

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.

VPM Facial recognition technology

Context

Facial recognition technology is a tool that processes facial biometrics to help identify individuals. It has many uses and can be deployed for a variety of law enforcement purposes. Different forms of facial recognition technology can give rise to different legal and human rights considerations and obligations.

Policy at a glance

This policy includes:

- the legal framework, including human rights and privacy considerations, applicable to the use of facial recognition technology
- permitted purposes of facial recognition technology use
- facial recognition technology use that requires approval
- the approval process for applications to use facial recognition technology, including in a pilot or trial.

Contents

Context	1
Policy at a glance	1
Contents	1
Definitions	1
Scope and application	2
Responsibilities and procedures	2
1. Legal framework	2
2. Use of facial recognition technology	3
3. Approval to use facial recognition technology	4
Related documents	5
Further advice and information	5
Update history	5

Definitions

Attendance identity verification: a category of retrospective facial recognition used to assist with the accurate identification of a person in police custody and to identify whether any LEAP warning flags apply to the person.

Biometric: a measurement or physical characteristic that may be used to identify an individual. Biometric information is personal information.

Facial recognition technology: facial recognition technology processes facial biometric information to identify individuals. It takes a variety of forms (i.e., live, operator-initiated and retrospective).

Live facial recognition technology: a category of facial recognition that compares a live camera feed of faces against a reference list to find a match.

Operator-initiated facial recognition technology: a category of retrospective facial recognition where a member in the field captures a photo of an individual and simultaneously uses a facial recognition tool to process the biometric data captured by the photograph to identify the person.

Retrospective facial recognition technology: a category of facial recognition technology that involves two steps. The first step is the collection, not necessarily for the purpose of facial recognition, of images and/or dynamic video (i.e., from mobile phone, CCTV etc.) which includes the face of an unknown person. The second step is the use of facial recognition technology to compare the images or video clips against relevant police data holdings (e.g. custody photographs held on LEAP).

Reviewer: police performing duties in a specialist role within the Criminal Identification Unit (CIU), Forensic Services Department (FSD), who perform specialised facial recognition and facial comparison tasks using local enterprise access and national systems for intelligence or investigative purposes.

Also refer to the general **VPM Dictionary** for definitions and acronyms.

Scope and application

This VPM applies to all Victoria Police employees.

Responsibilities and procedures

1. Legal framework

1.1 *Applicable law*

Facial recognition technology is a form of biometric surveillance and is governed by a range of legal frameworks and obligations that apply to Victoria Police. This includes the *Charter of Human Rights and Responsibilities Act 2006* (the Charter) and the *Privacy and Data Protection Act 2014* (PDP Act).

Any use or proposed use of facial recognition technology by Victoria Police must be legally compliant. As facial recognition is an emerging technology, any use of facial recognition technology that requires approval must be accompanied by legal advice that assesses the lawfulness of the proposed use as part of the approval process outlined in section 3 of this policy.

1.2 *Charter of Human Rights and Responsibilities Act 2006*

Victoria Police is bound by the legal obligation on public authorities in s.38 of the Charter. This requires that all decisions and actions (including the use or proposed use of any form of facial recognition technology) properly consider and act compatibly with the protected human rights in the Charter.

Human rights relevant to the use of facial recognition technology by police include s.8 (recognition and equality before the law – which protects individuals from discrimination); s.12 (freedom of movement); s.13 (privacy and reputation); s.16 (freedom of association and peaceful assembly); s.17 (protection of families and children); s.18 (participation in public life); s.19 (cultural rights) and s.21 (liberty and security of person).

The efficacy of any proposed facial recognition technology must be scrutinised prior to piloting/adoption/use, as certain tools have been shown in other jurisdictions to be ineffective in accurately identifying certain ethnicities and gender identities. This can result in biased and discriminatory deployments of the technology.

1.3 *Privacy and Data Protection Act 2014*

Victoria Police is bound by the legal requirements set out in the PDP Act relating to the processing of sensitive personal information, including the processing of facial biometrics using facial recognition technology.

Any use of facial recognition technology must be fully compliant with the PDP Act, including relevant Information Privacy Principles (IPPs). This includes the requirement that sensitive personal information collected and processed as part of the facial recognition process is only used and disclosed for legitimate purposes (IPP 2) and only for the primary purpose for which it was collected (unless an exemption applies – IPP 2).

Data quality must also be accurate (IPP3 – Data Quality), which will likely be most relevant when creating reference lists or facial biometric datasets against which the facial recognition system will search for any positive matches. Further information regarding the application of the PDP Act to facial recognition technology can be found on the website of the Office of the Victorian Information Commissioner.

Victoria Police employees must ensure that:

- the collection of facial biometrics is necessary for policing functions or activities
- the collection of facial biometrics is lawful and is not done in an unreasonably intrusive way
- the use or disclosure of facial biometrics is required or authorised by or under law.

2. Use of facial recognition technology

Employees must only use facial recognition technology to inform and enhance decision making, rather than to independently make decisions or determine outcomes. Refer to the Victoria Police Artificial Intelligence Ethics Framework for further information regarding ethical guidelines for the use of artificial intelligence products within Victoria Police.

Facial recognition technology may be used to help police establish who a person is or whether their image matches against other images held by Victoria Police, for policing purposes.

2.1 *Permitted use*

Permitted uses of facial recognition technology (e.g. the use of iFace for attendance identity verification) are those listed on the Digital Services and Security Department (DSSD)- Artificial Intelligence Tools register. The register can be found on the DSSD intranet page.

2.2 *Permitted purposes*

Permitted purposes of facial recognition technology are:

- to aid investigations by providing an investigatory lead as to the potential identity of an unknown person of interest, victim or witness
- confirming where a person of interest appears within a set of imagery held by Victoria Police
- for attendance identify verification.

The CIU, FSD can provide information, support and advice regarding facial identification. Contact the CIU, FSD for further support.

3. Approval to use facial recognition technology

3.1 *Facial recognition use that requires approval*

Facial recognition technology that does not appear on the Artificial Intelligence Tools register requires approval to use. Once an AI tool is approved for use, it is added to the register.

Employees seeking to use, including as part of a pilot or trial:

- retrospective facial recognition technology (other than operator-initiated)
- any form of operator-initiated facial recognition technology

must first seek approval to do so, via their chain of command, from their respective Assistant Commissioner/Executive Director.

Employees seeking to deploy:

- live facial recognition technology, including as part of a pilot or trial

must first seek approval to do so, via their chain of command, from their respective Deputy Commissioner/Deputy Secretary.

All applications to use these types of facial recognition technology must be supported by information described at section 3.3 of this policy. For further information about the application process, refer also to the **Facial recognition technology Practice Guide**.

3.2 *Further considerations applicable to use of facial recognition technology*

Some facial recognition technology use may present greater risk when deployed in operational contexts. This includes covert deployments and uses involving identification of individuals in the context of counter terrorism and serious and organised crime. In these circumstances, approval to pilot or use facial recognition technology may require a deployment model that includes a qualified reviewer to assist with the accurate identification of a person. Prior to seeking approval of the proposed use, advice should be obtained from the CIU, FSD, on whether a qualified reviewer is required.

3.3 *Content of applications*

Applications to use facial recognition technology must be made using the Request to Use Artificial Intelligence Products form available on the DSSD intranet page.

Applications for facial recognition technology use must address:

- the operational need for use of the facial recognition technology
- potential legal, security and other risks and mitigations, where applicable
- human rights and privacy impacts (see section 3.4 of this policy)
- confirmation from CIU, FSD as to whether a qualified reviewer is required for deployment of the facial recognition technology.

Applications will be provided by DSSD to the AI Ethics Committee (AIEC) for consideration.

3.4 *Guidance for addressing human rights impacts*

Applications must include an assessment of the human rights impacts of the proposed use to ensure efficacy and guard against potential biased and discriminatory deployments of the technology. The assessment must include all of the following:

- the lawful basis for the proposed use of facial recognition technology
- whether and in what way any human rights may be limited (adversely impacted) by the proposed use of facial recognition technology
- whether the proposed use of facial recognition technology is demonstrably justified, having considered each of the thresholds outlined in s.7(2) of the Charter (proportionality framework) (refer to **VPM Human rights standards**).

Applications for a proposed new use of facial recognition technology must also be accompanied by legal advice that assesses the lawfulness of the proposed use, considering facial recognition is an emerging technology.

Related documents

- Victoria Police Artificial Intelligence Ethics Framework
- VPMP Appropriate use of information
- VPMP Information access
- VPMG Information system access
- VPMG Identifying offenders
- VPMG Portable computing devices
- VPMG Portable recording devices
- CCI 08/23 – Restrictions on the use of applications on Victoria Police devices
- CCI 10/17 Mobile Device Deployment

Further advice and information

For further advice and assistance regarding this policy, contact the Manager, Strategy & Policy, DSSD via the STAFF_OFFICER_CDO-DSSD-MGR PBEA.

Update history

DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
19/08/2024	First issue.	FF- 261980
22/10/2025	Amended with minor clarifications and to add references to supporting material.	FF-233436