Public information release

Source Policy

These Procedures and Guidelines support and must be read in conjunction with the following:

- VPMP Information sharing

Application

Procedures and Guidelines are provided to support the interpretation and application of rules and responsibilities. They include recommended good practices and assessment tools to help employees make lawful, ethical and professional decisions. Employees should use the **Professional and ethical standards** to inform the decisions they make to support interpretation of Procedures and Guidelines.

Procedures and Guidelines are not mandatory requirements on their own. However, where rules and responsibilities state that employees must have regard to Procedures and Guidelines, the Procedures and Guidelines must be used to help make decisions in support of the rules.

Procedures and Guidelines

1. Overview

In accordance with **VPMP Information sharing**, Victoria Police will identify and release 'public information' into the public domain. 'Public information' includes documents and datasets identified for release:

- To inform and reassure the public about the integrity and performance of Victoria Police's practices and systems.
- To comply with the Victorian Government's DataVic Access Policy (DVAP), which enables the use of Victorian Government data by the public in order to:
  - support research and education
  - promote innovation
  - support improvements in productivity
  - stimulate growth in the Victorian economy.

- The DVAP supports open and accountable government by allowing the public access to Victorian Government information so that it can be used and reused by the community and businesses.

- Unclassified and non-personal information should be considered for release unless access is restricted for reasons of privacy, public safety, security and law enforcement, public health, and compliance with the law.

- Data release in accordance with DVAP is to be in line with DVAP mandatory standards. Compliance with this guideline and the associated processes will ensure that data release is in accordance with the DVAP standards.

2. Responsibilities

2.1 Public Information Sub Committee

- The Public Information Sub Committee (PISC) is responsible for the development and monitoring of the public information release process. The PISC reports to the Information Management Committee (IMC) on public information release, including DVAP issues.

- The PISC is chaired Protective Security and includes representatives from various Departments and Commands. It meets as required, at a minimum annually.

2.2 Information Management Committee

The IMC is responsible for public information release and the implementation of DVAP within Victoria Police on behalf of the Chief Commissioner. The Chief Commissioner has overall accountability for implementation of DVAP within Victoria Police.

2.3 Media and Corporate Communications Department

Media and Corporate Communications Department (MCCD) is responsible for:

- final approval of the release of public information (in line with **VPMP Information sharing**)

- providing appropriate notifications prior to publication

- creating and maintaining data records on the DataVic website

- publishing data on Victoria Police internet site(s) (excluding those directly published by Corporate Statistics)

- external management of suggestions received through DataVic website

- updating the online DVAP suggestion register to record outcomes

- moderating and managing the treatment of online feedback on public information.

2.4 Protective Security

Protective Security is responsible for:

- management of DVAP requirements on behalf of Victoria Police
- internal management of suggestions for public information release (including suggestions received through DataVic)
- management of the PISC
- maintenance of the public information register and information asset register.

2.5 Information Owner

- The Information Owner for public information is the relevant Department Head responsible for the information, document or data. An Information Owner may also hold the position of System Owner (the person responsible for data in a corporate application) or Accountable Officer (the person responsible for policy instruments and other documents in a specific subject area).
- Information Owners have overall responsibility for any documents or data that are publicly released in accordance with these procedures.

2.6 Information Manager

Information Owners may delegate authority to an Information Manager, who is responsible for:

- developing, documenting and maintaining the process for obtaining and preparing the public information
- obtaining and preparing the dataset or document in line with the documented process
- ensuring that all appropriate approvals are obtained in sufficient time to allow publication of the dataset within the nominated timeframe.

3. Identification and approval

3.1 Identification of potential public information

- Information Owners are to identify information that may fit the criteria for public release in section 1. If they believe information should be considered

by PISC for release, they should advise Protective Security Enterprise Information.

- Information proposed for release under DVAP is to be able to be produced periodically within existing resources. Information Owners can nominate an appropriate period between updates.

- PISC will consider suggestions from Information Owners. It will also consider publicly releasing information that is commonly requested through the Freedom of Information Office, Corporate Statistics and DVAP to identify potential additions to the Victoria Police public information catalogue.

- Identification of additional information and datasets for public release will occur periodically as considered appropriate by PISC members, but not less than annually.

3.2 Assessment of information

- PISC and the Information Owners are required to undertake a formal assessment of the information proposed to be published as public information. This assessment will identify if the information or dataset meets the criteria for release.

- Advice and approval from the Manager of Corporate Statistics is to be sought for any information that is to be obtained from the following systems or datasets:

  - Crime Statistics and Reporting System (CSRS)
  - Member Activity Sheet (MAS)
  - Computer Aided Dispatch (CAD)
  - Collision Management and Information System (CMIS)
  - Fixed Penalty Payment System (FPPO)
  - Use of Force data
  - Vehicle Impoundment data
  - NSCSP Survey data.

- The assessment is to be conducted and recorded using the appropriate checklist available from the Protective Security intranet site:

  - C110 DVAP assessment checklist
  - C120 Public Information assessment checklist.

3.3 Recording of information datasets

- Protective Security is responsible for the maintenance of an Information Asset Register (IAR) in accordance with the Whole of Victorian Government Standards.

- All datasets proposed for release under DVAP are to be recorded on the IAR. The IAR will record the details of the information including release dates under DVAP.

- Information Owners can ensure their information is recorded on the IAR by contacting Protective Security Enterprise Information.

3.4 Recording of public information

- Protective Security is responsible for the maintenance of a public information register to ensure appropriate publishing, review and removal of public information.

- Each published dataset or document will be recorded on this register for review by PISC at each meeting.

4. Preparation of information

4.1 DVAP information – dataset preparation and format

- As DVAP requires information to be periodically released, the process for obtaining and preparing a dataset requires documenting.

- A copy of this process is to be provided to Protective Security for the IAR. This process is not to be released to ensure any aggregated or de-identified data released using this process is not able to reconstructed.

- DVAP requires information to be released in a machine-readable, reusable and open format such as comma separated values (CSV) or an extensible mark up language (XML).

- If information is not to be published in an open format the justification should be documented in the dataset assessment.

4.2 Non-DVAP public information

- Documents that are assessed as suitable for public release but are not datasets (such as policy documents or evaluation reports) are to be in an internet readable format, preferably PDF.

- Non-DVAP public information is to have an expiry timeframe when the information will be removed from the internet site.

4.3 Aggregation and de-identification

- Information that may enable identification of an individual or business is to be aggregated and/or de-identified. This is essential for information that contains personal or health information (Refer to **VPMG Information privacy**).

- Advice on aggregation and de-identification should be sought from Corporate Statistics.

- If the information is to be aggregated and de-identified prior to release, the documented process is to include the procedure for the aggregation and/or de-identification of the information. This procedure is to be tested and consistently applied by the Information Manager.

4.4 Data statements

- In order to avoid datasets being misrepresented or misused, the Information Manager should prepare a data quality statement for each dataset to be released. Assistance can be sought from Corporate Statistics.

- A data quality statement can be prepared using the National Statistical Service online data tool (www.nss.gov.au/dataquality).

- The Information Manager is required to produce a metadata information set for inclusion on the DataVic site for data released under DVAP.

- The metadata set template is available from the Protective Security intranet site (see links to the right).

4.5 DVAP information – Licensing

- The default licence for information released under DVAP is *Creative Commons Attribution (CC BY)*. This license allows the public (including commercial and non-commercial entities) to copy, adapt or modify, distribute and license their resulting work to others.

- Advice is to be sought from Protective Security Enterprise Information if the use of the released information is to be restricted. If justified, information released under DVAP can be restricted so that users:
  - may not use the information for commercial purposes
  - may not alter, transform, or build upon the information
  - may only license work using the same license conditions.
- If a restrictive copyright is to be applied, the information is unlikely to be suitable for release under DVAP. Advice from Legal Services should be obtained on copyright restrictions applied to publically available information.

5. Approval and publication

5.1 Approval prior to publication

- Approval for publication is to be obtained prior to the release or update of public information.

- Final approval for publication is to be obtained from the Director of Media & Corporate Communications Department (MCCD) in accordance with **VPMP Information sharing**. When seeking this approval the following information is required:
  - the approved information assessment
  - the completed data quality statement (if applicable)
  - the metadata information set (if applicable)
  - reason for a non standard license (if applicable)
  - details of any changes in the collection or preparation process since last publication, and the affect this may have had on the information (if applicable).

5.2 Notification prior to publication

- Once approval has been given to release a document, the Freedom of Information office and MCCD will determine the relevant notification requirements. MCCD will notify the relevant Executive Command member(s).

- If appropriate, the Office of the Chief Commissioner will notify the Department of Justice and/or the Minister prior to publication.

- Publication cannot occur until appropriate notifications have been made.

5.3 Publication of datasets

- Information released under DVAP is to be hosted on a Victoria Police internet site and linked to a record in the DVAP internet site.

- Sites hosting Victoria Police information released under DVAP are to have appropriate terms and conditions of use to manage legal compliance risks in accordance with the Victorian Government Intellectual Property Policy.

- Once approved for publication, MCCD is to:
  - upload the information to an appropriate Victoria Police internet site
  - embed the appropriate licence (creativecommons.org/choose)
  - create/update the data record on the DataVic internet site.

5.4 Notification of relevant stakeholders

Following publication, the Information Owner is responsible for arranging the notification of relevant stakeholders (including Victoria Police employees). MCCD is to provide advice and assistance.

Further Advice and Information

For further advice and assistance regarding these Policy Procedures and Guidelines, contact Protective Security.

Update history

Date of first issue	15/10/13	
Date updated	**Summary of change**	**Force File number**
25/03/19	Administrative amendments to reflect name change from IMSSD to Protective Security.	FF-139207