting a card is usually a complicated process involving going through a number of sub-menus to the 'Format Card' function. Again, this does not in fact delete anything. It merely tells the camera to write a new file structure and route path on the card and tells the camera that it can write over deleted images.

In both scenarios, deleted images can **very easily be recovered** from cards where either deleting or re-formatting has been undertaken using freely available card recovery software. **The security of the camera and memory card is therefore paramount.**

Procedures for keeping cameras and memory cards secure
Follow these steps to ensure cameras/ imaging equipment and the associated non-removable or removable storage media are kept secure.

Step	Action
1	Assign the cameras and imaging equipment to a named position or employee. The supervisor of that named position or employee must be aware of and maintain a record of whose custody the camera/imaging equipment is in.
2	Keep the equipment locked in a secure location when not in use (room, safe, office, cabinet, or vehicle).
3	Ensure camera and equipment security is subject to regular: • internal control checks by the Area or District HQ group concerned, to coincide with other internal control checks • spot checks by an identified manager of the Area or District HQ group concerned to ensure all images are erased.

Released under the Official Information Act 1982

4	The person assigned the camera/imaging equipment must: • ensure that they retain control of the camera at all times when in use • report any loss to their supervisor as soon as possible to commence inquiries. Depending on the circumstances of the loss, the matter may need to be reported to the PNHQ duty officer in terms of the No surprises policy. (If lost equipment with accessible images falls into the wrong hands, serious breaches of privacy may result causing significant embarrassment to Police).
5	Where a digital camera or memory card is no longer functioning or required the camera or card must be disposed of in accordance with ICT policy. (Contact ICT for advice). This applies to all recording media.

Australasian Digital Imaging Guidelines
Download a copy of the Australasian Digital Imaging Guidelines.

CCTV evidence
See Crown Law's Guidelines for Using Digital CCTV Evidence in Law Enforcement.

Released under the Official Information Act 1982