Western Australia Police Force

Privacy Impact Assessment

OVERT LIVE FACIAL RECOGNITION

Technology Portfolio

Innovation

November 2025

OVERVIEW

Business Owner	Technology Portfolio, Innovation
Responsible Officer	Superintendent Steve Thompson PD11042
Executive Sponsor	Commander Dario Bolzonella PD08430
Title	Overt Live Facial Recognition (OLFR)
Lifecycle Stage	Trial proposal
Vendor	NEC
Overview	OLFR is a real-time facial recognition technology that compares live camera feeds against alert lists to identify individuals of interest to police. It supports proactive policing, enhances operational efficiency, and improves public safety. The proposed trial draws on UK policing models, principally from the Metropolitan Police Service.
Purpose	To assess the feasibility and effectiveness of OLFR in identifying high-risk individuals and support strategic policing objectives in Western Australia.
Objective	• Improve identification and location of individuals wanted for arrest or subject to legal restrictions • Enhance public safety and operational efficiency • Reduce reliance on manual and reactive methods
Is this replacing or improving an existing system or process?	OLFR will improve and supplement existing policing and intelligence methods. OLFR offers a scalable and timely alternative to traditional approaches.
Agency Benefits	Potential Agency benefits include: • Real-time alerts and rapid identification • Improved enforcement and prevention capabilities • Enhanced event security and offender management • Efficient resource use and cross-district reach
Community Benefits	Potential Community benefits include: • Increased public safety and confidence • Faster location of vulnerable individuals • Transparent and respectful engagement protocols • Reduced risk of harm from high-risk individuals

Consultation	**How individuals have been informed, consulted and consent provided:** For the OLFR trial, consultation occurred primarily through stakeholder engagement and governance processes. The UK model emphasises transparency measures such as public signage during deployments and engagement with community groups. WA Police Force has adopted similar practices, which include impact assessments and stakeholder briefings prior to deployment. **Public availability of scope and objectives:** The scope and objectives of the OLFR project are documented internally and are expected to be made publicly available through WA Police Force transparency measures, such as recording and reporting of deployment locations, public notifications and signage, once the trial progresses beyond initial planning. **Formal processes for appeal or withdrawal:** As OLFR operates in public spaces for law enforcement purposes, individuals cannot opt out of being captured by CCTV if they decide to walk through the OLFR zone. Governance frameworks include complaint and review mechanisms for individuals who believe they have been adversely affected, consistent with WA Police Force accountability processes.
Authorised Users	Authorised users include trained WA Police Force personnel responsible for OLFR operations: • OLFR operators monitor live feeds • Engagement officers adjudicating alerts • Supervisor oversight of deployments • Technical staff managing system configuration and data governance
Training Requirements	All authorised users undergo training before participating in OLFR deployments. Training focus is on cover: • System functionality and alert adjudication • Privacy and security obligations under the *Privacy and Responsible Information Sharing Act 2024* (*PRIS Act 2024*) and WA Police Force policies • Ethical use of AI and bias mitigation • Operational protocols for lawful and proportionate engagement

DATA AND INFORMATION

Information and Data Usage

Type State specific information being used (i.e., images, statistics)	Source State where information is being sourced (i.e., IMS, individuals)	Category Select appropriate category from *PRIS Act 2024* from drop-down list.	Classification Select appropriate classification label from drop-down list.
Biometric templates (facial recognition)	In situ from CCTV footage within the "Zone of Recognition"	Sensitive Personal	PROTECTED
CCTV footage	Live CCTV camera feeds	Personal	OFFICIAL: Sensitive
Alert list images	Police database (IMS)	Sensitive Personal	OFFICIAL: Sensitive

Aboriginal Information

Will any information to be disclosed include **sensitive Aboriginal family history** or **sensitive Aboriginal traditional information**?	No
Will the activity under the agreement primarily or especially affect Aboriginal people?	No
If this assessment is for an Information Sharing Agreement AND any of the above answers are YES you will need to additionally complete an Aboriginal Information Assessment.	

Security and Purpose

Information Security	All information collected and processed through OLFR is handled in strict accordance with WA Police Force information security policies, privacy frameworks, and applicable legislation, including the *PRIS Act 2024*. Appropriate safeguards, retention protocols, and access controls are applied to ensure lawful, proportionate, and secure management of personal and sensitive data. Additional parameters adopted by WA Police Force includes: • Biometric data encrypted and deleted immediately if not a match (non-matched biometrics not retained) • Encrypted alert lists • Data stored in Australia • Agency's existing Security Framework
Permitted Purpose	The information collected and processed through OLFR is used exclusively for lawful policing and public safety objectives. OLFR's purpose is to assist law enforcement functions by identifying and locating individuals wanted for arrest, subject to court orders, or posing risks to community safety. OLFR also enhances community policing by enabling proactive deployments in crime hotspots and public events to prevent harm and maintain public confidence.

AI AND AUTOMATED DECISION MAKING

Does the project or activity involve an AI Function or automated decision-making process?	Yes
If the project or activity does contain an AI function or automated decision-making process, please answer the following questions and complete the AI Assurance Framework Assessment. **If the project or activity does not contain an AI function or automated decision-making process, the following questions in this section and the AI Assurance Framework Assessment are not required to be completed.**	
Software	Facial Recognition Software. Current engagement with NEC is ongoing. If endorsed the technology will be the NEC's NeoFace Watch technology using the NeoFace M40 algorithm. This algorithm is used by the Metropolitan Police in an operational policing environment and has been assessed and benchmarked by National Institute of Standards and Technology (NIST) and UK National Physical Laboratory (NPL).
Description	OLFR detects faces in live CCTV feeds, extracting biometric features. These are compared against an alert list that triggers alerts based on similarity scores.
Decision-making	Generated alerts are reviewed by trained officers before engagement. There are no automated decisions or enforcement. Resultant alerts are treated as lines of enquiries.
Performance and Fairness	The OLFR system is monitored through continuous performance evaluation and fairness checks to ensure accuracy and compliance with ethical standards. Algorithm calibration includes monitoring date to ID any demographic basis. Post-deployment reviews will assess detection accuracy, false positive rates, and operational outcomes, with adjustments made as required. Independent audits and oversight by governance committees will provide additional scrutiny to maintain fairness and transparency. (Incorporates UK model methodology)
Funding	This is a trial/proof of concept. The WA Police Force OLFR project requires support, and funding is not yet determined. This will be subject of a submission at the appropriate time.

RISK ASSESSMENTS

Information Privacy Principles (IPP) Assessment

See Appendix 1: IPP Risk Assessment Register – OLFR

Outcome Summary	A Privacy Risk Assessment was conducted on the OLFR project across the eleven Information Privacy Principles (IPP) in the *PRIS Act 2024* (Appendix 1). The highest risk identified was in relation to IPP 4 (Information Security), namely the retention of biometric data beyond legal limits, inadequate deletion protocols, unauthorised access and lack of encryption or audit trails. The risk assessment determined that all identified risks had adequate controls, and after the implementation of those controls, there was a **low residual risk** for all categories. For IPP 6 (Access & Correction), the WA Police Force believes the exemption provided in S. 27 of the *PRIS Act 2024* is applicable. For IPP 10 (Automated Decision Making), please refer to the AI Risk Assessment (Appendix 2). The risk assessment also considered that OLFR is in a trial stage that will assess the feasibility and effectiveness of the project in supporting strategic policing objectives in Western Australia.
Consequences	• Non-compliance and breach of Privacy legislation • Legal challenges • Loss of public trust and confidence resulting in reputational damage • Misuse of personal data • Unlawful engagement due to false alerts • Perceived surveillance by communities • Discriminatory outcomes
Mitigation Actions	• AI and IPP impact assessments • Industry, government and community stakeholder engagement and consultation • Communication strategy, public awareness (i.e. signage), Officer briefings and industry briefings • Recording and reporting of deployment locations • System only recognises and matches with individuals on watch list • Ongoing deployment reviews and post-deployment evaluations • Human adjudication • Biometric data encrypted and deleted immediately if not a match, with non-matched biometrics not retained • Encrypted watchlist • WA Police Force existing Security Framework and protocols • Governance Committee review and oversight • Data stored within Australia

Artificial Intelligence (AI) Assessment

See Appendix 2: AI Risk Assessment Register – OLFR

Outcome Summary	An AI Risk Assessment was conducted on OLFR across the five Ethics Principles from the WA Government Artificial Intelligence Assurance Framework (see Appendix 2). The highest risk identified was in the Transparency category, namely due to insufficient public awareness, limited stakeholder and community engagement, and the absence of feedback mechanisms to capture effectiveness. The risk assessment determined that all categories had excellent controls, and after the implementation of the proposed controls, there was a **low residual risk** for all categories except Transparency which has a **moderate residual risk**. The risk assessment also considered that OLFR is in a trial stage that will assess the feasibility and effectiveness of the project in supporting strategic policing objectives in Western Australia.
Consequences	• Loss of public trust and confidence resulting in reputational damage and negative community • Community resistance • Poor management of industry and government consequences • Legal and policy non-compliance • Deployment beyond approved scope • Police operations compromised • Improper deployment • Failure to comply with policing standards and processes • System downtime or inaccurate alerts
Mitigation Actions	• Communication strategy, public awareness (i.e signage), officer briefings and industry briefings • Industry, government and community stakeholder engagement • Governance Committee review and oversight • Proposed pre-deployment impact assessments • Ongoing deployment review and post-deployment evaluations • Human adjudication and verification with supervisor oversight • Agency's existing discipline processes • Comprehensive training covering ethical use, privacy and data protection • Superintendent level determination of suitably trained staff, including supervisors and action plans • Strict retention and deletion policies in line with WA Police Force data ownership and legislation • Biometric data encrypted and deleted immediately if not a match. Non matched biometrics not retained • WA Police Force Security Framework and protocols

Version Control

Version	Date	Author	Change Description
1.0	10/05/2026	Paul Gelmi	