

Victoria Police Manual

The Victoria Police Manual is issued under the authority of the Chief Commissioner of Police 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.

Information and records management

Context

The purpose of this policy is to uplift information management through consistent records management practices across Victoria Police.

Information including records, documents and data is generated at every stage of policing and Victoria Police employees have responsibilities around protection and access to information.

This policy includes:

- responsibilities of authorised users to collect and describe/name records in a meaningful way
- responsibilities of authorised users to protect Victoria Police information from inappropriate use, destruction, damage and unauthorised access
- guidance regarding minimum retention periods for different types of records
- responsibilities of authorised users regarding Force File creation and movement
- guidance regarding the storage of physical and digital records, disposal of physical records and archiving and
- specific guidance for the management of personnel records.

Contents

Context.....	1
Contents	1
Definitions.....	1
Scope and application.....	3
Responsibilities and procedures	3
1. Management and use of Victoria Police information.....	3
2. Management of specific records	5
3. Storage of Victoria Police information.....	6
4. Collection and access to personal information.....	7
5. Retention of records.....	8
6. Disposal of records	9
7. Compliance, monitoring and reporting.....	12
Related documents	12
Further advice and information	13
Update history	13

Definitions

Authorised user - a person who is authorised by Victoria Police to access:

- a corporate application and its information by the relevant System Owner (or their delegate) and/or

- information/records not stored in a corporate application, such as hardcopy documents or images, digital documents or audio/visual material whether stored on removable devices/media, personal drives or network drives by the relevant Information Owner (or their delegate).

Caretaker period - when an election has been called but a new government is yet to be confirmed.

Data - information that can be understood, analysed and reused to its full potential. Data can be incorporated into unique datasets saved in IT applications, databases or spreadsheets.

Destruction – the rendering of records as unreadable and irretrievable. The preferred process for destruction for Victoria Police information and information equipment or media is internal destruction.

Disposal - the process that determines if police records should be stored internally pending destruction at the end of information lifecycle, transferred to the Victoria Police Archive Services Centre (VPASC) (temporary records) or transferred to the Public Records Office Victoria (PROV) to be preserved as state archives (permanent records).

Duplicate information – limited to:

- working papers containing rough notes, calculations used solely to assist in the preparation of other records such as correspondence, reports and statistical tabulations
- drafts not intended for retention as part of the agency's records, the content of which has been reproduced and incorporated in the agency's recordkeeping system or
- extra copies of documents and published material kept solely for reference.

Inactive official information – information that is no longer being worked on or referred to for current activities.

Information asset – defined by the Office of the Victorian Information Commissioner (OVIC) as -

- a body of information, defined and practically managed so it can be understood, shared, protected and used to its full potential. Information assets support business processes and are stored across a variety of media and formats (i.e., both paper based as well as electronic material)
- having a recognisable and manageable value, risk, content and lifecycle
- being a specific report, a collection of reports, a database, information contained in a database, information about a specific function, subject or process.

Information asset register - an OVIC requirement to maintain a central list of IT systems and/or applications used to collect police information as digital assets such as data, documents, images and footage.

Information lifecycle - the period covering creation or receipt of information through to lawful disposal at the end of the cycle unless the records are deemed permanent by the PROV.

Non-records – limited to facilitative and/or transitory information that has no ongoing value to Victoria Police or the public, was not used to form the basis of a decision and does not record any decisions or work activities.

Original records - true and authentic information from a trusted primary source. Originals are hardcopy or digital but not both. **Public Records Office Victoria** – the archive of the state and local government in Victoria who issue standards regulating the creation, maintenance and security of public records, as well as maintaining and preserving public records.

RecFind - tracks the physical location of paper records (e.g., force files, investigation files, diaries and daybooks, Visual Audio Recorded Evidence (VARE Register), personnel files) and other artefacts.

Record owner – Officer in charge or equivalent, responsible for records that are unique to a specific business area, station or site regarding the creation, use and management of the records under their care.

Records - trusted information (e.g., from an approved IT system, government) created and/or used by Victoria Police in the course of doing business. All records are owned by Victoria Police whether they are physical or digital. Examples of records include documents, data, emails, official notes made in police diaries and notebooks (hardcopy and OneNote), force files, photographs, maps, images, footage and videos.

Retention and Disposal Authority – a Retention and Disposal Authority (RDA) is a mandatory standard for record keeping including the selection, retention and disposal periods of public records issued by PROV for all state and local governments.

Minimum retention period – the period of time a record (hardcopy and digital) must be retained by Victoria Police according to RDAs issued by the PROV.

Scope and application

This policy applies to all Victoria Police employees, Victoria Police approved third parties and Victoria Police contracted third parties.

Responsibilities and procedures

1. Management and use of Victoria Police information

Victoria Police's information management obligations come primarily from the *Public Records Act 1973*, supported by mandatory standards issued by the PROV. The standards apply to all Victoria Police information in accordance with the information lifecycle, including the preservation of records of continuing value (permanent). This includes from collection, recording, use, sharing and review, retention and destruction of information.

Employees and Victoria Police contracted and approved third parties must only access, use or disclose digital and/or hardcopy Victoria Police information where they have a demonstrable, legitimate business need directly related to the performance of their current duties with Victoria Police. Failure to act in accordance with this duty, breaches or violations of this policy may lead to management or disciplinary action or charges under sections 227, 228 and 229 of the *Victoria Police Act 2013*.

It is an offence under the *Crimes Act 1958* for individuals or organisations to destroy documents that they know are reasonably likely to be required in a future legal proceeding, with the intention of keeping the documents out of evidence. It is also an offence under the *Public Records Act* to unlawfully destroy a public record.

All authorised users:

- must manage Victoria Police information (regardless of media or format) appropriately throughout the entire information lifecycle
- should, where possible, create and manage information digitally (see section 2 of this policy for information management requirements in specified circumstances)
- must collect and manage all high-level business decisions, evidence and formal activities on physical files, where they cannot be managed digitally, (e.g., force files, personnel files, case files, briefs of evidence, issue cover sheets, briefing notes, official police diaries, daybooks and notebooks used for operational activities)

- must ensure that records are created and stored to enable retrieval in an acceptable timeframe and format
- must protect Victoria Police information from loss, unauthorised access, destruction and modification
- must describe records in a meaningful way and link related information where appropriate so that they can be found over a long period of time (seven – 100+ years) and include version numbers in the titles of physical and digital records where versions are not captured automatically - refer to the Information and Records Management Hub for further guidance and exceptions
- must not share, release or disclose information that is not related to the performance of their current duties or functions
- must only share information where it is justified through legislation, formal agreements or a genuine policing requirement and must occur through approved and/or legal avenues to ensure the information sharing is appropriate and legitimate. Refer to VPM Information security for further information regarding sharing information
- may share, release and disclose information externally, where appropriate, with Victoria Police partner groups and agencies.

Work unit managers must:

- ensure new personnel under their management are given adequate training in information management and their responsibilities under this policy
- ensure departing personnel are aware of their ongoing obligation not to disclose police information under the Victoria Police Act
- collect active and inactive official member diaries, daybooks, notebooks and physical files prior to separation
- register inactive official member diaries, daybooks, notebooks into RecFind (if not already registered) and transfer to VPASC
- prior to an authorised user's separation, ensure RecFind is updated for any force files currently held by authorised users who are leaving the organisation.

Divisional heads must ensure:

- all information is appropriately managed, transferred and/or archived during restructures, creation or shutdown of projects, taskforces or units
- that information has and is actively managed by an appropriate owner at all times. Where an owner is not specifically identified, ownership and responsibility is assigned to the department head
- appropriate business continuity strategies and plans are in place.
- All business continuity strategies and plans must specifically address information management (including records management) for all data and information systems managed by the Department. For further information about business continuity, refer to **VPM Business Continuity Management**.

2. Management of specific records

2.1 Force Files

All authorised users:

- must retain corporate hard copy records for high level/enterprise actions or decisions in physical Force Files to ensure consistent and transparent decision-making
- must ensure Force Files are complete with all relevant supporting documentation, comments and final decisions/approvals attached and folio numbered
- must describe Force Files in a meaningful way so they can be found easily by others who need access to active and inactive Force Files
- must update RecFind when transferring Force Files to other authorised users or business areas; this applies to authorised users who are relocating to another business area or are separating from Victoria Police
- must transfer inactive or completed Force Files to VPASC where they will remain until the end of the information lifecycle.

Refer to the Information and Records Management Hub for further guidance on:

- creating a Force File
- retrieving Force Files from the current owner/Action Officer
- searching for existing Force Files
- sharing/moving Force Files and updating locations in RecFind
- appropriate disposal processes.

2.2 Cabinet-in-Confidence records

Cabinet-in-Confidence records may be received or created and maintained by Victoria Police, including submissions, memos and correspondence passed to government departments and Ministers from Victoria Police.

Authorised users who create or receive Cabinet-in-Confidence records:

- must not delete or destroy the records
- must store the records in a secure location (e.g. on a network drive) or by agreement with the Security Information and Privacy Division (SIPD), Digital Services and Security Department (DSSD)
- where possible, should manage the records digitally.

If security breaches involving Cabinet-in-Confidence records occur, the Department of Premier and Cabinet may seek information from Victoria Police about the movement and audit trail of Cabinet-in-Confidence records. For this reason, the use of a Classified Document Register to track the movement of Cabinet-in-Confidence documents is encouraged.

For further information refer to the Victorian Government's Cabinet handbook. Further information relating to the Caretaker Period is also available on the Information and Records Management Hub and by contacting the Information and Records Management Unit, SIPD, DSSD via the INFORMATION-MANAGEMENT-MGR PBEA.

2.3 Social media

Social media posts are records when they contain evidence of official police business and are created or received by authorised users in the course of their duties.

Authorised users must treat the following as records:

- original posts on a social media site
- responses, if any are received, to the original post
- relevant posts identified when monitoring social media sites
- content republished by Victoria Police when the content has come from elsewhere.

Social media records are bound by the *Privacy and Data Protection Act 2014*. Refer to **VPM Information privacy** for further guidance on the Privacy Principles.

Refer to the **VPM Social media and online engagement** and **VPM Corporate communications** for further guidance on the appropriate use of social media.

3. Storage of Victoria Police information

All authorised users:

- are responsible for the information they create and store
- must store digital records in an official IT system or application (refer to Information Guide Where to Store Digital Police Records on the Information and Records Management Hub) or on a Victoria Police issued device. Refer to applications on the Victoria Police intranet homepage for a list of supported IT systems and applications
- if no IT approved system is available, must store information on a network drive (refer to Information Guide - Where to Store Digital Police Records on the Information and Records Management Hub) or an approved storage media device and
- must not store original records on non-IT approved systems and applications unless a Security Risk Assessment has been completed and approved by SIPD, DSSD.

For more information, refer to **VPM Information security**.

3.1 Physical documents

All authorised users:

- must transfer all physical files and documents that need to be retained for seven or more years to VPASC. Contact VPASC via the VPASC-ARCHIVE-SERVICES-MGR PBEA for exemptions that may apply. This practice should be undertaken at least annually to proactively manage storage capacity. Refer to the Information and Records Management Hub for further guidance on transferring and retrieving records stored at VPASC; refer to section 5 of this policy for guidance on document retention
- must take reasonable measures to protect records in their care from exposure to fire, floods, water leaks, pests or unauthorised access and
- must not store physical records in shipping containers or with:
 - chemicals and flammable materials
 - overhead pipes or plumbing
 - air conditioning units, machinery or plant equipment.

3.2 *Digital files and documents*

All authorised users:

- where possible, should create and manage information digitally to increase responsiveness and mobility to work remotely, strengthen innovation by working faster and smarter and reduce the cost of manual processes and storage of hard copy records.
- when storing information on electronic devices or media, must take reasonable measures to ensure the information is protected from loss, deterioration or damage.
- must save and store digital files and documents in a secure location. Refer to **VPM Information security** for further guidance.

4. Collection and access to personal information

All personal and health information held by Victoria Police, whether or not it is also in the public domain, must be managed in accordance with the Information Privacy and Health Information Privacy Principles contained within the *Privacy and Data Protection Act 2014* (PDPA) and *Health Records Act 2001* (HRA) respectively. Refer to **VPM Information privacy**.

Authorised users must also consider and act compatibly with human rights in their decisions and actions managing personal and health information, in accordance with the *Charter of Human Rights and Responsibilities Act 2006*. Refer to **VPM Human rights standards** for more information.

Authorised users must only collect and retain personal information when it is necessary for their functions or activities. Collecting personal and health information for another purpose may breach the PDPA and HRA.

Information and system owners must ensure that access to personnel information is limited to authorised users with a legitimate business reason to access the information to perform their duties.

4.1 *Personnel records*

Personnel records of all current and past employees are maintained in hard copy and digital files. These records contain personal and health information which must be collected, stored, used and disclosed in accordance with the PDPA and the HRA.

Access to personnel records is restricted to senior management, direct supervisors, employees' line managers, and administrative staff responsible for personnel/payroll functions, selection panel convenors and internal investigation or auditing areas. The Victoria Police Museum has access to service records relating to retired and deceased employees only.

All employees:

- must protect personnel records while in their care for legitimate organisational purposes and
- have a right to make a formal request in writing to Payroll Services to view and/or correct their own personal information via the following PBEA: PAYROLL SERVICES-MGR. The request, approval/rejection and any subsequent actions must be recorded. Employees can view their information in the presence of the responsible payroll practitioner once proof of identity has been established. Copies of personal information will be provided on request.

Upon receipt of a request to view a personnel file, the relevant payroll practitioner must undertake an information audit to remove references to any person other than the individual concerned.

Confidential information (e.g., complaints or investigations related to the *Equal Opportunity Act 2010*), internal investigations by Professional Standards Command, injury management and WorkCover claims must be kept separate from general personnel records. For further information refer to **VPM Complaints** and **VPM OHS Incident management** respectively.

Hard copy personnel records are held at the following locations:

- past employees – VPASC
- current employees – within Payroll Services.

Digital personnel records must be stored electronically on corporate systems, such as the human resources and financial systems. Digital records may also be held on Victoria Police networks. Wherever possible, general personnel records should be retained in the corporate human resources system. Personnel records are not to be held on portable computing devices without appropriate encryption and physical security controls. Refer to **VPMG Portable computing devices**.

For further guidance on privacy and health information refer to **VPM Information privacy**.

4.2 *Sharing information from personnel records with third parties*

Information from personnel records (including employment history, statements of earnings and leave records) can only be granted to third parties in accordance with the PDPA, HRA and **VPM Information security**.

5. Retention of records

Retention of information is based on the subject matter and whether records are considered temporary or permanent, rather than the format of the record (e.g. emails).

All authorised users must:

- apply the processes outlined in this policy and the Information and Records Management Hub to ensure information is retained until it can be disposed at the end of the record lifecycle
- regularly review Victoria Police information to ensure that it remains necessary for police activities and to determine retention or disposal actions
- retain Victoria Police information in accordance with the relevant legislation and must not dispose of information until it is reviewed and authorised in accordance with this policy; scanned copies can be deleted as duplicate information
- retain all records with retention periods of seven years or less in respective business areas or stations. This includes police diaries, daybooks and notebooks used to record operational activities. Contact VPASC via the VPASC-ARCHIVE-SERVICES-MGR PBEA for exemptions that may apply (i.e., station closure/refurbishment, lack of physical storage space).

5.1 *Retention and Disposal Authorities*

RDAs issued by the PROV outline the minimum retention period for all police information whether paper or digital. There is an alignment between Victoria Police Business Classification and Retention (BCR) tool and the RDAs. Wherever possible, Victoria Police

processes and systems should automate the application of the appropriate element of the Victoria Police BCR tool to information recording. This will reduce administrative and reassessment activities for determining the retention and disposal requirements for the information. Refer to the Information and Records Management Hub for guidance on the retention period of records.

All authorised users:

- are responsible for applying an appropriate protective security marking to all documents created or received from external sources (e.g., other agencies, law enforcement, business or community groups). Refer to **VPM Information Security** for further information.
- must adhere to the minimum retention periods outlined in the RDAs. Refer to the Information and Records Management Hub for a complete list of RDAs applicable to Victoria Police
- must include the version number in the title of physical and digital records excluding documents stored in SharePoint as the version is captured automatically; for further guidance refer to the Information and Records Management Hub

Refer to the Information and Records Management Hub for how to manage and use records through all stages of the information lifecycle.

Refer to the Victoria Police BCR tool on the Information and Records Management Hub for a full list of corporate and operational records held by Victoria Police and their minimum retention periods.

6. Disposal of records

All employees should periodically review the hardcopy and digital records under their control to identify and properly dispose of duplicate information and non-records.

Duplicate information and non-records can be destroyed, using a destruction process appropriate to the media and protective marking of the material, without authorisation as part of normal administrative practice (i.e., reasonable business practices). This includes:

- working documents, such as notes or calculations, used to assist in the preparation of other records
- minor drafts and similar temporary documents, where the content is reproduced elsewhere and the information will not be needed to show how the work has progressed or actions approved
- minor updates of content, such as those in databases, which will not be needed to show actions, decisions or approvals
- communications for the purpose of making minor arrangements
- duplicate copies
- periodic backups of records, information, data, software and settings for recovery in case of technical failure and/or catastrophe and are duplicate copies of official business records/data that is held elsewhere on a managed system.

If there is doubt whether information can be destroyed as part of normal administrative practice, contact VPASC for advice.

Employees must seek approval to dispose of Victoria Police files and documents, which are not able to be destroyed as part of normal administrative practice. Only record owners can seek approval to dispose of original digital files and documents. To dispose of police information, the

record owner must request approval from the Information and Records Management Unit, SIPD, DSSD.

For assistance to transfer physical files earlier than seven years due to space restrictions, safety reasons, permanent shut down of station/site, scheduled refurbishment or other situation, contact VPASC.

Refer to the Information and Records Management Hub for further guidance on the disposal process for Victoria Police files and documents.

6.1 *Destruction process*

The destruction process includes:

- identifying duplicate information, non-records or inactive official information
- assessing information/equipment
- authorising destruction
- identifying suitable destruction method (contact SIPD for advice)
- destroying information
- recording, verifying and reconciling records destruction.

6.2 *Identifying inactive official information*

Work unit managers must ensure that:

- official information determined to be inactive is transferred from the workplace through regular reviews
- local procedures require all inactive hardcopy information to be either:
 - transferred to VPASC for retention
 - identified for potential destruction.
- local procedures require inactive digital information on shared drives, any removable media or personal directories to be either:
 - transferred to DVD (or other suitable archival storage media under advice from Protective Security) and sent to the VPASC for retention
 - printed and incorporated into a hardcopy filing system
 - identified for potential destruction.

6.3 *Criteria for destruction*

Prior to seeking approval for the destruction of Victoria Police information, work unit managers must confirm that the information meets all of the following criteria:

- it is covered by a current RDA
- it is not a permanent record under the RDA (refer to the Information and Records Management Hub)
- the minimum timeframe for retention under the RDA has elapsed
- it is unlikely to be required as evidence in any future court proceedings
- it is unlikely to be requested under Freedom of Information (FOI)

- it does not have any historic significance to Victoria Police or the greater Victorian community (contact VPASC for advice).

6.4 Destruction

Employees who identify hardcopy records as meeting the criteria for destruction, must complete and submit a Record Destruction Request [VP Form 1455] (available from the Information and Records Management Hub) to their work unit manager.

- If the work unit manager supports the application, the form must be emailed to VPASC via VPASC-ARCHIVE-SERVICES-MGR@police.vic.gov.au. From here an assessment will be made (e.g. granted or not granted in accordance with legislation and business need)
- The only Victoria Police information excluded from the requirement to seek authorisation are:
 - duplicate information and non-records
 - records obtained under s.26 to s.29, *Sex offenders Registration Act 2004* – See **VPM Registered sex offender management**
 - forensic samples taken and any related material and information addressed by s.464ZG(3), *Crimes Act 1958* – See **VPM Forensic procedures**, or
 - protected information as defined under s.30D, *Surveillance Devices Act 1999*, restricted records and stored communications as defined under s.5, *Telecommunications (Interception and Access) Act 1979* (Cth); see **VPMP Investigation support**.
- Despite the above records/information being excluded from requiring destruction authorisation, this material still needs to comply with disposal requirements commensurate with the handling requirements of the material.

Once the Form 1455 has been completed and submitted, employees must ensure information is:

- stored in containers (pending destruction) that meets the security requirements appropriate to the security classification level of the information
- transferred (prior to destruction) in a manner that is compliant with security safeguards relating to the security classification of the information
- destroyed within a week of the authorisation
- verified and reconciled as destroyed by VPASC through submission of the destruction certificate.

Employees working offsite must ensure that all Victoria Police information is returned to Victoria Police premises for destruction.

Work unit managers are responsible for:

- arranging a transfer request with VPASC for any inactive official information (either digital or hardcopy) that is a permanent or long-term record (retained for more than seven years) under the RDAs – transfer requests must include appropriate storage and handling and can include restrictions on access or notification/approval of requests for access to records where justified
- ensuring the destruction process is completed and authorised and
- ensuring the destruction process meets the minimum requirements for non-public domain or classified material and the type of medium holding the information.

For further information about the methods of destruction, refer to **VPM Information and information equipment disposal**.

6.5 *Recording destruction*

Destruction of all records must be documented so that Victoria Police is able to provide evidence of when and how destruction took place. This requirement applies equally to all records regardless of format (i.e., digital records or paper records). Proof of destruction may be required in litigation proceedings, in response to FOI requests or as requested from the PROV.

Work unit managers must ensure that on completion of destruction:

- a disposal certification is:
 - completed and signed
 - attached to the approved application for destruction
 - returned to VPASC or retained on an official file.
- appropriate registers are updated to reflect the destruction. This could include the Classified Document Register or correspondence registers.

6.6 *Failure in handling or destruction requirements*

In the event of damage to police files or documents (minor or major), contact the Information and Records Management Unit as soon as practicable.

The accidental or deliberate failure to observe requirements around the handling and destruction of official resources (including Victoria Police information) is a security incident. Accordingly, failure to adhere to the requirements of this policy must be reported to the Security Incident Registry.

Refer to **VPM Security incident management** for more information on the categories of security incidents, as well as reporting procedures.

If destroyed or damaged information is requested (e.g., through FOI or legal proceedings) employees must be able to provide a copy of the VPASC record of the unplanned damage or destruction to the requestor.

7. Compliance, monitoring and reporting

- Where appropriate, audits and reviews of Victoria Police functions and activities should include an assessment of compliance with the information management and information security policies and guidelines.
- Work unit managers must include compliance with information management and information security policies as part of their workplace inspections. Refer to **VPM Information security** for guidance on specific requirements for inspections.

Related documents

- Public Record Office Victoria Standards
- VPM Information security
- VPM Information privacy
- Victoria Police Business Classification and Retention Tool

Further advice and information

For further advice and assistance regarding this policy, contact the Information and Records Management Unit, SIPD, DSSD via the INFORMATION-MANAGEMENT-MGR PBEA.

Update history

DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
28/01/2026	New policy to consolidate and replace VPM Information categorisation, collection and recording, VPMP Appropriate use of information, VPMP Information use, handling and storage, VPMP Information review, retention and disposal, VPMP Information management and information security framework, VPMP Information management and information security roles, VPMG Information and information equipment disposal, VPMG Personnel records, Information management and information security organisational policy statement.	FF-215906