NSW Police Force

New South Wales
Police Force

# Body-Worn Video Camera
# Standard Operating Procedure

## EDUCATION & TRAINING COMMAND

# Document Control Sheet

## *Document Properties*

| | |
|---|---|
| **Title** | Body-Worn Video Camera Standard Operating Procedure |
| **Subject** | Use of Body-Worn Video Cameras by NSW Police |
| **Command responsible** | Education & Training Command |
| **Authorisation** | Deputy Commissioner, Corporate Services |
| **Security Classification** | UNCLASSIFIED |
| **Publication date** | 27/11/2018 |
| **Current version number** | Final Version 2.2 |
| **Review date** | 1 July 2019 |
| **Copyright statement** | Copyright of this document is vested in the Commissioner of Police. © 2016 |

## *Modification History*

| Version # | Version approval date | Authorisation | TRIM / Summary of changes |
|---|---|---|---|
| 1.6 | 25 August 2017 | MEIG | Draft SOPs |
| 2.2 | 14 May 2019 | CET | Final Version |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# 1. Introduction

## 1.1 Purpose

These Standard Operating Procedures (SOPs) have been developed to guide police in the lawful use of Body-Worn Video (BWV) cameras. It also provides advice to police on when it may not be appropriate to use such equipment.

BWV cameras support operational policing activities. They will be used where police believe it is appropriate to record the events taking place or the environment they are operating in. The cameras will support police investigations by recording visual and audio evidence of an incident or crime.

The *Surveillance Devices Act 2007* allows police to use BWV in a broad range of situations. Police can record in public places, in private dwellings and premises (e.g. businesses), and in vehicles where they are lawfully entitled to be.

The use of BWV cameras will be incident specific, and the cameras will be worn on a police officer's uniform/clothes in an overt manner. Members of the public will be advised they are being recorded if it is practicable to do so before or at the time of activating the recording. If it is not practicable to do so before or at the that time, as soon as is reasonably practicable after activating the recording.

The use of BWV cameras and the content produced is governed by the *Surveillance Devices Act 2007 (the Act)* which treats Body-Worn Video recordings as **'protected information'**. This means the footage can only be used under certain circumstances as prescribed in the *Act* or under a regulation made under the *Act*. There are penalties in the *Act* of up to seven (7) years Imprisonment for the unlawful use or disclosure of such footage. If police fail to record something of relevance, they may be asked to explain their decision to a supervisor or a court.

BWV content will be securely stored, archived and disposed of in accordance with the *State Records Act 1998* disposal authorities.

**Five Guiding Principles** provide the basis for proper use of BWV cameras by NSW Police officers.

The principles are:


**Body-Worn Video camera equipment will be used by NSW Police in the lawful execution of their duties. Police will use their judgement when deciding to use it and its use will be obvious and overt.**

The *Surveillance Devices Act 2007* allows police officers to use BWV cameras overtly in the execution of their duties. When operating the cameras use will be in accordance with the Standard Operating Procedures (SOPs) and training developed for BWV use. It is expected that BWV use will be incident specific.


**Body-Worn Video will be used by police to record events, incidents and evidence. There will be some instances where Body-Worn Video should not be used and some occasions when its use may not be appropriate.**

The BWV SOPS and BWV training will assist police in making decisions when these issues arise. In addition, they will provide guidance to police who encounter vulnerable members of the community where use of the camera may require additional consideration.

**Body-Worn Video supports conventional forms of evidence gathering; it does not replace them.**

The BWV devices operate as a modern-day equivalent of a police notebook and provide a contemporaneous record of observations and events in the field. Police officers will continue to follow current procedures for best evidence collection and management and best practice for the presentation of evidence at court.

**Body-Worn Video recordings will be securely processed and managed in accordance with relevant legislation, policy and procedures.**

The BWV cameras, the BWV application and any associated BWV content are the property of the NSW Police Force. Data retention, review and disposal will be in line with relevant legislation and current guidelines developed in consultation with NSW State Records Authority. The NSW Police Force will, to the best of its ability, ensure the integrity of BWV content throughout the upload, storage, retrieval for official use and disposal process.

**The NSW Police Force will provide general information to the community on the use of Body-Worn Video by police.**

In implementing BWV, the NSW Police Force will provide general information to the public about BWV devices and their use by police officers.

Police will undergo comprehensive training prior to using BWV equipment. For further advice in relation to the lawful use and release of BWV content or other multimedia material, please contact the Operational Legal Advice Unit, Police Prosecutions Command in the first instance.

## 1.2 Scope

These Standard Operating Procedures apply to operational police.

## 1.3 Prohibited use of personal recording devices

All personnel are **prohibited** from using non-issue personal recording devices.

# 2. Body-Worn Video Use

## 2.1 Body-Worn Video and Official Police Notebooks

BWV will not replace the need to make a written record in an officer's official police notebook. BWV cameras support police conducting operational activities, by recording evidence and behaviour. When using BWV as part of evidence gathering officers should record use of BWV in their official notebook and where appropriate, include reasons for the exercise of police powers.

## 2.2 Conditions of Use

**BWV cameras should be used by police who have undertaken relevant training** ie: if you are trained and there is a BWV camera available you should use it. Training includes legislation, camera operation and use of the BWV application.

A BWV camera can be used by a police officer wearing uniform or plain clothes, but any use must be overt and in the lawful execution of duty. Overt use refers to the use of a BWV device in a way that it can be seen and identified as a video and audio recording device. The device is to be worn so that it is observable and not hidden, concealed or secreted. Officers will, when practicable, announce to persons they are speaking with that their conversation is being recorded by the BWV camera being worn by the officer.

Any police officer in plain clothes must provide evidence they are a police officer and identify themselves as such.

All police officers wearing police uniform, whilst engaged in duties of operational response, should wear as part of their uniform a BWV camera for use in accordance with these SOPs. Police engaged in proactive and/or investigative duties should also take and use BWV cameras in support of their policing activities.

## 2.3 Police Use of Body-Worn Video – General Information

A police officer will activate their BWV camera when it is appropriate to do so. In making the decision to activate the BWV cameras a police officer will use their own judgement and take into account a number of factors including:

- Officer safety and protection
- The need to capture evidence
- Accountability
- Community expectations
- Contentious situations
- Involvement of vulnerable people
- Protection for offenders and the community
- Any other relevant factors that exist

Police can use BWV to:

- record private conversations they have with others, whether or not all parties to the conversation consent to the recording; and

- record events in any location, regardless of whether it is a public place or private property

Use of BWV includes the capturing of events unfolding as police approach a location or recording their initial approach towards a person. Section 50A (3) of the *Surveillance Devices Act 2007* allows recordings which are inadvertent, unexpected or incidental.

The *Surveillance Devices Act* also covers the unintended capture of secondary or nearby conversations taking place when police are speaking with another party.

Police should use the BWV camera during their shift to record incidents they attend, evidence they see and conversations they have with members of the public.

BWV recordings should be incident-specific (whether or not the recording is ultimately required for use as evidence). Police will not be required to record their entire shift or every interaction that occurs whilst they are on duty.

Once a BWV camera is activated to record, the person being recorded should be advised of the presence of the camera and that it is recording their actions and conversation. If it is not practicable to do so before or at the time, as soon as is reasonably practicable after activating the recording. The recommended statement to be used by police when using BWV to record a conversation is:

> **"I am wearing a Body-Worn Video camera and our conversation, and your actions are being recorded. Do you understand that?"**

A BWV camera **<u>should</u>** be used in the following circumstances:

- when police would normally use their official police notebook to record information
- to capture evidence or record something of relevance
- when exercising a police power or performing a policing function
- first response crime and incident investigation. BWV can be very effective for recording the location of objects and evidence at the scene of a crime or during a search situation in the field
- licensed premises (Business) inspections and patrols
- policing incidents involving antisocial behaviour
- vehicle stops
- conversations with members of the public which may relate to an incident, is relevant to an investigation, potential criminal proceedings, or contains possibly valuable information
- situations where the use of force is anticipated, except search warrant entries
- when conducting intimate (strip) searches (Law Note 46: *R v Jimenez* [2000])

All recordings should be treated as having evidentiary value until confirmed otherwise. The primary investigating officer at the scene of an incident should activate their BWV camera to record any evidence relevant to the investigation. Other BWV users attending the same incident should consider using their camera to collect their own evidence.

## 2.4. Filming of Strip Searches

Police must provide the best possible evidence available, including BWV footage of police actions. However, LEPRA dictates the need for police to ensure the protection of rights and dignity of people with whom they interact.

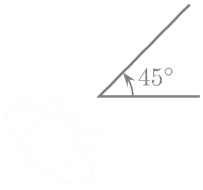
A person's privacy is not a sufficient reason to cease filming a strip search conducted in the lawful execution of an officer's duty. Particular care is required to ensure the person's privacy is adequately protected by ensuring the footage cannot be viewed by people without a lawful reason to do so.

Officers must be certain of their powers regarding strip searches before commencing any strip search. This is covered in Section 31 of LEPRA as follows:

> *A police officer may carry out a strip search of a person if:*
>
> *(a) in the case where the search is carried out at a police station or other place of detention—the police officer suspects on reasonable grounds that the strip search is necessary for the purposes of the search, or*
>
> *(b) in the case where the search is carried out in any other place—the police officer suspects on reasonable grounds that the strip search is necessary for the purposes of the search and that the seriousness and urgency of the circumstances make the strip search necessary.*

Police must familiarise themselves with the rules pertaining to strip searches contained in Section 33 of LEPRA.

The searching officer is to ensure, if they are wearing a BWV camera, that it is turned off during the conduct of a strip search. The support officer is to record the search using a BWV camera. During the strip search, compliance is required with all relevant provisions of LEPRA.




T2(d)

## 2.5 When not to use Body-Worn Video:

A BWV camera **should not** be used in the following circumstances:

- to record an entire rostered shift, except where justified in the specific circumstances
- to record material that is not related to the lawful execution of police duties
- to covertly record material
- within 25 metres of a suspect device or flammable material
- for work surveillance purposes
- when the filming does not comply with LEPRA (e.g.: if a male police officer was to record a female suspect during a strip search)
- in connection with the execution of a search warrant prior to or during forced entry
- A courtroom or court precinct unless responding to an incident.

## 2.6 When it May Not be Appropriate to Use a Body-Worn Video Camera

The primary purpose of BWV is to capture real-time information and evidence. Common sense, experience and good judgement should be used when making a decision to use BWV. The recording of vulnerable members of the community, in particular young persons and individuals with intellectual or physical disabilities, may present challenges that attract discretion.

### 2.6.1 Unrelated/prejudicial Commentary

BWV should not to be used to record general police conversation, for example, when patrolling in a police vehicle. Police are reminded that appropriate language should always be used and commentary that may amount to opinion or hearsay evidence (which may be prejudicial) should be avoided.

### 2.6.2 Professional Conversations

Police should not record images or conversations dealing with strategy, methodology, tactics and lines of enquiry or other case-related issues. Officers should, where possible, avoid recording police specialist equipment, preparation and execution of tactical activities, discussions with other police or personnel from other agencies at incidents or major operations. If in doubt about such content, BWV users should seek advice from a Supervisor.

### 2.6.3 Capture of Confidential Information

T1(f)

### 2.6.4 Interactions with Vulnerable Persons

Police may attend incidents where parties in the matter may be considered to have special needs or could be classified as vulnerable persons. These people may be witnesses, victims or persons of interest.

Use of Body-Worn Video in such situations may need to be considered in light of the vulnerability of the person with whom police are dealing. Appropriate communication is required to ensure understanding of the Body-Worn Video camera, its purpose and use.

Clause 24 of the Law Enforcement (Powers and Responsibilities) Regulation 2005 provides the following guidance for vulnerability:

- children (young persons under the age of 18)
- people who have impaired intellectual functioning
- people who have impaired physical functioning
- people who are Aboriginal or Torres Strait Islanders
- people who are of non-English speaking background

Body-Worn Video is another way of recording investigative processes. When interacting with a person identified as vulnerable, police will, where practicable, announce that interactions are being recorded in such a way as to be understood by the vulnerable person. A support person may be required to assist in this process. Once it is clear the vulnerable person does understand the reasons the Body-Worn Video is being used, police should ensure that evidence of their understanding is included in the recording.

### 2.6.5 Vulnerable Person Requiring a Support Person or Interpreter

Where police encounter a vulnerable person that requires a support person or interpreter, every effort should be made to find a suitable person to fulfil these roles. Body-Worn Video may still be used to capture evidence of the scene. If and when a support person/interpreter arrives, inquiries can continue with the vulnerable person as per normal police procedure, including the use of Body-Worn Video, if considered appropriate.

Police must use accredited interpreters in operational and legal matters to communicate with people who:

- are unable to communicate in English
- have limited understanding of English
- are more comfortable communicating in their first language
- are deaf, hearing impaired or speech impaired or
- are support people for child victims, offenders and witnesses

In some cases, police may choose to cease the use of Body-Worn Video in favour of other available means of recording the situation.

### 2.6.6 Body-Worn Video Use on Private Premises

T1(f)

### 2.6.7 Objections to Recording

The legislation allows for police officers to record incidents without consent. Therefore, users are not required to obtain the expressed consent of a person being recorded. Best practice is to record the objection and inform the person that their objection has been noted but that the recording will be continued. However, if continued recording would result in important information not being disclosed, then police should consider ceasing the recording to obtain such information.

Police may also cease recording if they believe there are compelling reasons for doing so. These reasons should be placed on the video record prior to the recording being stopped or recorded in an official police notebook.

## 2.7 Uploading and Tagging Body-Worn Video Footage

At the end of a shift return the BWV camera to the docking station where uploading will begin automatically. Footage will remain on the local server until it is 'tagged' by the user as content that is of evidentiary value ie: the footage may be relevant to an investigation, disciplinary procedure, legal claim or complaint. Failing to tag material with such relevance may lead to managerial or disciplinary action. Content not tagged is considered non-evidentiary and will remain unclassified on the local server for a period of six months, when it will be automatically deleted.

BWV footage/content can be tagged under three (3) categories:

1. Evidence
2. WHS (Work, Health & Safety) – only to be used where the content is not already tagged as evidence and it relates to a work, health and safety issue that might be in the interests of the BWV user and/or the NSWPF to keep
3. Complaint – only to be used where the content is not already tagged as evidence and only where an officer believes that keeping such footage may assist in the investigation of a possible future complaint

Create a relevant COPs record for incidents the subject of BWV content. This may be an Event, Intelligence Report, Case etc. Access the BWV application and tag any relevant BWV content as evidence.

Obtain the corresponding COPs record number (event, intelligence report, case number) to complete the tagging process. Once tagged, the BWV content will be moved to secure storage in the VIEW IMS database. Access View IMS to review BWV content (see BWV Intranet page for information on viewing BWV content).

When tagging BWV content as evidence, consider whether the content contains sensitive material or requires additional security considerations. If so, select the 'PII/Security' check box. This will ensure that due consideration is given to whether the BWV content should be treated (de-identified etc) prior to release to third parties (accused/defence, public release, etc).

After tagging, BWV content will have archive, disposal and destruction protocols assigned in accordance with the *State Records Act 1998 (NSW) retention and disposal authorities*. BWV content not tagged as evidence will be securely stored and scheduled for destruction after six (6) months from the date of recording.

### 2.8 Using Body-Worn Video Footage

If an officer's image has been, or may have been recorded by BWV, and that officer has concerns about their image being released (eg: provided as part of a brief of evidence), they must advise the OIC of the case if they want their image to be redacted prior to release.

Do not use, communicate or publish BWV content unless it falls within one of the authorised uses identified within *section 40* of the *Surveillance Devices Act 2007 or* permitted by regulation, such as:

- in criminal court proceedings
- Coronial inquests and inquiries
- where the material has been disclosed in open court or where the material has entered the public domain
- the investigation of offences
- brief/statement preparation, or advice on whether a prosecution should be commenced and for what offence
- investigation of complaints including oversight by the Law Enforcement Conduct Commission
- connected with the training and education of police
- connected with the exercise of a law enforcement function by a police officer
- investigation of critical incidents

Do not copy, use or disclose BWV material for non-official purposes, such as to show to any unauthorised person or share on social media.

In certain circumstances, it may be lawful to release BWV footage to news media with authority. Refer to Section 4.5 of these procedures, and the NSW Police Force Media Policy for further information.

The *Surveillance Devices Act 2007* provides a prohibition on the use, communication or publication of **protected information**. Section 40 of the *Act* creates offences for the unauthorised release of such information. Unauthorised release includes if a person:

- intentionally, knowingly or recklessly uses, communicates or publishes any protected information
- intends to endanger the health or safety of any person or prejudice the effective conduct of an investigation into a relevant offence

Penalties range from two to seven years imprisonment.

Advice should be sought from the Office of General Counsel if there is uncertainty about whether BWV footage can or should be disclosed.

BWV content is not to be shown to any unauthorised person/s solely for entertainment, personal enjoyment or curiosity.

A complete copy of BWV footage, or an edited version for court, defence and prosecution may be created. Images from the footage can also be captured as photographs for use as evidence and may require compliance with the Crimes (Forensic Procedures) Act. Copies of BWV footage for production at court can be made in many video formats including DVD. In some cases, custom editing may be required for BWV content. Refer to section 3.5.2 of these Standard Operating Procedures.

## 2.9 Viewing Body-Worn Video Footage – Accused Person/Legal Representative

Where BWV content is to be used to support a charge or legal process, police may offer the accused, and/or their legal representative, an opportunity to view BWV content. This should be offered before the date of first court mention and/or before entry of a not guilty plea. If the opportunity is accepted, viewing of the BWV footage is to be facilitated under police supervision.

If an accused or their legal representative requests further viewing of BWV footage, this may also be facilitated.

## 2.10 Review and Audit

Police supervisors will have access to BWV footage for auditing of compliance with Body-Worn Video procedures and standards. The BWV application will generate random 'dip samples' for checking by police supervisors on a regular basis or on demand.

## 2.11 Release of Body-Worn Video Footage

Police are the subject of various requests for the release of information through legal process (subpoena), under the direction of oversight agencies (LECC) or pursuant to the Government Information (Public Access) Act (GIPAA). The Information Access and Subpoena Unit and Office of General Counsel facilitate the NSW Police Force response and provide advice regarding such requests.

Established procedures for police to follow are set out in the Police Handbook, Chapter 'S' for Subpoenas and Chapter 'G' for GIPAA requests.

The NSW Police Force may wish to release BWV images for reasons of public safety or for investigative purposes. The release of any material for public viewing is to be coordinated through the Police Media Unit once authorised through the chain of command.

### 2.12 Trouble Shooting

If a BWV camera is not operating, report the issue to a supervisor. The supervisor must investigate, and once confirmed, remove the camera from operation. A 'RASP' request indicating the camera fault is to be generated, with a note regarding whether or not BWV footage requires retrieval.

If a BWV kiosk, docking station or software is not operating as it should, report the issue to a supervisor. The supervisor must investigate and once confirmed, initiate a 'RASP' request outlining the problem. If the entire operating system is not functioning, consider suspending camera use until the malfunction has been repaired and the system returned to operational status.

## 3. Body-Worn Video Evidence

### 3.1 Evidentiary Content

Evidentiary content is video footage of an incident or encounter that can be used for evidentiary purposes, such as a recording of crime, an arrest, a search, use of force, an interaction or confrontational encounter with a member/s of the public

### 3.2 Relying on Body-Worn Video Content as Part of Evidence

Police should view BWV footage of an incident and interactions with witnesses, prior to preparing police or witness statements.

Include in the fact sheet that BWV footage was taken during police attendance at the incident, describe what has been recorded and is available to the court.

Should there be a disruption to recording an incident, the user should produce the available footage supplemented with a written statement detailing any other evidence. This should include the reason, if known, for the equipment failure or recording disruption/malfunction.

If the reason for failure requires further investigation, it may be necessary to obtain a statement from a suitably qualified expert. It may also be appropriate that the BWV equipment is sealed and stored as evidence.

### 3.3 Police Officer Statements

A statement introducing BWV footage to court should contain relevant information regarding chain of custody. If there is a break in recording, the user should include details and reasons in their statement. Further information in relation to exhibits may be found in the Police Handbook – Chapter 'E' 'Exhibits' and the EFIMS Standard Operating Procedures.

A police officer may view another police officer's BWV footage to refresh their memory of an incident, which must be included in their statement. After viewing the relevant file/s, a RASP request is required for production of a DVD.

A BWV statement format has been developed and can be located on the BWV Intranet site.

## 3.4 Witness Statements

BWV can be used to capture first account witness statement/s at or nearby a scene of crime. Witnesses should be permitted to review their account prior to making and signing any written statement. Care should be taken to ensure that witnesses are not permitted access to any aspect of the recording other than their own first account. The witness statement must refer to viewing the BWV footage to refresh their memory prior to completion of their statement.

## 3.5 Briefs of Evidence

Where relying on BWV footage as part of your evidence, you must produce copies of the relevant footage in an appropriate format for the location of the court hearing (usually DVD) as part of the Brief of Evidence. Copies of BWV are obtained by submitting a RASP request. All BWV footage produced for viewing purposes will have a 'caveat' screen prior to the video that provides information concerning penalties for unlawful disclosure or publication of the material.

BWV footage will form part of the Brief of Evidence prepared for:

- Defence (1 x copy)
- The Court (1 x copy supplied to the Prosecutor)
- File (0 x copy – there only needs to be a reference to the View IMS file name)

If the BWV content contains sensitive material (refer to the Criminal Procedures Act, 1986, Sec. 281B), then such sensitive material is not to be provided to the defence and steps should be taken to edit this material out.

The caveat screen will warn the accused or their legal representative that the footage is 'protected information' under the Surveillance Devices Act; is subject to copyright; and may only be used for the purposes of preparing a defence to the charge/s. Police are reminded that BWV footage should not be disseminated further than the confines of legal process and the court. However, formal requests for BWV footage may be made via subpoena or GIPAA applications which should be dealt with in the usual manner.

In some circumstances, a BWV camera may have been used at an incident, but the BWV content is not being relied upon as evidence in any legal process that follows. This may occur where the BWV footage does not show anything relevant to the offence. Consideration must be given to Section 62 of the Criminal Procedure Act 1986 (NSW) in these circumstances which requires a brief of evidence in indictable proceedings to contain:

a. Copies of all material obtained by the prosecution that forms the basis of the prosecution's case

b. Copies of any other material obtained by the prosecution that would affect the strength of the prosecution's case

c. Copies of any other material obtained by the prosecution that would affect the strength of the prosecution's case

Most courts will have facilities to view BWV footage as part of normal court proceedings. Contact should be made with the Police Prosecutor of the court where the matter is to be heard to ensure that adequate video playback facilities are available. BWV footage can be produced in a number of playable formats. Ensure that a copy is produced that is compatible with the equipment available at the court where the matter is listed.

### 3.5.1 Informant / OIC – BWV Destruction Orders

Where BWV footage has been supplied to the defence, at the conclusion of the court matter the OIC should seek an order for return of that footage. Upon return, and after the appeal application time has lapsed, BWV copies are to be destroyed in the presence of a witness, with a note of the destruction recorded in an official police notebook. Reference the destruction in the relevant COPS Event or other record.

### 3.5.2 Custom Editing of Body-Worn Video Footage

In some cases, BWV footage may require custom editing, for example de-identification of facial images; or editing out portions to capture relevant footage to assist the Court. In such circumstances a 'RASP' request is required with sufficient detail to ensure an appropriate edited copy is provided. Any editing undertaken must be recorded an may later require explanation to a supervisor or court.

### 3.5.3 Transcription

Where a transcript of a BWV recording is required, make application in the same manner as for an ERISP transcript.

Even when the exhibit concerned has been the subject of an audio transcription, the video contains important visual information such as actions and gestures that can put language into context. Even if a transcript is provided, the video exhibit should still be shown in conjunction with the written text. (Refer to ERISP Transcription Guidelines for further information)

# 4. Information and Records Management

## 4.1 Security of Body-Worn Video Records and Metadata

The NSW Police Force has a secure and auditable video management system to process and manage BWV content. The content is stored on a secure server as the **Master Copy** and cannot be altered or tampered with. All BWV recordings should be treated as having evidentiary value until confirmed otherwise. Police must tag all recordings with evidentiary value for retention.

All untagged BWV content will initially be treated as non-evidentiary and securely stored. Unless this is changed that content will be destroyed in six (6) months.

A police officer responsible for recording BWV content will identify and classify content to be kept using a tagging application. All BWV content tagged as 'evidence' will be treated as evidentiary material and will be kept in accordance with the *State Records Act 1998* (NSW)

disposal authority governing the retention and disposal of police records. All BWV recordings in relation to Critical Incidents must be tagged to ensure retention until the conclusion of the coronial inquest or inquiry, unless earlier ordered by a coroner.

The BWV application will automatically create a metadata record for each BWV content file. It contains information about the recording including the time and date captured and the identification of the camera. Metadata will be kept indefinitely. Metadata does not contain personal information of those people recorded.

The BWV application has encrypted security and will only allow police to access content they have uploaded. Police supervisors and systems administrators can access BWV content other than their own for 'dip sampling', quality review and audit purposes. Police can access BWV content for viewing prior to statement and brief of evidence preparation. Each time an officer accesses BWV content, including copying a file, a record is created. These activities can be audited through the BWV Application and the Police VIEW Information Management System.

### 4.2 Archiving and Disposal

BWV content is governed by *State Records Act 1998 (*NSW*)* retention and disposal authorities (DA220, DA221 and GA28). These disposal authorities relate to specific offence types that govern the length of time records are required to be kept by the NSW Police Force.

Once the BWV file has reached the date applicable to its disposal authority classification, it will be permanently deleted from the system. The metadata record of its existence within the system will be retained permanently.

### 4.3 Work, Health & Safety Incident

If a Work, Health & Safety issue has been captured on BWV such as a slip, trip, fall incident, the video can be tagged to support the P902 Incident Notification and any subsequent investigation.

### 4.4 System Audits (CMF)

Police Area, Districts and Specialist Commands where BWV cameras are assigned will establish Command Management Framework (CMF) checks of the equipment, any content stored on the BWV system and VIEW IMS. Dip samples of content will be generated for supervisors to assess them against training, compliance with BWV SOPs and policy, as well as the *Statement of Values* and *Code of Conduct and Ethics*.

Commanders are to ensure that:

i. all BWV equipment (cameras and batteries) are maintained; inspected weekly; and included in the CMF report
ii. dip samples (recommend 1% minimum of weekly uploads) are conducted for compliance with BWV SOPs and policy
iii. ensure any damaged or unserviceable cameras are removed and arrange for them to be repaired or replaced
iv. COPS events are reviewed to ensure the appropriate activation of BWV

### 4.5 Release of Body-Worn Video to the Public

The NSWPF may release BWV images to the public for a number of reasons, including:

- tracing wanted suspects
- locating people who have escaped or absconded from custody
- public safety

Please refer to the NSW Police Force Media Policy for further information.

### 4.6 Critical Incidents and Body-Worn Video

Where a BWV has been used to record events relevant to an event which subsequently becomes a Critical Incident Investigation, action should be taken to secure the BWV camera as soon as possible. At the earliest opportunity the Senior Critical Incident Investigator is to be informed of the existence of BWV content relevant to the incident.

No attempt should be made to view or download any footage from the BWV camera until the Senior Critical Incident Investigator, or a member of the Critical Incident Investigation Team, is present to supervise the process.

Police directly involved in a Critical Incident should be provided the opportunity to view relevant BWV footage prior to being interviewed.

Please refer to the NSW Police Force Critical Incident Guidelines for further information.

## 5. Further Information

### 5.1 Advice and Contacts

For advice on the application of these Standard Operating Procedures please contact:

**Education & Training Command**

For general advice about the NSW Police Force use of BWV please refer to the following sites.


NSW Police Force BWV Intranet page

NSW Police Force Internet page

# DFU Mobile Phone Guide and FAQ

*"Generally, there are at least three things at a crime scene, a victim, an offender, and a mobile phone."*

DFU has the ability to extract data from mobile phones, SIM cards, and flash card memories that are installed in phones.

Mobile phones have evolved beyond simply making and receiving phone calls. Current technology allows phones to be used as digital cameras and provide access to the internet. Most models of mobile phones are closer to computers than a standard phone, allowing a user to install programs, create documents and do other things commonly associated with a computer.

Phone technology has already advanced to the point where a mobile phone comes as an "all in one package" having the same functions as computers, MP3 players, GPS, PDAs, and many other devices.

**DISCLAIMER:** Phone technology is constantly evolving. All information in this guide was accurate at the time of publishing. If you have any questions please contact us.

## Mobile Phone Frequently Asked Questions (FAQ)

## Potential Data

### How can information from mobile phones assist me?

- The data that mobile phones contain can add a lot of *corroborating** evidence to an investigation.
- Recent call lists can confirm a person is associated with another, especially since missed calls do not show up on CCR and reverse CCR's.
- If you don't capture SMS's live through an intercept you have little chance of getting anything except the time and data from the Telco. An SMS in a phone may indicate a time and meeting place.
- Offenders regularly film, or photograph associates, proceeds of crime, the actual offence, and many more.
- Contacts lists can show all associates and can be used in other intelligence tools to map out associates and drug infrastructures.

* As with all investigations you should not rely on just one piece of evidence. Just because some information is on a phone does not mean it was the owner who put the information on there. Use evidence from a phone to corroborate and enhance evidence or vice versa.

### Examples of investigations where phone data has been highly valuable

- A murder investigation had no evidence to place the accused at the scene where she met the victim before leaving and ultimately taking his life. A picture on a phone was taken of the accused with the time and date shortly before the murder, which was good enough to show the exact location of the accused at that time.
- A young girl was sexually assaulted, and the offender used SMS to procure her. He denied this and deleted all messages. DFU retrieved 20 deleted messages from the SIM card which clearly showed he had procured the victim.

- A male planned a robbery of a bank. He sent an SMS to a friend asking him to do the job with him. One hour after that SMS the bank was robbed of a large sum of money. 30 minutes later he sent an SMS to his friend indicating how much he just got from the job.
- A group of males robbed a bank wearing a balaclava, pull over jacket, and used a sawn off shot gun. They took photos of each other on their phones wearing the same gear and with the balaclava and shot gun. The time and date on the phone was just before the robbery

- **What information can DFU extract from a SIM?**

T1(f), T1(h)

- **What information can DFU extract from a mobile phone?**

Each mobile phone model can be vastly different and may not store or allow the extraction of certain data.

- Contacts
- Short Message Service (SMS)
- Call Register (Received, Dialed, Missed)
- Calendar
- Pictures
- Videos
- Audio
- Multimedia (MMS)
- Web
- Tasks (To do list)
- EMS (Enhanced Messaging Service)
- Notes
- Phone settings (You must specify you require this, eg. ringtone set)
- Installed programs

- **What can DFU get from a flash card in a phone?**

Generally a flash card is an extension of the phone's memory, allowing more information to be stored on the phone. Deleted data from flash cards can be recovered but generally date and time data might not be recovered regarding that particular file.

- Pictures
- Videos
- Audio
- Installed Programs

- **What information can DFU NOT get from a mobile phone?**

- T1(h)

T1(h)

# PINs and security

## What do I do if the SIM card has a PIN?

T1(h)

T1(h)

# Seizure and handling

## What should I look for during a search warrant or seizing a phone?

- **Handsets.** old and new
- **Packaging.** The original boxes the handsets came in as they may have phone numbers or PIN codes in them
- **SIM cards.** Some people will use multiple SIMs in the same phone
- **Flash memory cards.** These cards can be used in phones and computers. Check computers for the devices. See here for pictures of the different types of flash cards (coming soon)
- **Battery charger.** DFU can charge all batteries but life is easier when the charger is with the phone

## Should I switch the phone off straight away?

This decision will rest with you. Contact DFU in the first instance for advice.

Leaving the phone on runs the risk of incoming messages or calls overriding any deleted messages on the SIM card. If getting data off the phone is urgent and there is a risk that switching it off will enable the security on the SIM and phone then it may be best to leave the phone on.

You may have to take the phone to DFU straight away or obtain a charger to ensure the battery does not run out. While DFU holds a range of phone chargers for common models, it is quite possible that we won't have the charger for your specific model.

## Can DFU examine a phone if it needs to have a fingerprint or DNA examination?

You need to decide what is more important - the fingerprint/DNA evidence or the data. In order to do a phone examination the phone and SIM must be handled (with gloves). The buttons on the phone must be pressed and the case removed which can sometimes require manipulation and force.

There is a chance that fingerprints could be smudged or removed. There is also a chance that DNA evidence could be contaminated. DFU take all precautions they can to prevent this but we recommend that biological forensics are performed prior to data extraction.

However, DNA and fingerprint examinations also have a chance of destroying the phone if the chemicals that are used interfere with the circuit of the phone. Again this is a risk you must decide upon.

- **IMPORTANT:**
  DFU does not have a clean-room facility for handling exhibits contaminated with biological or chemical substances. We cannot accept these exhibits at DFU for examination. You will need to discuss your requirements with DFU and make any arrangements for an examination at a suitable facility to proceed.

# DFU Involvement

### How long will it take to get the data from the phone? How will it be presented?

Processing time can vary widely. Some supported phones can extract data in minutes, and the process is quick enough for you to wait at DFU. As phones become more complex and contain more storage, the processing time increases significantly.

Some phone models require a lot of effort from DFU to extract the data, and may require some research to find out how it can be done. We often extract data in a raw format, which can mean a lot more time is required to make it presentable for you.

Please note however that all phone jobs, however straightforward, are subject to the same acceptance criteria and Request for Assistance procedure as other jobs.

You will normally receive a printed report. If you want the data in an alternative format, please discuss this with SEEB beforehand. A Results CD or DVD can be created but generally only if the amount of information is too large to be printed, or if it includes video, audio or other data that cannot be meaningfully presented in printed form.

- ### What about the data that DFU cannot extract?

Not all phones allow all data to be extracted. The common practice is to photograph or film the actual screen of the phone.

If there is a small amount of data to be filmed on the phone, DFU staff may film it for you. If there is a lot of data (such as 100 SMS) we will ask you photograph or film the information you believe is relevant. DFU can assist with cameras if necessary.

- ### Will DFU provide a statement?

We will provide covering statements for reports generated by DFU. The statement will generally not contain any evidence and will only introduce the reports regarding each phone.

If the structure of information or definition of phone related information - e.g. "what is an SMS", or "how can deleted data be retrieved" - needs to be explained in court, a DFU specialist will need to be called.

DFU cannot give evidence on the content of the data in the report, i.e. "who sent this SMS" or "who does this number in the contact list belong to".

# Technical Stuff

### Some dates & times do not match information I have about the phone... or why is the date and time zero?

Each phone handles information differently and may store date and time based on the network date and time (which is always correct) or based on the phone's date and time. Most phones lose the date and time as soon as you remove the battery from the phone. If the user does not reset the date and time, future information may record the unset date and time. Testing of the phone type can determine if this is occurring.

If you know the date and time is incorrect you can use other methods to help determine the date and time such as comparing call records to information in the phone

- ### Can I get a phone tested to confirm results?

Yes, if the matter is serious enough and DFU believes we can produce relevant evidence. An example of testing may be on whether the phone stores certain dates and times based on the network time or the time set in the phone.

Please consult with DFU if you require further testing and we will assess your request.

- ### What is the difference between GSM, 3G and CDMA phones?

GSM, NextG and 3G (3 GSM) are basically the same, however 3G is a 'next generation' network. 3G allows far more information to pass between phones, such as access to the internet and video phone calls. Both can use normal (GSM) SIM cards whilst a 3G phone can use a 3G SIM card.

GSM handsets, including 3G phones, are uniquely identified by a number called the International Mobile Equipment Identity (IMEI). The IMEI is normally recorded on a label inside the battery compartment of the phone, along with the phone model name. Be aware that removing the battery to obtain these details can cause phone date and time to be lost.

CDMA phones do not have SIM cards and are mostly found in remote areas. They also have an ESN (Electronic Serial Number) instead of an IMEI. To get the phone number for a CDMA phone you submit an IASK on the ESN.

END OF INFORMATION