

Victoria Police Manual

The Victoria Police Manual is issued under the authority of the Chief Commissioner in s.60, Victoria Police Act 2013. Non-compliance with or a departure from the Victoria Police Manual may be subject to management or disciplinary action. Employees must use VPM Professional and ethical standards to inform the decisions they make to support compliance.

Child abuse material investigations

Context

Sexual offending committed against any member of the community is unacceptable, and Victoria Police is dedicated to investigating and successfully resolving such matters.

Investigations relating to the production, distribution or possession of Child Abuse Material (CAM) will often require the analysis of computers, phones or electronic devices. Currently there are two methods for analysing these devices:

- at the Cybercrime Squad, or
- at one of the Griffeye sites located in some SOCIT offices and Multi-Disciplinary Centres around the state.

The Cybercrime Squad and Griffeye sites facilitate the analysis process, providing for the safe handling of CAM and management of CAM investigations.

The investigation of any sexual offending can be difficult, however; sexual offending against a child is especially confronting and can have an adverse effect on employee wellbeing if not managed effectively. Victoria Police places great importance on promoting, supporting and maintaining the mental health and wellbeing of Victoria Police employees.

This policy provides clear responsibilities and procedures for the safe handling and management of CAM investigations. It addresses the:

- sensitive nature of CAM investigations
- welfare of employees
- legislative requirement to avoid exposure of CAM to persons not directly involved with the investigation
- management of offender welfare.

Contents

1.	Seizure of devices/investigation of offences	2
2.	PALM – property handling and recording requirements.....	3
3.	CAM analysis	3
4.	Handling CAM.....	6
5.	Brief preparation	6
6.	Brief service.....	8
7.	Finalisation and disposal.....	8
8.	Employee welfare	10
9.	Offender welfare management.....	12

Definitions

Child Abuse Material – as defined in the *Crimes Act 1958*, CAM refers to any film, audio, photograph, printed matter, computer game, text, electronic material or any other thing of any kind

that describes or depicts a person who is, who appears to be, or is implied to be a child, being a victim of torture, cruelty or physical or sexual abuse, engaging in sexual activity or depicted in an indecent sexual manner or context, and a reasonable person would regard as being, in the circumstances, offensive.

Australian Child Abuse Classification Schema (ACACS) – this model is a scale of categories (1 to 4) describing different forms of files, both legal and illegal. Category 1 directly correlates to Interpol Baseline and depicts a real pre-pubescent child under 13 years of age. Category 2 is CAM that does not fit into category 1 but is still illegal to possess within the relevant jurisdiction. Category 3 is non-illegal content of investigative interest and category 4 is ignorable.

Scope

This policy applies to all employees involved in CAM investigations including but not limited to: members from SOCITs, CIUs, the Joint Anti Child Exploitation Team (JACET), prosecution employees, Digital Forensic Officers and frontline members.

In the case of Professional Standards Command (PSC), CAM must be managed internally by PSC in line with the principles of this policy. PSC has an independent structure relevant to the management of CAM.

Responsibilities and procedures

1. Seizure of devices/investigation of offences

- It is important to be aware that offences arising from CAM investigations can be diverse depending upon the behaviours being investigated.
- There is both State and Commonwealth legislation covering offences involving CAM and the appropriate legislation should be utilised dependent on the behaviours being investigated.
- Likewise, there are similar warrant provisions as well as password requirements in both jurisdictions.
- At the commencement of the investigation the informant should seek advice and support from the JACET and/or the Cybercrime Squad or E-Crime Liaison Officers, and consult with the Office of Public Prosecutions (OPP) or the Commonwealth Director of Public Prosecutions (CDPP) to determine the:
 - relevant jurisdiction
 - investigation strategies
 - appropriate warrant
 - search planning
 - evidence seizure
 - relevant charges; and
 - court requirements.
- The JACET and the Cybercrime Squad intranet pages, and the CDPP website, have helpful information regarding the investigation of CAM offences; including sample affidavits and warrant packs.
- Employees must contact the Cybercrime Squad or JACET for advice before considering the provision of electronic copies of images/videos/text. This advice is intended to ensure legislative compliance and appropriate handling of any reports containing CAM.

2. PALM – property handling and recording requirements

- Employees should comply with existing property management policy when managing seized property that contains CAM (see **VPM Property and exhibit management**).
- The Cybercrime Squad has processes in place to cover the continuity of devices left overnight or longer at the Cybercrime site.
- The informant is responsible for entering the analysis reports (referred to under sections 3.1 and 3.2) onto PALM and to enter that file number against the device/s analysed.
- The computer, phone or other electronic digital device should be retained until the investigation and any associated court proceedings and appeals are finalised (refer to section 7.3).

3. CAM analysis

When categorising CAM employees must use the ACACS.

The informant is responsible for conducting the categorisation. This process should be completed with the assistance of the Griffeye program which assists by identifying previously categorised CAM files. Informants will still need to manually categorise any un-identified images.

Prior to commencing any CAM categorisation, members must complete the Interpol Baseline Classification online learning module available on the Victoria Police Learning Hub.

The task of categorising the CAM can be shared as a way of minimising trauma to an informant. This is preferable where a large amount of CAM needs to be categorised. If this process is adopted the informant must conduct a final check of the categorised CAM to ensure the files meet the legislative definition and comply with ACACS. The informant's supervisor is responsible for ensuring compliance with best practice strategies (see section 8.3).

3.1 Griffeye

Griffeye is the application used by VP to categorise CAM. Griffeye is installed on stand-alone computers located at a number of rural and suburban SOCIT sites (a list of these sites is located on the Cybercrime Squad's intranet pages – which is continually updated as the software is rolled out to more sites).

Each of these sites has at least one Griffeye Operator, who is a SOCIT member trained in the functions of the Griffeye program.

Process

- To facilitate access to Griffeye the informant must confirm with the local Griffeye Operator that capacity exists to action their request. Where capacity does exist the informant must:
 - submit a Request for Analysis form (obtainable from the Griffeye Operator) to their unit supervisor for approval. Please note: the Request for Analysis report, located on the Cybercrime Squad's Intranet page, must not be used for Griffeye requests
 - ask their supervisor to forward the approved request to the local Griffeye Operator
 - liaise with the Griffeye Operator to arrange a suitable time to utilise the program.

- Informants must complete user training in the categorisation process (in addition to the Interpol Baseline Classification online learning module) prior to using Griffeye. The Griffeye Operator is responsible for providing this training at the allocated site.
- The Griffeye Operator is only responsible for setting up and operating the Griffeye software; they are not responsible for completing the categorisation of the CAM.

Reports

At the conclusion of categorising the CAM, the Griffeye Operator will provide the informant with:

- a report for each device analysed containing a sample selection of relevant images or videos rated against each category of the ACACS (commonly referred to as a representative report). As this report contains CAM the following actions should be taken:
 - enter the report onto PALM to ensure continuity and compliance with legislation. For ease of management it should be entered under the same PALM entry as the offender's devices
 - store the report in accordance with section 4 of this policy.
- a report of the Categorised Image/Video Files which includes all CAM file paths, date and time stamps, metadata, and whether the file is deleted or not.

Copies of any images/videos/text must only be provided where the purpose is compliant with s. 51J of the *Crimes Act*.

Where electronic copies are provided, they must be contained on an encrypted storage device.

Uncategorised CAM

In the instance where Griffeye has confirmed the existence of uncategorised CAM on the device/s, the informant must categorise these images manually using the ACACS in accordance with the 1000/50 limit described below.

This process can be conducted at the Griffeye site if the applicable device can be accessed. Otherwise the informant should contact the Cybercrime Squad who will help to facilitate this process (refer to section 3.2).

1000/50 limit on categorisation conducted by an informant

- Once the Griffeye case has been created and the material is ready for the informant's categorisation, it is recommended the informant visually scan the files pre-categorised by Griffeye as Category 1 and 2 files, to ensure accuracy prior to any reports being generated. The informant should note the number of files that have been pre-categorised as illegal files by the Griffeye program.
- It is recommended the informant conducts a visual scan of all the files in the Griffeye case prior to commencing the categorisation process to establish the extent of the offending and breadth of depravity of the files.
- The informant should then categorise an additional 1000 illegal image files and 50 illegal video files (combination of Category 1 and 2).
- On some occasions a Griffeye case will contain less than 1000/50 un-categorised illegal content image and/or video files. On these occasions the entire content of the device must be categorised as the categorisation limit has not been met.
- **Example:** The total number of files ingested into the Griffeye case is 100,000.

Griffeye pre-categorises 4000 illegal image files and 400 illegal video files (i.e. known CAM images/videos). The investigator should categorise a further 1000 illegal image files (bringing the total number of categorised illegal images files to 5000) and a further 50 illegal video files (bringing the total number of categorised illegal video files to 450).

- The informant must ensure the categorised CAM image and video files is a fair and reasonable cross-section of all the illegal files in the possession of the accused, and not just the first CAM files identified by the informant.
- The investigator must ensure that each device associated with the Griffeye case contains at least one categorised illegal file. This allows for forfeiture of each device.

Possible contact offending

- If during the categorisation process it is identified that possible contact offending has occurred, the JACET Victim Identification Team (VIT) must be consulted for advice and assistance. It is strongly recommended that investigators categorise all files in instances where contact offending has been identified and this should only be commenced after consultation with a supervisor and approval by a Senior Sergeant or the Unit OIC.

3.2 The Cybercrime Squad

Process

Requests for analysis of CAM stored on a device must be submitted to the Cybercrime Squad by the informant:

- submitting the Request for Analysis online form (located on the Cybercrime Squad's intranet page) to their unit supervisor for approval. The granting of approval will automatically forward the request to the Cybercrime Squad; and
- including a list of all devices requiring analysis.

The informant will be notified when to attend the Cybercrime Squad to undertake a Managed Analysis of the devices to ensure continuity of evidence. The Managed Analysis process involves:

- informants completing user training in the categorisation process (in addition to the Interpol Baseline Classification online learning module) prior to commencing their work. This training will be provided by a Cybercrime Squad member at the allocated site
- a Cybercrime Squad member facilitating the categorisation process for the informant
- the informant categorising the CAM in accordance with the ACACS
- as Cybercrime Squad employees are not involved in CAM categorisation, they must not be included as witnesses on the brief of evidence.

Reports

Upon completion of the analysis a Cybercrime Squad employee will provide the informant with a number of reports. The informant will need to provide a storage device for the electronic reports. Dependent upon the type of evidence, scope of the investigation and number exhibits, the informant will be provided with:

- a single representative report produced across the Griffeye case

- a sample selection of relevant images or videos, as selected by the informant, rated against each category of the ACACS. As this report contains CAM the following actions must be taken:
 - enter the report onto PALM to ensure continuity and compliance with legislation. For ease of management, it should be entered under the same PALM entry as the offender's devices
 - store the report in a locked safe or cabinet in accordance with section 4.
- a Summary report, which includes a table outlining the ACACS categorisation of all files. This report does not include CAM and should be included on the brief as normal and remain on the brief upon filing
- a storage device which contains an electronic report of the informant's Categorised Image/Video Files report and include all CAM file paths, date and time stamps, metadata, and whether the file is deleted or not.

Electronic copies of any images/videos/text must only be provided where:

- it is necessary or appropriate to include electronic copies; and
- the purpose is compliant with s. 51J of the *Crimes Act*.

Where electronic copies are provided, they must be contained on an encrypted storage device.

4. Handling CAM

- Under certain circumstances Victoria Police members and VPS employees involved in the investigation of offences are permitted to handle CAM, as provide under section 51J(a) of the Crimes Act.
- In the normal course of their duties VPS property officers should not handle CAM. Where hard copies are required to be stored or retrieved, only members involved in the investigation may handle the CAM.
- When the informant receives the report containing the sample CAM, they must:
 - place the report in a sealed envelope
 - attach a 'WARNING' cover sheet to the front of the envelope
 - securely store the envelope at their workplace within a locked safe or cabinet in the property office or other location determined by the work unit manager. The safe or cabinet must not be able to be opened by unauthorised employees, including property officers.

5. Brief preparation

5.1 Brief of evidence

- The brief of evidence should be compiled in accordance with **VPMG Brief preparation and management**. The brief should also include:
 - the Summary report which includes the ACACS table
 - the Categorisation Image/Video Files report for each analysed device
 - a request for forfeiture order for all seized devices and any CAM generated as evidence to be destroyed [VP Form 745] for matters prosecuted by police prosecutors and the Office of Public Prosecutions (OPP). For Commonwealth matters, consult with the Commonwealth Director of Public Prosecutions (CDPP).

- The brief must not include the CAM images. The inclusion of the reports allows for the evidence to be assessed without having to view the images. The brief may include text-based CAM, contained in the summary of facts.
- For further guidance, refer to the CAM Practice Guide.

5.2 *Evidence required*

It is important the brief of evidence reflects the level of criminality of the offender.

The summary of charges and the informant's statement must clearly describe, in words, the level of criminality shown in the offender's collection of CAM. This will assist the court when assessing the sentencing options for the offences (especially where the CAM has not been viewed by the court).

To achieve this, the summary and the informant's statement should include, but not be limited to, the following information:

- whether actual children were used
- the nature and content, including age of the children and the gravity of the sexual activity portrayed and the distress levels of the children involved
- the extent of any cruelty or physical harm occasioned to the children
- the number of images or videos and number of children depicted (it's important to inform the court where possible, of the number of victims and not just the number of images – the exact number may not be able to be calculated however a general assessment should be made)
- the volume of videos, images and other CAM (stories, emails, chat logs, etc. should be considered) located on each device
- the amount of CAM images and videos located - total and in each category
- if known, how the material was obtained (purchased, peer to peer, grooming, manufactured etc. including the names of the application used to obtain and to view them on)
- duration of possession, access or downloading
- the offender's purpose for possession - for own use or for sale or dissemination
- the number of persons to whom the material was disseminated/transmitted
- whether any payment or material benefit was made, provided or received
- degree of planning, organising, skill or sophistication in acquiring, storing, disseminating or transmitting the material
- whether the offender acted alone or in a collaborative network or with like-minded persons
- any risk of the material being seen or acquired by vulnerable persons, particularly children
- any other matter unique to the case which court should have regard to when passing sentence.

It is important to be aware that the summary of charges cannot be used as evidence at court. This means the informant must include in their statement, all evidentiary

information contained in the summary, including production of exhibits such as the analysis report.

On occasion, the evidence contained in the informant's statement may be hearsay; this should remain in the statement so it can be adduced at court.

Informants should liaise with the OPP, CDPP or Serious Sexual Offence Unit at the earliest opportunity to help identify, and where necessary rectify, any issues.

6. Brief service

6.1 *Defence/accused*

- When the brief has been authorised it can be served on the accused or their legal counsel.
- The defence must not be provided with any printed or electronic copies of the CAM as they are not exempt under the *Crimes Act*.
- The informant or prosecutor may produce the printed reports containing the sample CAM for the defence counsel (not including the accused).
- Should a barrister or solicitor from the defence counsel request to view material the informant is to arrange a suitable time and place to provide that opportunity. Material must not be copied and it must be securely stored. The viewing must not be conducted using the seized items (accused's devices)

6.2 *Prosecutions agencies*

- After brief service, any produced representative reports will be retained by the investigator until requested by the courts or prosecution agency.

7. Finalisation and disposal

7.1 *Forfeiture*

- The brief should include a forfeiture order request (see section 5.1). An application should then be made to the Court for the destruction of the computers/storage devices/phones/discs/etc. used to store the CAM.
- Requests to return the device to the accused must not be granted as removal of all CAM content cannot be guaranteed. If an application is made, the matter should be adjourned and advice sought from the Cybercrime Squad.
- An application for forfeiture should also be made to destroy any CAM generated by Victoria Police as evidence for this matter (for example; sample booklets/discs generated by the Cybercrime Squad).

7.2 *Completion at court*

- Upon completion of the matter at court, the informant will be notified to collect, in person, the brief and sample CAM from the Prosecution Unit.
- The informant should then file the brief, including the Summary report with the ACACS table, in accordance with **VPMP Information review, retention and disposal** and the G500 Victoria Police Information Retention, Archiving and Destruction Handbook instructions.

- CAM must not be filed with the brief. Instead, it must be disposed of in accordance with section 7.3 of this policy.

7.3 *Disposal*

When a matter has been finalised all CAM and related reports (both seized from the offender and generated by Victoria Police for evidentiary purposes) must be destroyed as follows:

- hard copy CAM and related reports created by Victoria Police for evidentiary purposes – shredded in the presence of a senior sergeant with a notation made in the member's diary/day book and a notation attached to the brief/investigation file
- electronic CAM files stored on computer/hard drive/encrypted storage device by Victoria Police for evidentiary purposes – deleted in the presence of a senior sergeant with a notation made in the member's diary/day book
- the informant must advise the Cybercrime Squad that the matter has been completed at court to enable appropriate disposal of CAM data held at the Cybercrime Squad
- devices seized from offenders that have been granted forfeiture by the court – contact Central Property Management Unit to have the item disposed of correctly
- devices seized from offenders where consent to dispose has been given via a signed Notice of Abandonment – contact Central Property Management Unit to have the item disposed of correctly.

As it is impossible to guarantee that a device has successfully had all the CAM removed (may contain hidden or encrypted files), it is advisable to apply for the destruction of the offender's computers/hard drives/devices found to contain CAM, in accordance with a forfeiture order (see section 7.1) or Notice of Abandonment.

After the destruction of the Summary report and any device/s, then the Property portfolio manager or senior sergeant of the work unit can complete the PALM property entry.

7.4 *Disposal where a conviction was not made at court*

A disposal order can also be applied for when a conviction was not made at court. The order grants the destruction of either a seized item containing CAM, or of the CAM itself.

An application should be made when the seized item, or electronic matter contained in the seized item:

- was not the subject of a criminal proceeding; or
- was the subject of a criminal proceeding for a CAM offence and:
 - the charge was discontinued/withdrawn or permanently stayed; or
 - the person charged was acquitted or found not guilty; or
 - the charge was dismissed; or
 - the person charged was released on an undertaking under s.75 of the *Sentencing Act 1991*.

As it is impossible to guarantee a hard drive has successfully had all the CAM removed, an application should always be sought to have the seized item destroyed unless consent has been given via a signed Notice of Abandonment.

In the instance where this is not possible the application should seek approval to have all of the data wiped (including all user data, operating systems, installed programs).

The application should be made to the court by completing VP Form Notice of Application for Child Abuse Material Disposal Order [Form 1480].

When notifying an interested party of a Notice of Application for Child Abuse Material Disposal Order members should include a covering letter (located on the JACET intranet page). Members should consider:

- the welfare of the intended recipient by, where possible, making the notification in person
- whether personal service is appropriate in the circumstances to ensure sufficient notice.

8. Employee welfare

Due to the confronting nature of viewing CAM it is important that employees and supervisors are aware of the responsibilities and strategies that should be implemented and/or considered in order to avoid any adverse effects on employees' mental health and wellbeing.

Employees and supervisors who are working in a SOCIT or Family Violence Investigation Unit should seek the support of the Specialist Investigator Support Unit (SISU) at the commencement of the investigation.

8.1 *Responsibilities - investigators*

As part of the process of categorising CAM, the member must:

- view the CAM during business hours only and notify the supervisor of what work is being undertaken
- only conduct the categorisation process in a designated area, to ensure no unauthorised employees or visitors are able to view the content
- ensure that all material and storage mediums are securely stored during breaks and at the end of each day of the viewing process
- record all hours spent categorising CAM:
 - in their diary
 - on the appropriate safe-t-net entry
 - in the Oracle time attribution system.

8.2 *Responsibilities - supervisors*

When informed that a member will be categorising CAM during their shift, supervisors must:

- have a discussion with the member and come to an agreement of the scope of the viewing task (that is: what outcomes are being sought with respect to the investigation)
- consider implementation of any other appropriate welfare strategies.

Safe-t-net

The supervisor/manager is responsible for looking after and monitoring the mental health and wellbeing of the member. To assist with monitoring the wellbeing of members the supervisor/manager must record all exposure to CAM as an event on safe-

t-net. As part of this process the entry on safe-t-net should be completed by the member's supervisor/manager by:

- recording the entry against the respective member's name
- selecting 'CAM investigation' from the drop down subject field
- including in the free text field the amount of hours the member spent categorising the CAM (for the entire investigation).

The member's welfare should be managed using the safe-t-net entry in accordance with the processes detailed on the safe-t-net intranet page.

Refer to the safe-t-net intranet page for further information on the functions and principles of safe-t-net.

8.3 *Welfare for all employees*

If an employee feels adversely affected by their exposure to CAM investigations they should stop categorising immediately, notify their supervisor at the earliest opportunity, and seek assistance (see below) and/or employ wellbeing strategies (outlined at section 8.4).

Employees can seek support directly from the services provided by Health, Safety and Wellbeing. These services include:

- 24 hours, seven days a week wellbeing assistance on 1300 090 995
- the Employee Assistance Program provided via SMG health (1800 273 865) or Acacia Connection (1300 364 273)
- Police Psychology Unit – who offer support and advice on the management of mental health and counselling services
- Welfare Services – comprises of four specialist areas (chaplaincy, internal witness support, peer support and welfare) that support the physical and mental wellbeing of employees
- BlueSpace website – provides information on Victoria Police support services as well as other publicly available support services.

8.4 *Strategies*

There are a number of strategies that should be used to help promote and maintain an individual's mental health and wellbeing whilst categorising CAM. The strategies include:

- finishing the day with a different task not associated with CAM, to refocus the mind and disconnect from the categorisation task
- preparing mentally to avoid looking at the images from an emotional perspective, but rather to view the job as an analytical task, to progress the investigation
- avoiding working with material when tired, unwell or overwhelmed by other issues in life
- viewing the material in short periods of time (maximum of one hour) with breaks in-between
- limiting viewing material on any given day to no more than four hours

- being aware of any unexplained changes in behaviour or emotions and taking appropriate action (take a break, notify the supervisor, speak with a colleague, contact welfare services)
- working in an organised and systematic manner, so as to avoid seeing the material more than once
- turning the volume down or off if it is not required
- keeping the size of the image to the minimum required to complete the task
- playing music while completing the task
- participating in some form of exercise after viewing the CAM
- seeking out an appropriate person to talk with if the task becomes overwhelming
- monitoring reactions and mood over the following days and weeks and taking appropriate action if adversely affected.

For more strategies and ideas refer to Mental Health Information on the Police Psychology intranet page.

9. Offender welfare management

Members intending to interview a person in relation to allegations of sexual offences involving children and/or CAM need to be aware of the suspect's welfare. A person suspected of committing sexual offences involving children and/or CAM is considered to be at a heightened risk of suicide and self-harm.

When interviewing a suspect for CAM offences, the member must consider the suspect's welfare. Refer to **VPM Sexual offence investigations** for further information and strategies on interviewing suspects accused of child sex offending.

Prior to the suspect's release, members must provide a printed copy of the *Information and Support Referral brochure* to the suspect. A copy of the brochure must also be provided to any support person who the suspect has given permission for the member to contact.

If a child is identified as a victim of a sexual crime, either exploitation or a contact offence, refer to **VPM Sexual offence investigations**.

Related documents

- VPM Victim support
- VPM Sexual offence investigations
- VPM Management of people in police care or custody
- VPM Interviews and statements
- G500 Victoria Police Information Retention, Archiving and Destruction Handbook instructions
- Code of Practice for the Investigation of Sexual Crime
- Information and Support Referral Brochure
- Practice Note – Suspect Welfare Management

Further advice and information

For further advice and assistance regarding this policy, contact your supervisor, or the Officer in

Charge of the Joint Anti Child Exploitation Team (JACET).

Update history

DATE OF FIRST ISSUE	04/07/2016	FF-088455
DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
25/09/17	Removal of ambiguity relating to the classification of CAM and update to terminology and disposal process to reflect July 2017 legislative amendment. Also update to legislative reference for handling CAM.	FF-113779
21/10/19	Instrument names amended to reflect updated property management policies	FF-116667
10/02/20	Amended to allow electronic copies of material, clarify disposal processes and to reflect the change in classification system	FF-139241
22/3/21	Amended to reflect change in categorisation system to the Interpol Baseline, change from NetClean to Griffeye.	FF-148042
22/05/2025	Updated instrument names to reflect VPM Management of people in police care or custody.	FF-240370
08/12/2025	Updated to correct work unit names and other terminology.	FF-215409
11/12/2025	Updated to include limits on the number of CAM files requiring classification (1000/50 model) and other corrections or elaborations to processes.	FF-215409