STANDARD OPERATING PROCEDURE

Digital Evidence Management

February 2018

INDEX

Government of South Australia
SafeWork SA

DOCUMENT CONTROL SHEET

REVIEW

This SOP must be reviewed every 36 months from the date of issue. However, this document must be immediately modified if legislation, practices and/or procedures change.

Document Details

Responsible Officer	Executive Director, SafeWork SA
Approval	9 February 2018
Version	4
Issued (date)	February 2018
Next Review	February 2021
RecFind Number	SAFE18/0095 PT1

Change History

Previous		**Change from previous version**	**Author**
Version	Issue Date		
1	Sept 2005		CALI
2	Sept 2008		CALI
3	March 2013		Operational Support Team
4	Jan 2018	Current process	Corporate Services

Contact Person

Name	[redacted]
Position	Principal Skills Support Officer – Resources, Corporate Services
Telephone	[redacted]
Email Address	[redacted]

Endorsed

[redacted]
Executive Director
SafeWork SA

9 / 2 / 2018

PURPOSE

This Standard Operating Procedure (SOP) outlines the procedures and risk mitigation processes for using **digital evidence** in a regulatory environment.

Digital evidence is any type of electronic evidence captured, stored or accessible via computer based equipment that supports or refutes a theory of how an offence occurred or that addresses critical elements of an offence, for example voice, photographic and video recordings of a workplace accident or an individual. **Digital evidence** is usually presented in hard copy, on a screen and/or via audio playing equipment.

The meaning of other terms and acronyms can be found in the Glossary of Terms (Appendix 3) and are highlighted in **bold** throughout this document

BACKGROUND

Digital evidence is used by SafeWork SA (SWSA) to present information about an **inspector**'s observations and conversations during their day-to-day work and investigative activities. This also includes **digital evidence** obtained by an **inspector** from sources other than themselves.

The *Evidence Act 1929* requires original **digital evidence** to be managed appropriately for its admissibility in a Court of Law. The **digital evidence**'s **integrity** and **authenticity** must be known, recorded and maintained.

The *State Records Act 1997* classes all original **digital evidence** captured in the course of official (SafeWork SA) business as an official record so evidence must be managed accordingly.

Policy

SafeWork SA will maintain the **integrity** and **authenticity** of captured **digital evidence** by ensuring:

- **inspector**s are lawfully **authorised** to collect such evidence;
- the **equipmen**t supplied to capture the evidence is fit-for purpose, and appropriately prepared, used and maintained;
- **inspector**s are **trained** and assessed in the use of **digital evidence equipment** and of the procedures for collection, management and use of **digital evidence**; and
- appropriate **resources and processes** are put in place for the management of **digital evidence** – including in particular the keeping of records as part of the audit trail for **digital evidence**.

Authority to collect Digital Evidence

The authority to collect and use **digital evidence** only given when:

- the legislation in that is being enforced or administered gives authority to a person appointed under that legislation to take **digital evidence**; and
- a person is formally appointed as an **inspector** or authorised officer under that legislation.

The following legislation administered/enforced by SWSA gives '**inspector**s' the power to take **digital evidence**:

- *Work Health & Safety Act 2012 (SA)* (WHS Act)
- *Dangerous Substances Act 1979* (DS Act)
- *Mines & Works Inspection Act 1920*
- *Petroleum Products Regulations Act 1995*
- *Shop Trading Hours Act 1977*

For example, section 165(1)(d) of the WHS Act states that '**inspector**s' may:

take measurements, conduct tests and make sketches or recordings (including: photographs, films, audio, video, digital or other recordings).

The following Acts administered and enforced by SafeWork do not give **inspector**s the authority to take **digital evidence** and therefore such evidence cannot be taken part of the administration or enforcement process:

- *Employment Agents Registration Act 1993*
- *Explosives Act 1936*
- *Fair Work Act 1994*
- *Long Service Leave Act 1987*

Inspectors must ensure they are acting within the defined authorities of the particular legislation to which their investigation pertains. For example, an **inspector** must not exercise their power to enter a workplace under the WHS Act and then use any **digital evidence** gathered to support a breach of the DS Act.

Digital Evidence Equipment

Inspectors are provided with a **digital camera** as part of the standard kit of equipment they receive when they start with SWSA. While the smart phones issued to **inspector**s have cameras they are not to be used for the collection of evidence.

Inspectors in the Investigation Team are also issued with digital video cameras and voice recorders for use in **comprehensive investigation**s.

Correct maintenance of **digital evidence** capture and storage equipment is essential. All equipment utilised in the **digital evidence** management chain should be maintained in accordance with the manufacturers' specifications and recommendations.

Only authorised technicians should perform repairs and modifications to **digital evidence** capture equipment.

SWSA employees requiring **digital evidence equipment** maintenance, repair or replacement must organise this through the Senior Administrative Officer, Corporate Services.

Training

All persons involved in **digital evidence** capture and handling will be trained in:

- the practical use of their digital camera; and
- this Standard Operating Procedure.

Trainees will be formally assessed in the management of **digital evidence** (with the assessments being documented).

Corporate Services is responsible for coordinating the digital camera and evidence training and its record keeping.

Training of the use of digital video and audio recorders for staff in the Investigation Team is provided within that Team.

PROCEDURE

Audit Trail

The most important factor in the use of digital imagery for evidentiary purposes is to be able to verify the continuity of the original image from the point of capture through to the disposal or archiving of the image. An audit trail is essential to achieve this outcome

The audit trail can be hand written, electronic or a combination. The audit trail assists in authenticating the origin and **integrity** of the evidence.

The audit trail records must include the following information:

- date and time of action;
- details of the case;
- details of the location where the original evidence was obtained;
- description of the original evidence;
- description of the equipment and medium used to capture the original evidence;
- description of the media used to record the original evidence (**disc** or memory stick);
- details regarding the downloading of the original evidence from the recording medium to the storage medium;
- details regarding actions to ensure the **integrity** of the original evidence (i.e. making a 'Master Copy' on a DVD, putting this in an evidence bag and storage arrangements);
- the image numbers;
- details defining the original copy and working copies;
- details regarding any person who has accessed the original evidence in a manner that could affect the **integrity** of that evidence; and
- any alterations made to a working copy.

Please note that some information will be recorded at the time of original evidence capture (e.g. field note book); and other information will be recorded during other evidence management processes. For example:

- Should an image be deleted from the original master copy either intentionally or accidentally it must be recorded in the audit trail.
- If the image is deleted after authority is given a notation should be included in the audit trail specifying what authority was given and why it was given.

The level of audit trail documentation required should be commensurate with the complexity of the processes applied to the evidence. SWSA's Investigations Team can provide further detail on the appropriate level of audit trail recordkeeping for complex **digital evidence** management processes.

The audit trail will be monitored by the relevant Team Managers and Team Leaders.

Digital Evidence Capture

Pre-use equipment checks

Staff involved in the capture of **digital evidence** must be familiar with the features and operation of the equipment they are using.

Prior to using any equipment for **digital evidence** capture, the equipment user will take the following minimum actions:

- review the equipment's operating instructions;
- check the equipment kit has all the components;

- sufficient number of charged batteries are available;
- the operator adjustable settings are set appropriately;
- the equipment's time and date settings are correct;
- there are adequate supplies of, or storage space available on, the recording media;
- any media protection settings will not prevent the recording being made; and
- the equipment is fully operational.

File Format – Photographs

The file format to be used for capturing evidentiary images shall be JPEG FINE at the highest resolution the camera is capable of.

Any system of image capture used must be capable of producing an original image or, in the case of video, a sequence of images which form an accurate representation of the objects or events being recorded. This original image or sequence of images must be preserved for possible evidential use. The process for preserving the evidence is detailed in section Managing Digital Evidence of this procedure.

File Format – Audio and video recordings

Equipment used for capturing digital audio and/or video recordings must allow replaying on a Microsoft Windows based program such as *Windows Media Player*.

Storage Medium

SWSA **Inspector**s generally utilise rewriteable storage media such as the capture device's internal memory, memory stick, compact flash or SD-CARD when capturing original **digital evidence**. The **inspector** is then responsible for making a binary non-editable (Master) copy of the evidence to non-reusable **disc** such as CD-R and DVD-R when required for retention as an exhibit. (See Master Copy and appendix 1 and 2 of this SOP).

Third Party Capture

Digital evidence captured by a third party (i.e. SAPOL, CFS, or a witness) can only be used as evidence when the original evidence collection can be authenticated. A witness statement verifying the **authenticity** of the captured evidence is required from the person who originally captured the evidence.

If **digital evidence** is captured by an Industry Team **Inspector**, not an Investigating **Inspector** as part of a comprehensives investigation, the statement of the Industry Team **Inspector** will need to verify not only the image capture but any additional actions relevant to the audit trail.

Managing Digital Evidence

Original Evidence

Original evidence is an official government record and needs to be retained pursuant to the *State Records Act 1997.* Part 6A of the *Evidence Act 1929* places its own set of requirements on original evidence. Compliance with this procedure ensures original evidence is managed in a way to meet the requirements of these Acts.

Original evidence shall be managed according to its known and/or possible end use.

For matters that are unlikely to proceed to a **comprehensive investigation** such as complaints, audits and licensing see Appendix 1

For matters more likely to proceed to a **comprehensive investigation** such as **critical events** see Appendix 2.

Original evidence must never be altered before a master copy CD/DVD has been created.

Master Copy

A Master Copy is a **disc** with a binary (replica) copy of the original evidence as captured. The master copy is the evidence that will be produced to a Court of Law if the **integrity** of presented **digital evidence** is questioned.

SWSA uses specially labelled DVD-R discs for master copy disc creation, long term **digital evidence** storage. These DVD-R are held by the Keswick based Investigations Team.

SWSA employees who capture original evidence are responsible for creating a master copy disc when required as per Appendices 1 and 2 of this procedure.

The master copy:

- should never be used, except to make subsequent working copies if the original working copies did not work; and
- only in the case of any doubt being cast upon the **integrity** of the presented images will the master copy be subjected to analysis; and
- be stored in an Evidence Storage Facility protected from electro-magnetic fields; and
- the master copy shall be stored with any necessary specialty software required to enable images to be viewed or heard in the future (e.g. some computer aided drawings provided by experts require special software).

Working Copies

When required (see Appendices 1 and 2), working copy discs of **digital evidence** can be made onto separate discs following creation of the master copy disc.

- Note: Where the working copy is an exact copy of the original evidence and is accompanied by an audit trail, it too may be produced in evidence as the original evidence, should a master copy disc be damaged or is unable to be read.

Alterations and enhancements can be made to evidence on working copy discs. See section Enhancing Digital Evidence for further information on this matter.

- Three (3) working copy discs are always required for any matter where a brief of evidence is being produced (one for the file, one for Crown Solicitors Office and one for defence lawyers).
- Additionally one (1) working copy disc is always required for any file forwarded to the Coroner.

Each working copy disc must be made from the original evidence's capture storage medium or the master CD/DVD, and NOT from another working copy.

Deleting Evidence

A crucial factor in using **digital evidence** for Court purposes is to be able to prove that no original evidence has been deleted without authority. Any deletion of evidence, either intentionally or accidentally, may be the subject of challenge and legal debate during Court proceedings, and must therefore be recorded in the audit trail. If an original evidence file is deleted in error, the deleted file will be obvious as the recording equipment generates a unique number for each evidence file.

Should a file be deleted from the original storage medium or during preparation of a master copy, the reason and circumstances surrounding the deletion must be documented in the audit trail. It does not matter if the deletion was intentional or accidental.

If a recording or photograph is taken that is either not relevant to the matter in hand, or is one of several images of the same thing, it should not be deleted as its deletion will be evident on the master copy disc. The irrelevant evidence does not need to be presented in any investigation file, brief of evidence or fatality file.

Deleted **digital evidence** can sometimes be recovered. This should not be relied upon to recover any accidentally deleted images. If an image is accidentally deleted do not use the medium to capture any further images, as the further images may overwrite the deleted image.

Should restoration of deleted evidence be required, contact the Investigation Team to arrange an expert witness to recover the deleted evidence.

Presenting the Evidence

Printed Images and Photographic Logs

Photographic prints that are required for evidentiary purposes can be made from a working copy disc.

Images used in the body of a brief of evidence or fatality file can only be used to assist the author of a brief to better explain a situation. The images must not be used in an attempt to persuade a point of view. The image is simply there to assist the author of the brief/fatality file describe what was viewed at a particular point in time.

All evidentiary images used in a brief of evidence shall be printed on paper, on one side. These images may include detail such as pointers, arrows and highlights. The printed image must reference the primary evidence digital image number.

A full and complete Photographic Log must be included with all **comprehensive investigation** files, briefs of evidence, and fatality files. Photo Log template is available through:

- Excel>>New>>My Templates>>Inspector Tools>>Photo Log

Audio Files

Audio files are recorded by an **inspector** to assist them recall what they heard or were told at a particular point in time.

Audio recordings of conversations shall be transcribed and presented in a written form depending on the purpose of the conversation, and be included in the investigation file, brief of evidence or fatality file as applicable.

Audio files that have been used as the basis for a statement will in most cases need no further transcription, as the statement will speak for the recording.

A dot point synopsis of any **general voice recording** shall be documented and placed in the case file. The Investigation Team may require **general voice recording**s to be transcribed verbatim, in which can be organised by their Senior Administration Officer.

Any audio files recorded for the purpose of a record of interview or a formal record of a conversation will be transcribed verbatim.

Audio evidence files will be managed in the same way a digital image is managed, with the exception they cannot be printed. Refer to sections Original Evidence and Master Copy of this SOP.

Video Files

Video evidence files will be managed in the same way an image is managed, with the exception that they cannot be printed. Refer to sections Original Evidence and Master Copy of this SOP.

Enhancing Digital Evidence

The actions an **inspector** takes to have any **digital evidence** enhanced and presented to a Court of Law must be documented and form part of the audit trail.

All **digital evidence** used in legal proceedings must include a description of any enhancements, restoration or compression made to that evidence. For example:

- A photograph of a room is taken but the image is too dark to make out what needs to be seen. The image can be lightened and this would be noted in the caption of the report or brief.
- Enlargements can also be useful to make serial numbers or wear marks easier to see.

Only enhance working copy images - not the Master Copy.

Do not use the terminology “manipulation” in your records as that infers that the **integrity** of the evidence may have been compromised.

Any process that involves the technical restoration or analysis of **digital evidence** must be undertaken by a person capable of appearing as an expert witness if that evidence is to be presented during any legal proceedings. Contact Investigation Team to source an Expert Witness should restoration or analysis of original **digital evidence** be required

The actions an **inspector** takes to have any **digital evidence** enhanced and presented to a Court must be documented and form part of the audit trail.

Summary

Whatever the digital media used, the following outcomes will be evident in a brief of evidence or fatality file:

- working copy disc(s) labelled and included;
- a full and complete photographic log;
- transcripts of any audio recordings in the requisite format;
- an audit trail demonstrating that the chain of evidence has been maintained and evidencing any enhancements made to working copy discs or presented evidence; and
- a bagged and labelled master copy disc lodged as an exhibit (in readiness for Court use)

FURTHER INFORMATION

Related documents:

- Australasian Guidelines for Digital Imaging & Processing
- SOP: Evidence Management
- *State Records Act 1997*
- *Evidence Act 1929*

Appendix 1: Original evidence management for matters unlikely to be referred to the Investigations Team

Purpose of Digital Evidence Capture	Action
Any matter where it is unlikely a prosecution will be considered. E.g: ■ Complaints ■ Audits ■ Licensing ■ Approvals	**Digital evidence** collected in these cases is classed by State Records as *transitory* and/or *ephemeral*. ☐ Copy the photos to the SWSA MS Excel Photographic Log as per Printed images & photographic logs of this SOP and print the relevant photographs. ☐ Create the requisite synopsis of any audio-recorded interview as per Audio Files of this SOP. ☐ Retain all original evidence on the capture devices' storage medium or copy them into the relevant electronic case file within your Team folder (in the G:/ drive) until you know the file is to be closed. **Unless** 1. The photos have been taken as part of an initial response to a **Critical Event** investigation and they are directly relevant to the **critical event** - as opposed to other unrelated non-compliances found on site; 2. A decision is made to refer a case to the Investigation Team for a **comprehensive investigation**; or 3. There has been a request for a review of an **inspector**s' decision and the matter is proceeding to the South Australian Employment Tribunal for resolution. If any of the above three triggers occur, the **Inspector** must produce: ■ a master copy disc as per this procedure, and ■ two working copies as per this procedure Once this is done, ■ One working copy can be kept in the compliance file. ■ The Master Copy must be placed in an evidence bag, then communicate with the Investigation Team Leader to organise for it to be deposited in the Keswick Evidence Storage Facility. ■ The second working copy should be given to the **Inspector** in the Investigation Team who is leading the investigation. Contact the Investigation Team if a transcript needs to be made of any audio-recorded interview as per this SOP
Original Image Deletion	The original images and/or recording should only be deleted from the camera or original storage medium (e.g. SD card) if: ■ they have been saved (unedited) in the relevant case file, in the Team folder on the G:/drive; or ■ a master copy and any required working copies have been made and

	stored as required.
When the file is closed	Do not store non-essential **digital evidence** on the G:/drive. **Digital evidence** relating to closed files should be stored in the relevant file in the T:/ drive along with the other documents etc relating to the case. Information stored on the T:/drive will still be accessible to the **inspector** involved in the case and their Team Manager/Leaders.

Appendix 2: Original evidence management for Critical Event investigations and other matters referred to the Investigation Team for a comprehensive investigation.

Eg ■ A Critical Event ■ Improvement notice ■ Prohibition notice And any other matter as determined by a Team Manager or Team Leader	1. Create a Master Copy disc and a working copy. **Important:** If the matter is a fatality investigation, a working copy disc as per this SOP must be made for provision to the Coroner. 2. Place the Master Copy in an evidence bag and organise for it to be lodged in the Keswick Evidence Storage facility in the presence of a Team Leader or Administration staff from the Investigation Team. The 'pink copy receipt' will go in the hard copy file and the 'yellow copy' will be attached to the evidence bag. 3. The working copy should be put in a cover in the relevant hard copy file. 4. Record these actions contemporaneously in your field note book and subsequent **inspector**'s statement. 5. Create, complete and print a full SWSA MS Excel based photographic log as per this SOP; and 6. Create the necessary synopsis or transcript of any audio-recorded interview as per this SOP. **Cases where Investigation Team involvement is no longer required** Occasionally, incidents that are initially declared **Critical Event**s (when the facts are gathered) turn out to be better addressed by Industry or DS Teams and Investigation Team involvement is no longer required. In such cases, any digital images taken as part of the initial response by the Investigation's **Inspector**/s will be: ■ used to create a Photo Log – with a hard copy of the log being printed for placement on the hard copy compliance file; and ■ the original images will be saved in the appropriate Investigation Team case file on the G:/drive.
Original Image Deletion	The original images and/or recording can only be deleted from the camera or original storage medium (e.g. DS card) if: ■ they have been saved (unedited) in the relevant file in the G:/drive; or ■ a master copy and any required working copies have been made and stored as required.
When the file is closed	Do not store non-essential **digital evidence** on the G:/drive. **Digital evidence** relating to closed files should be stored in the relevant file in the T:/ drive along with the other documents relating to the case. Information stored on the T:/drive will still be accessible to the **inspector** involved in the case and their Team Manager/Leaders.

Appendix 3: Glossary of Terms

Authenticity	Means the ability to confirm the **integrity** of the presented evidence and that the presented image/video/audio matches the original evidence.
Comprehensive Investigation	Means an investigation undertaken by the Investigation Team either into a matter that has been declared a **Critical Event** or has otherwise been referred to them for a detailed investigation.
Critical Event	Means any critical incident other matter reported to SWSA through the Help Centre or other means (e.g. the media or Minister's Office) that is deemed a '**critical event'** by a: • a **C&E Team** Manager • the Investigation Team Manager • the **On-Call Duty Manager** • the Chief Inspector • the Director Investigations or • the Executive Director.
Digital Evidence Equipment	Means any equipment used to capture, store and/or play **digital evidence**
Digital Evidence	Means any type of electronic evidence captured, stored or accessible via computer based equipment that supports or refutes a theory of how an offence occurred or that addresses critical elements of an offence, for example voice, photographic and video recordings of a workplace accident or an individual. **Digital evidence** is usually presented in hard copy, on a screen and/or via audio playing equipment.
General Voice Recording	A **general voice recording** is a recording of a discussion or conversation gathering information that may be of use at a later point in time.
Integrity	Means the original evidence as obtained by the person who captured that evidence was not modified as a result the act of seizing, acquiring and managing the evidence.
Inspector	Means an 'Inspector' or 'Authorised Officer' appointed under the: ■ *Work Health & Safety Act 2012 (SA)* ■ *Dangerous Substances Act 1979* ■ *Mines & Works Inspection Act 1920* ■ *Petroleum Products Regulations Act 1995* ■ *Shop Trading Hours Act 1977*
Original Evidence	Means the original image, video or audio file captured by the **digital evidence** capture equipment and as seen or heard by the person who captured that evidence.