OFFICE OF THE
Information
Commissioner
QUEENSLAND

Camera surveillance through the privacy lens:

Local government use of camera surveillance in public spaces and privacy impact assessments

April 2026

Report No. 2 to the Queensland Legislative Assembly for 2025-26

Acknowledgement of Country

The Office of the Information Commissioner acknowledges Aboriginal and Torres Strait Islander peoples as the First Australians and recognises their culture, history, diversity and their deep connection to the land, waters and seas of Queensland and the Torres Strait.

We acknowledge the traditional custodians of the lands on which we operate and wish to pay our respects to their Elders past and present.

Copies of this report are available on our website at www.oic.qld.gov.au and further copies are available on request to:

Office of the Information Commissioner

PO Box 10143, Adelaide Street, Brisbane, Qld 4000

Phone +61 7 3234 7373 or Freecall 1800 OIC QLD (1800 642 753)

Email administration@oic.qld.gov.au

Web www.oic.qld.gov.au

ISBN: 978-0-9953725-8-0

OFFICE OF THE
Information Commissioner
QUEENSLAND

April 2026

The Honourable Patrick Weir MP
Speaker of the Legislative Assembly
Parliament House
Brisbane QLD 4000

Dear Speaker,

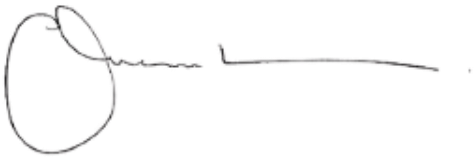
I am pleased to present a report to the Queensland Parliament titled, *'Camera surveillance through the privacy lens: Local government use of camera surveillance in public spaces and privacy impact assessments',* following a review conducted by the Office of the Information Commissioner under section 135 of the *Information Privacy Act 2009* (Qld).

The review examines the use of privacy impact assessments by Queensland's local governments when implementing, expanding or upgrading camera surveillance systems in public spaces. The review also examines privacy impact assessments undertaken by six local governments.

The report details responses provided by local governments to a questionnaire about their management of privacy issues and risks in association with the use of camera surveillance. The report identifies opportunities for improvement, and makes six recommendations about privacy impact assessments to local governments and all agencies operating camera surveillance in public spaces.

In accordance with subsection 193(5) of the *Information Privacy Act 2009* (Qld), I request that the review report be tabled in the Legislative Assembly.

Yours sincerely,



Joanne Kummrow
Information Commission

Table of contents

1 Executive Summary

As we move through our local communities going about our daily lives, increasingly our image, location and movements are being captured by camera surveillance systems installed in public spaces to monitor and respond to public safety risks and deter unlawful and unsafe conduct.

In doing so, camera surveillance systems capture the personal information of individuals and are subject to information privacy protections under the *Information Privacy Act 2009* (Qld) (**Information Privacy Act**).

The Information Privacy Act protects individuals' privacy when government agencies collect, store, handle, manage, use or disclose personal information, such as an individual's image or location.

Local governments are increasingly adopting advanced surveillance technologies, including body-worn cameras, drones, and artificial intelligence-enabled systems. These advancements underscore the need for robust privacy protections to address the unique risks associated with these technologies.

The review was conducted by the Information Commissioner under section 135 of the Information Privacy Act.

This report details findings and recommendations made by the Office of the Information Commissioner (**OIC**) following a review that examined the use by Queensland's local governments of camera surveillance systems in public spaces, and whether and to what extent local governments conduct privacy impact assessments to ensure they are meeting privacy obligations under the Information Privacy Act.

A privacy impact assessment supports agencies in meeting their obligations under the Information Privacy Act, including the privacy principles. If undertaken prior to implementing, expanding or upgrading a camera surveillance system, a privacy impact assessment assists an agency to identify risks and issues upfront, putting the agency in a position to proactively manage or mitigate any risks.

Taking a 'privacy-by-design' approach and incorporating privacy protections into a system from the start is more efficient and cost effective than reverse engineering privacy protections into an established system.

Given the prevalence of camera surveillance systems in public places installed and operated by local governments and their capture and collection of individuals' personal information, it is critical that the public trust that agencies are taking privacy seriously and meeting their obligations under the Information Privacy Act.

Findings

Based on responses received from 50 out of 78 local governments, the review found:

- Most local governments have established privacy policies and strategies to manage privacy. They recognise the importance of privacy in fostering public trust and cooperation, particularly in the context of camera surveillance systems, which are implemented to enhance public safety.
- Local governments have identified and managed privacy risks associated with camera surveillance. However, their commitment to privacy is not always comprehensive or fully informed by the requirements of the Information Privacy Act.
- While privacy impact assessments are a critical tool for identifying and mitigating privacy risks, local governments do not consistently use them when implementing, expanding or upgrading camera surveillance systems. On average, privacy impact assessments have been conducted for just under half of camera holdings, with a focus on fixed cameras. Other types of surveillance technologies, such as body-worn cameras, drones, and artificial intelligence-enabled systems (for example, facial recognition), are often overlooked.

Privacy impact assessments

The review also examined a sample of privacy impact assessments provided by six local governments, which yielded mixed results.

While the privacy impact assessments focused reasonably well on privacy risks and strategies, the review found the assessments undertaken were not sufficiently thorough.

Key gaps include:

- insufficient examination of all project parameters in relation to privacy management
- limited consideration of whether camera surveillance is the most appropriate method to achieve project goals or how to minimise the collection of personal information
- lack of engagement with external expertise or lived experience, such as input from third party contractors or the community, to identify privacy risks and mitigation strategies
- inadequate coverage of emerging technologies, such as artificial intelligence (**AI**).

Recommendations

This report makes six recommendations arising from the review findings, which are set out in Section 2 of this report.

The recommendations are designed to enhance privacy practices and build public trust through local governments:

- **Adopting a 'privacy-by-design' approach**: This involves conducting a privacy impact assessment at the earliest stage of planning, implementing or upgrading camera surveillance systems. Proactively embedding privacy protections is more effective and cost-efficient than retrofitting them later.
- **Undertaking comprehensive privacy impact assessments**: Conducting thorough privacy impact assessments for all camera surveillance systems, including fixed cameras, body-worn cameras, drones, and artificial intelligence-enabled systems.
- **Evaluating alternatives**: Assessing whether camera surveillance is the most appropriate solution for achieving project objectives and exploring ways to minimise the collection of personal information.

- **Engaging stakeholders**: Involving external experts, community members and other stakeholders in the privacy impact assessment process to identify privacy risks and develop effective mitigation strategies.
- **Enhancing awareness and training**: Increasing agency awareness of legislated privacy obligations under the Information Privacy Act and undertaking agency training on the effective use of privacy tools, including privacy impact assessments.

By adopting the report's recommendations, local governments can demonstrate their commitment to protecting personal information, ensure they are meeting their privacy obligations under the Information Privacy Act (including the Queensland Privacy Principles) and foster community confidence in their use of camera surveillance in public spaces.

While the recommendations are directed at local governments, they are also relevant to other government agencies operating camera surveillance systems.

2 Recommendations

Based on the findings in this report, the Information Commissioner makes the following recommendations to all Queensland local governments and agencies operating camera surveillance in public spaces:

Recommendation 1

Within 12 months, **establish**

- **a policy** requiring a privacy impact assessment at the earliest stages of planning or upgrading camera surveillance systems
- **a procedure** for conducting a privacy impact assessment.

Recommendation 2

Within 12 months, ensure that any procedure for conducting a **privacy impact assessment includes**:

a) **evaluating alternatives** to camera surveillance as a solution for achieving project objectives

b) considering ways to **minimise the collection** of personal information

c) engaging all relevant **stakeholders** in identification of privacy risks and risk mitigation strategies, including

- members of the community affected by the proposed camera surveillance system
- external service providers involved in providing the camera surveillance.

Recommendation 3

Within three months, **undertake an audit and inventory** of agency-operated and funded camera surveillance systems in public spaces that capture personal information.

Recommendation 4

Within nine months, **undertake a thorough privacy impact assessment** of camera surveillance systems that capture personal information in public spaces.

Recommendation 5

Within 12 months, implement procedures to **mitigate privacy risks** identified for camera surveillance systems in public spaces that capture personal information. If procedures require longer than 12 months, document estimated timelines in an action plan.

Recommendation 6

Within 12 months, **increase awareness** for all agency staff of legislated privacy obligations under the Information Privacy Act, by undertaking training on the effective use of privacy tools, including privacy impact assessments.

3 Background

Local governments install and operate camera surveillance systems to promote and enhance community safety in public spaces. These systems can capture personal information, which makes them subject to the *Information Privacy Act 2009* (Qld) (**Information Privacy Act**).

Agencies operating camera surveillance systems in public spaces should ensure they consider information privacy impacts and manage privacy risks associated with the personal information they collect, store, handle, manage, use and disclose.

An effective way to assess and manage privacy risks is to undertake a privacy impact assessment (**PIA**) as part of a 'privacy-by-design' approach. 'Privacy-by-design' means including privacy as a key consideration in the early stages of a project and throughout its lifecycle.

Ten years ago, OIC assessed privacy safeguards for camera surveillance across agencies, including local governments.[1] At the time, OIC found that while agencies were generally aware of the need to manage the privacy impacts of operating camera surveillance systems, they did not use PIAs to assess their privacy obligations or to proactively manage associated privacy risks.

In August 2025, the Information Commissioner commenced a review (**Review**) under section 135 of the Information Privacy Act. The Review examined local governments' use of PIAs in relation to their use and expansion of camera surveillance in public spaces.

This Review is limited to camera surveillance systems in public spaces and does not include cameras located inside local government buildings.

[1] *Camera surveillance and privacy Review of camera surveillance use by Queensland government agencies and compliance with the privacy principles in the Information Privacy Act 2009 (Qld).* Report No. 2 of 2012/13 to the Queensland Legislative Assembly, tabled July 2012. Followed up 2015-16.

This report is in two parts:

(a) findings from a questionnaire sent to Queensland's 78 local governments to identify how many cameras they operate, how they manage privacy risks and whether they have conducted a PIA

(b) findings from an examination of a sample of six PIAs provided to OIC.

3.1 Local government use of camera surveillance

Local governments use camera surveillance in public spaces to:

- promote public safety, for example by placing cameras in visible locations to deter unlawful and unsafe conduct
- for law enforcement, for example to identify vehicles in breach of local laws or assist the Queensland Police Service to identify alleged offenders
- to monitor remote locations, for example for road accessibility
- to support respectful and safe interactions between agency officers and community members, for example, via fixed cameras or audio recordings while attending an incident, at a customer service counter or other public service access point.

Effective camera surveillance systems incorporate 'privacy-by-design'. Agencies adopting a 'privacy-by-design' approach consider privacy from the outset and design their camera surveillance system to mitigate or manage privacy risks. For example, an agency might consider whether:

- camera surveillance is necessary or whether there is another equally effective solution that does not collect personal information
- it is possible to install cameras in such a way that they do not collect personal information
- to purchase a type of camera surveillance system that enables redaction of personal information.

A visible commitment to privacy builds community trust in the government's collection, storage, use and disclosure of their personal information whilst pursuing community safety.

Since OIC first examined government agencies' consideration of privacy in camera surveillance in 2012,[2] agencies have increased:

- the number and types of camera systems operated in public
- incorporation of privacy considerations into these systems.

OIC examined privacy in camera surveillance in subsequent years:[3]

- in specific audits conducted in 2012-13 and 2015-16
- as part of a general examination of agency compliance in 2018-19
- as one element in compliance audits of individual agencies.

The comparison from 2015-16 to 2018-19 enabled assessment of the uptake of the privacy principles in camera surveillance. The local government sector reported an increase in adopting the privacy principles in the operation of fixed camera surveillance systems from 48% in 2015-16 to 72% in 2018-19.[4]

In 2019, 25% of agencies reported conducting PIAs.[5] The Information Commissioner commented:

> *Privacy impact assessments are core business.*
>
> *All agencies must protect individuals' personal information. Failure to do so exposes individuals to risk, erodes trust, jeopardises public take up of services, and damages an agency's reputation.*
>
> *Project management methodologies and tools should include privacy impact assessments as key deliverables during design, development and operation*

---

2 *Camera surveillance and privacy Review of camera surveillance use by Queensland government agencies and compliance with the privacy principles in the Information Privacy Act 2009 (Qld).* Report No. 2 of 2012-13 to the Queensland Legislative Assembly

3 Parliamentary reports are linked from the OIC website - https://www.oic.qld.gov.au/about/our-organisation/key-functions/compliance-and-audit-reports.

4 *10 years on Report No. 5 to the Queensland Legislative Assembly for 2018-19 Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld),* Report No. 5 to the Queensland Legislative Assembly for 2018-19, page 29.

5 *10 years on Report No. 5 to the Queensland Legislative Assembly for 2018-19 Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld),* Report No. 5 to the Queensland Legislative Assembly for 2018-19, page 30.

of all agency functions. This is core business for any agency when it is managing personal information.[6]

Agency compliance audits have also included an assessment of privacy and camera surveillance. Agency compliance audits of local governments have found that local governments consider privacy in the operation of camera surveillance. However, the audits also found that the local governments audited did not fully address their privacy obligations under the Information Privacy Act.

3.2 Handling personal information

The *Human Rights Act 2019* (Qld) establishes a right of privacy for all individuals in Queensland.[7] This includes the right not to have a person's privacy, family, home or correspondence interfered with unlawfully.

The Information Privacy Act requires agencies to adopt the privacy principles. Prior to the *Information Privacy and Other Legislation Amendment Act 2023* (**IPOLA**), the Information Privacy Act prescribed 11 Information Privacy Principles (**IPPs**) covering collection, storage, access, use and disclosure of personal information. It also required agencies to bind their contracted service providers to the privacy principles[8] and made conditions for disclosing personal information overseas.[9]

Post-IPOLA taking effect in July 2025, the Information Privacy Act prescribes the Queensland Privacy Principles (**QPPs**) which cover similar privacy protections. The Information Privacy Act makes provision for binding contracted service providers to the QPPs and continues to make provision for overseas transfer of personal information.[10]

Post-IPOLA and currently, the Information Privacy Act mandates that agencies must have a clearly expressed and current privacy policy about the management of personal information (a **QPP Privacy Policy**). Agencies must make their QPP

6 *10 years on Report No. 5 to the Queensland Legislative Assembly for 2018-19 Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)*, Report No. 5 to the Queensland Legislative Assembly for 2018-19, page 31.
7 Sections 11 and 25 of the *Human Rights Act 2019* (Qld).
8 Section 35 of the Information Privacy Act.
9 Section 33 of the Information Privacy Act.
10 Section 202 of the Information Privacy Act states the amendments to that Act do not apply to local governments for a year after commencement, that is until 1 July 2026, except for Chapter 3 and related provisions (QPP Codes).

Privacy Policy available free of charge and in an appropriate form, for example, by publishing the policy on their website.[11]

PIAs are a key strategy for ensuring compliance with the Information Privacy Act. A PIA prompts an agency to consider the collection, storage, access, use and disclosure of personal information in a structured way, against the requirements of the Information Privacy Act. It can ensure an agency recognises its obligations and the risks associated with their proposed project upfront. Agencies can then build privacy into their projects by design, addressing their privacy obligations and implementing strategies to manage or mitigate privacy risks.

Agencies using a PIA to build privacy into their systems will be more likely to have efficient and cost-effective approach to privacy.

3.3 Information Commissioner's Review

Under section 135 of the Information Privacy Act, the Information Commissioner may initiate a review of an agency's personal information handling practices to report on privacy related issues of a systemic nature generally, and make recommendations to address those issues, including by a report to the Queensland Parliament.

The recent changes to the Information Privacy Act and the introduction of new QPPs that replace the IPPs will come into effect for local governments from 1 July 2026.

The Information Commissioner recognises that agencies need time to fully embed practices that address the new legislative requirements. As a result, the Information Commissioner determined not to undertake audits to ascertain whether agencies have implemented the legislative changes. Rather, the OIC will continue to provide advice and assistance, and work alongside agencies to support their pathway to implementation.

[11] Queensland Privacy Principle 1, *QPP 1—open and transparent management of personal information*, QPP 1.3. QPP 1.4 prescribes what the privacy policy must contain. QPP 1.5 requires agencies to take reasonable steps to make its QPP privacy policy available—
(a) free of charge; and
(b) in an appropriate form.
QPP 1.5 gives an example of how an agency may make its QPP privacy policy available – by publication on the agency's website.

The Review examines local governments' use of PIAs for camera surveillance as a key tool for ensuring personal information is protected and safeguarded in accordance with the Information Privacy Act. It is not intended to assess their compliance with risk assessment requirements under the QPPs, but to better understand privacy practices with regard to camera surveillance in public spaces. For this reason, local governments are not identified as non-compliant in the Review if they did not perform a PIA, and the OIC did not subsequently assess whether other alternative actions taken by the local governments were sufficient to meet their obligations under the Information Privacy Act.

Nevertheless, the Information Commissioner and Privacy Commissioner continue to urge agencies to use PIAs to meet their risk assessment obligations under the QPPs as part of a 'privacy-by-design' approach.

3.4 Scope

The Review was conducted in accordance with section 135(1) of the Information Privacy Act[12] and relied on the accuracy and completeness of information provided by local governments to inform its findings.

While every effort was made to ensure the accuracy and completeness of the Review, it is important to acknowledge the limitations of relying on agency self-reports.

These limitations should be taken into account when considering the findings and recommendations of the Review.

3.5 Agency responses to Review findings

The six local governments, whose PIAs were examined, were sent papers describing the facts and findings. All agencies confirmed the accuracy of the facts.

[12] Section 135(1)(a)(i)(A) of the Information Privacy Act – a review of personal information handling practices of relevant entities, including technologies, programs, policies and procedures, to identify privacy related issues of a systemic nature generally.

For the findings:

- one agency confirmed the findings and advised they intended to conduct PIAs for all cameras
- one agency updated their PIA and forwarded it to OIC. This may be the subject of a follow-up review
- two agencies acknowledged the findings
- two agencies did not respond.

4 Results of a survey of all local governments

On 29 August 2025, the Information Commissioner wrote to all 78 local governments in Queensland asking about their consideration of privacy when operating camera surveillance in public spaces.

4.1 Summary of findings

50 out of 78 (64%) local governments responded. **Appendix 1** lists respondents and non-respondents. 47 out of 50 local government respondents to this survey use camera surveillance in public spaces.

The number of cameras local governments report using has increased by approximately 33% over the last 10 years, from just over 12,000 cameras in 2015 to just over 16,000 cameras in 2025.

New digital technologies and tools are used to a greater extent in 2025 compared to 2015. These include facial recognition, AI, body worn cameras and drones.

Respondents have all taken steps to manage privacy impacts. Common steps reported are:

- using signage and the agency website to notify the community about the camera surveillance
- keeping footage secure through secure storage, restricted access and a requirement for authorisation to access footage
- controlling the use of footage by defining and limiting acceptable uses
- controlling disclosure with structured policies and procedures, including for Queensland Police Service requests
- automatically deleting footage after a fixed period.

Most respondents have a privacy policy. Legislation now mandates that agencies have and make available a privacy policy. All agencies should have a privacy policy and ideally publish it on their website.

A small number of local governments responded to the questionnaire in a way that suggests they are not fully aware of their privacy obligations.

There has been a good uptake of PIAs compared to 10 years ago, when PIAs were almost non-existent. However, there is still work to do. Less than half of the respondents had conducted a PIA (20 out of 50 respondents). There were indications that some local governments did not appreciate the value of PIAs in assisting them to recognise and address privacy issues.

Local governments had typically not considered new technologies through a privacy lens, particularly the use of AI.

4.2 Questionnaire

The questionnaire used by OIC in the review is at **Appendix 2**. It consists of six open ended questions. The responses to the questions led to OIC forming three thematic conclusions. The conclusions, and the questions that informed them, are:

Local governments are increasing the number of camera surveillance systems used and incorporating new technologies in these systems

Question One – the number and types of cameras operated

Question Two – whether the camera system uses facial recognition

Question Three – whether the camera system uses AI

Local governments are committed to managing privacy impacts in camera surveillance systems

Question Five – the steps the local government took to manage privacy impacts

Question Six – whether the local government has a privacy policy

Local governments are not generally using privacy impact assessments to identify privacy risks and considering how to manage them

Question Four – whether the local government conducted a privacy impact assessment

The full questionnaire adopts a mixture of:

- yes/no questions and numerical questions for quantitative analysis
- open ended, text based questions to ensure local governments could respond fully and provide information that OIC may not have anticipated.

4.3 Respondent profile

As previously stated, 50 out of 78 (64%) local governments responded.[13] Appendix 1 lists respondents and non-respondents. 47 out of 50 respondents use camera surveillance.[14]

Some of the questions in the 2025 survey are similar to a 2015-16 OIC survey of privacy and camera surveillance. The response rate in 2025 is lower than in 2015-16, but is sufficient for analysis in this Review.[15]

There are five types of local government – shire council, regional council, city council, Aboriginal shire council and town authority.[16] The largest cohort of responses was from regional councils (24 out of 50 responses, 48%). There was a reasonable spread of responses from each type of local government, making the survey responses broadly representative of each type of local government, depicted in Figure 1.

[13] One local government responded too late for their response to form part of this report.
[14] The three local governments responding to the questionnaire and not using camera surveillance were one Shire council and two Aboriginal Shire councils.
[15] Supplementary material to the follow-up report tabled December 2015. *Information Privacy and Camera Surveillance Survey 2015 Local Government Sector Survey Report Queensland local government sector responses and comparative analysis with 2011 results.* In 2015, 54 out of 77 (70%) local governments responded to the survey.
[16] Rio Tinto is responsible for the administration of Weipa, which it carries out through the Weipa Town Authority. This is the one 'town authority'. It did not respond to requests made during the Review.

Figure 1

Response rates by local government type

Local government type	Number	Number of responses	Percent of each response type	Percent of overall responses
Shire	28	18	64%	36%
Regional	29	24	83%	48%
City	8	5	63%	10%
Aboriginal Shire	12	3	25%	6%
Town Authority	1	0	0%	0%
TOTALS	**78**	**50**		**64%**

Source: Office of the Information Commissioner Questionnaire, 2025

4.4 Growing numbers and types of camera surveillance

47 local governments reported using 16,029 surveillance cameras – fixed cameras, mobile cameras, body worn cameras and drones, depicted in Figure 2.[17] A small number of local governments hold the majority of cameras.

Figure 2
Number of cameras by type of camera operated by local governments (out of a total of 16029 cameras)

13,334 Fixed Cameras
(83% of cameras)

1,537 Mobile cameras
(10% of cameras)

1,060 Body Worn Cameras
(7% of cameras)

98 Drones
(1% of cameras)

Data Source: Office of the Information Commissioner Questionnaire, 2025

Creative Commons Images: https://www.pickpik.com/rotary-camera-monitoring-safety-surveillance-the-police-the-investigation-72052, https://visiondetectionsystems.com/, https://commons.wikimedia.org/wiki/File:Bernalillo-NM-Sheriff-Body-Worn-Camera.jpg, https://dronelife.com/tag/drone-privacy-policy/

[17] Percentages reported in whole numbers may not always total 100 due to rounding.

The average number of cameras per local government was 321 cameras.

Figure 3 depicts the average number of cameras per local government by type of respondent local government.

Figure 3
Average number of cameras by type and by type of local government

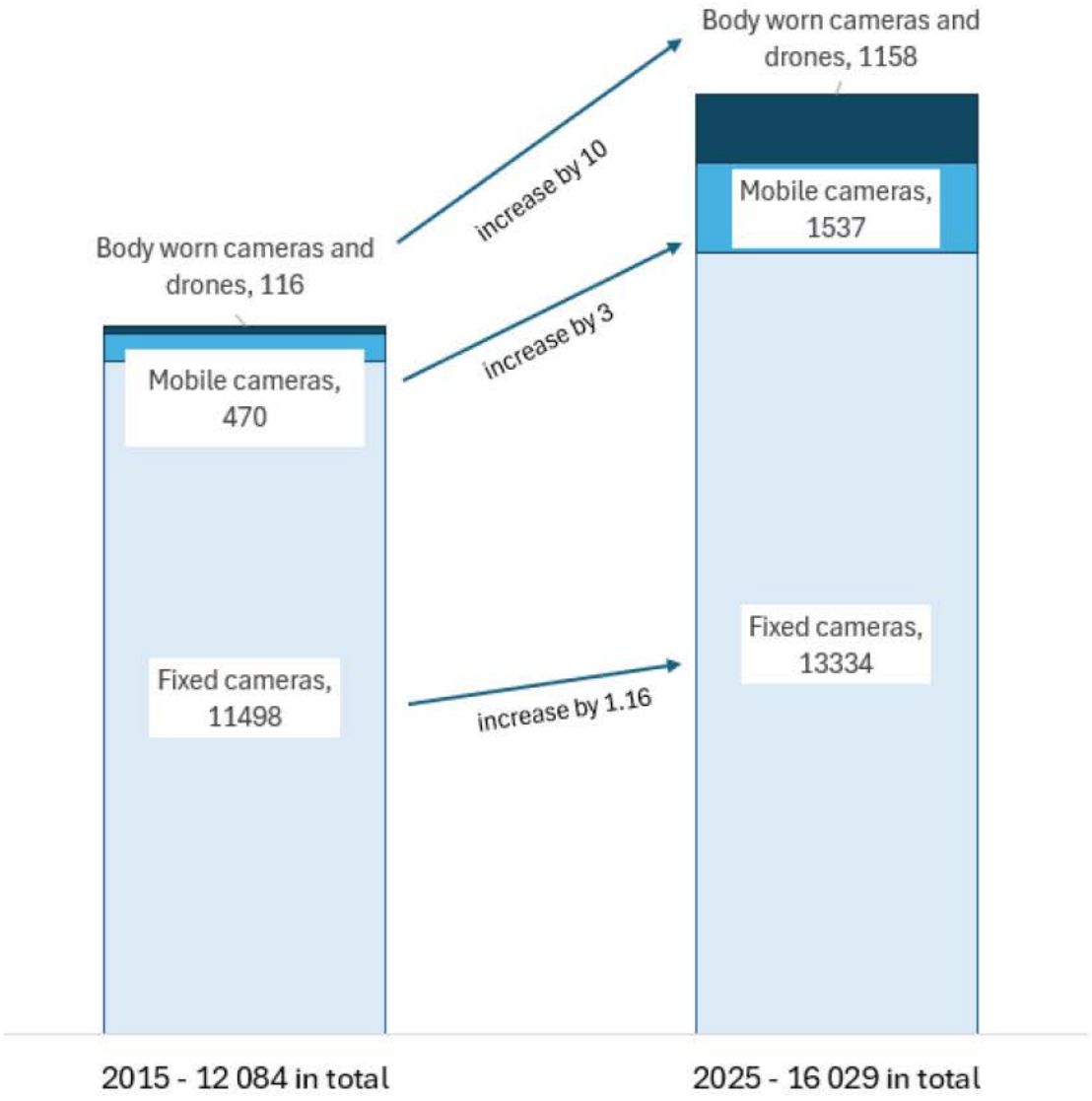
Type of local government	Average fixed cameras	Average mobile cameras	Average body worn cameras	Average drones	Average all cameras
Shire	74	5	4	1	84
Regional	204	25	21	2	252
City	1414	172	98	5	1689
Aboriginal Shire	8	0	0	0	8

Source: Office of the Information Commissioner Questionnaire, 2025

Over the last 10 years, the number of cameras used by local governments has increased from just over 12,000 to just over 16,000 cameras, representing a 33% increase. Further, in 2015, 13% of respondents reported they did not have any cameras, which has decreased to 6% in 2025.

Local governments have increased the use of all types of cameras. The greatest growth has been in body-worn cameras and drones, which increased tenfold between 2015 and 2025, as depicted in Figure 4.

Figure 4
Increase in number and type of local government cameras 2015-2025



Source: Office of the Information Commissioner Follow-up report 2015 and Questionnaire, 2025

Facial recognition

An emerging technology is facial recognition. Facial recognition is a type of AI applied to the images collected by surveillance cameras to identify individuals.

Six local governments reported having facial recognition as part of their camera surveillance systems. Two local governments said that the camera surveillance system had facial recognition capability, but the local government did not use it. The other four local governments use facial recognition capability as reported in Figure 5.

Figure 5
Use of facial recognition

Four local governments' descriptions of their use of facial recognition

- *'CCTV monitoring software that can do numberplate and facial matching (not against any database).'*
- *'Brief Cam operates in the background, however our system is not currently configured to do this. Our system operates 'similarity' search capabilities.'*
- *'… CCTV Platform (Verkada) does have some facial recognition capabilities.'*

  'The system is configured for general surveillance and does not use the biometric or facial recognition features as part of active monitoring and surveillance. Facial recognition is utilised when performing searches to retrieve footage for archival purposes for investigations.'
- *'The camera car does have facial recognition capability and the associated online software redacts faces for infringements.'*

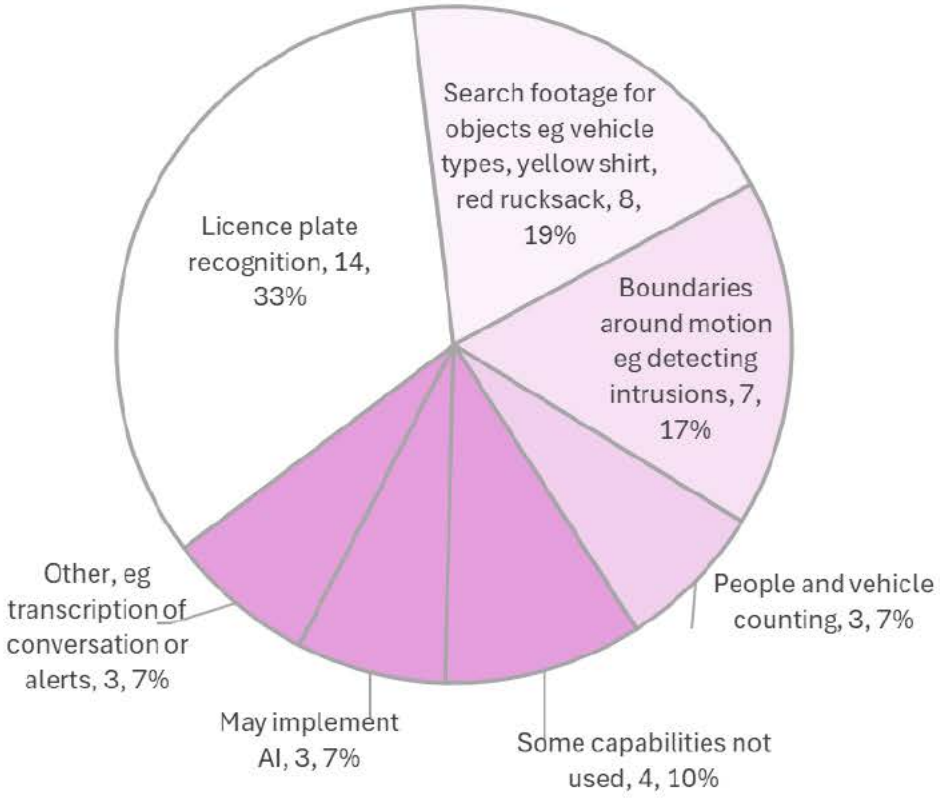
Source: Local Government responses to Office of the Information Commissioner Questionnaire, 2025,
Creative Commons Image: https://www.modernsystemsinc.com/ai-video-surveillance-for-kentucky-government-properties/

Artificial Intelligence

Local governments are starting to use AI for reasons other than facial recognition. If a local government uses AI in its camera surveillance, it typically uses it in multiple ways. 20 local governments reported using AI for the following purposes, as depicted in Figure 6:

- licence plate recognition was the most common with 33% of local governments deploying AI technology
- to search footage for objects, for example, vehicle types, personal characteristics such as a particular coloured clothing or backpack
- to put boundaries around motion, for example, detecting intrusions
- people and vehicle counting
- other, for example, transcription of recorded conversations or real-time alerts.

Figure 6
Use of AI in camera surveillance



Source: Office of the Information Commissioner Questionnaire, 2025

Case example: Use of AI to detect a pedestrian for public safety

*'The side arm waste collection fleet (48 vehicles) use an AI driven Pedestrian Detection System (**PDS**) (2 cameras per vehicle).*

The PDS is an industry leading type of technology that is designed to protect pedestrians that may walk within the danger zone of the collection arm on a side arm waste collection vehicle and stop the movement of the hydraulic arm when people are detected.

This system is not tracking faces or recording data, it is specifically looking for human forms in its detection arc. (3 x 5 m box extending out from the kerbside side of the vehicle).'

Image from SuperiorPak website, https://www.superiorpak.com.au/, suppliers to the Local Government using the technology, (downloaded 11 March 2026)

Image from Ipswich First (downloaded 11 March 2026)

https://www.ipswichfirst.com.au/world-class-safety-technology-for-new-ipswich-garbage-truck-fleet/

Source of text: Local Government response to Office of the Information Commissioner Questionnaire, 2025

Another local government listed the range of ways they use AI in conjunction with camera surveillance:

Broader uses for AI in conjunction with camera surveillance

- *'Crowd and Vehicle Counting - Useful for monitoring public spaces or traffic*
- *Loitering Detection - Detects objects that stay in a set area beyond a threshold time*
- *Intrusion Detection - Alerts when an object enters restricted zones*
- *Enter/Exit Detection - Monitors objects entering or exiting defined areas*
- *Attribute Analytics - Enabling faster searching based on physical attributes e.g. Colour of shirt, type of clothing, backpack,*
- *Virtual Line Crossing - Triggers when objects cross a designated line'*

Source: Local Government response to Office of the Information Commissioner Questionnaire, 2025

Local governments also reported some AI capabilities in their systems that they do not currently use, and advised that they may implement these in the future.

The types of local governments reporting usage of AI were City (3 out of 5 respondents, 60%), Regional (10 out of 24 respondents, 42%) and Shire (6 out of 18 respondents, 33%). One Aboriginal Shire reported using AI.

Local governments did not incorporate an assessment of AI in their PIAs. One shire council commented that they are considering implementing AI and that this had triggered the need to conduct a PIA '*in the coming months as we build out a more robust solution to our CCTV needs.*'

4.5 Local government commitment to privacy

All local governments that reported using camera surveillance also reported taking steps to manage privacy impacts.

This is consistent with findings in OIC's past audits. Ten years ago, agencies had not generally conducted a PIA for their camera surveillance, but most agencies reported considering privacy:

> *'Generally, the follow-up review noted increased inclusion of privacy considerations in the governance of camera surveillance systems, compared to 2011. In 2015, 80% of agencies reported that they actively informed the community about their use of camera surveillance. Each privacy element had been addressed by around half of the agencies in their surveillance camera policies, procedures and practices.'* [18]

The 2025 questionnaire prompted local governments with five specific questions about steps taken to address privacy considerations. The questionnaire had a free text field for local governments to report any additional steps taken. The specific prompts were:

- notifying the community about the operation of the camera surveillance system or type of camera
- data storage and security
- use of footage
- disclosure of footage
- retention and disposal of footage.

Local governments adopted multiple methods under each heading: there are more '*reported methods*' than '*respondents*'.

Notifying the community

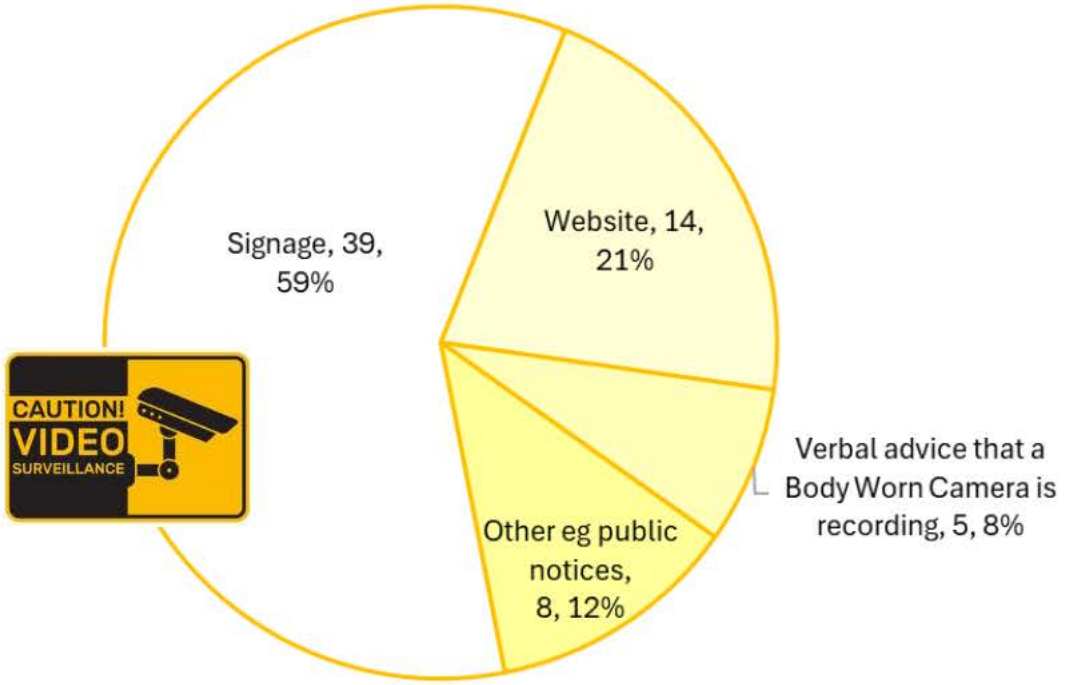
42 out of 45 respondents reported notifying the community. Three did not complete this question or gave an unclear answer.

[18] *Camera surveillance and privacy – follow-up review: Review of agency adoption of recommendations made under the Information Privacy Act 2009 (Qld)*, Report No. 1 of 2015-16 to the Queensland Legislative Assembly, page 7.

Allowing for respondents using multiple notification methods, there were 66 responses in total. The most common notification method was signage near cameras (39 out of 66 methods reported, 59%) or a notification on their website (14 out of 66 methods reported, 21%).

Five reported methods involved verbally notifying a member of the public if a body worn camera was in use (5 out of 66 methods reported, 8%). Figure 7 depicts the reported notification methods used by local governments.

Figure 7
Reported methods of notification about camera surveillance



Source: Office of the Information Commissioner Questionnaire, 2025,
Creative Commons Image: https://www.freepik.com/free-vector/different-cctv-system-badges-flat-set_9649349.htm

One local government stated notification in two instances was impractical:

Comment that collection notices are impractical
Litter & Dumping cameras are for a covert law enforcement purpose and do not have collection statements as this would be impractical and contrary to the enforcement purpose of the cameras. *ANPR cameras do not have a collection statement as that would be impractical on a moving vehicle.*

Source: Local Government response to Office of the Information Commissioner Questionnaire, 2025

There are alternative views for both of these instances:

- Deterrence is an important part of law enforcement. Notifying people of camera surveillance might deter unlawful littering and dumping.
- A camera based in a vehicle with automatic number plate recognition will not be constantly moving. For example, the vehicle will stop at traffic lights or come to rest when it is parked. Notice may also be provided using symbols or techniques such as QR codes that link to a longer policy. A visible notification on the vehicle will act as a deterrent and will build community confidence in the local government's attention to law enforcement.

Notification of the use of cameras is an important contributor to law enforcement, and it ensures local government compliance with Queensland Privacy Principle 5.

Data storage and security

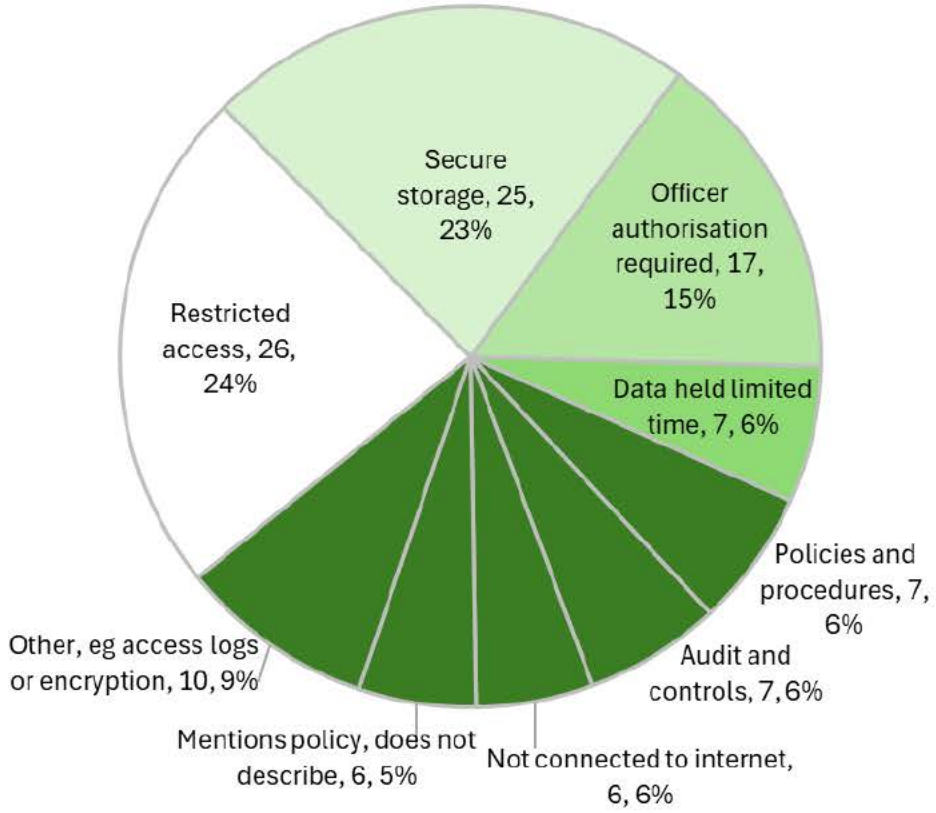
All respondent local governments reported using at least one data storage and security method. Most reported multiple methods: on average 2-3 methods for each local government.

The most common methods were restricting access to footage (26 out of 111 reported methods, 23%), secure storage (25 out of 111 reported methods, 23%) and requiring authorisation to access footage (17 out of 111 reported methods, 15%).

Local governments described a wide variety of other data security strategies, for example, data encryption, keeping the camera surveillance system disconnected from the internet, access logs, regular audits and restricting active monitoring.

Figure 8 depicts the breakdown of the 111 local government responses.

Figure 8
Data storage and security methods



Source: Office of the Information Commissioner Questionnaire, 2025

Use of footage

The most common method local governments reported for managing the use of camera surveillance footage was to have strictly defined uses (25 out of 63 reported methods, 40%).

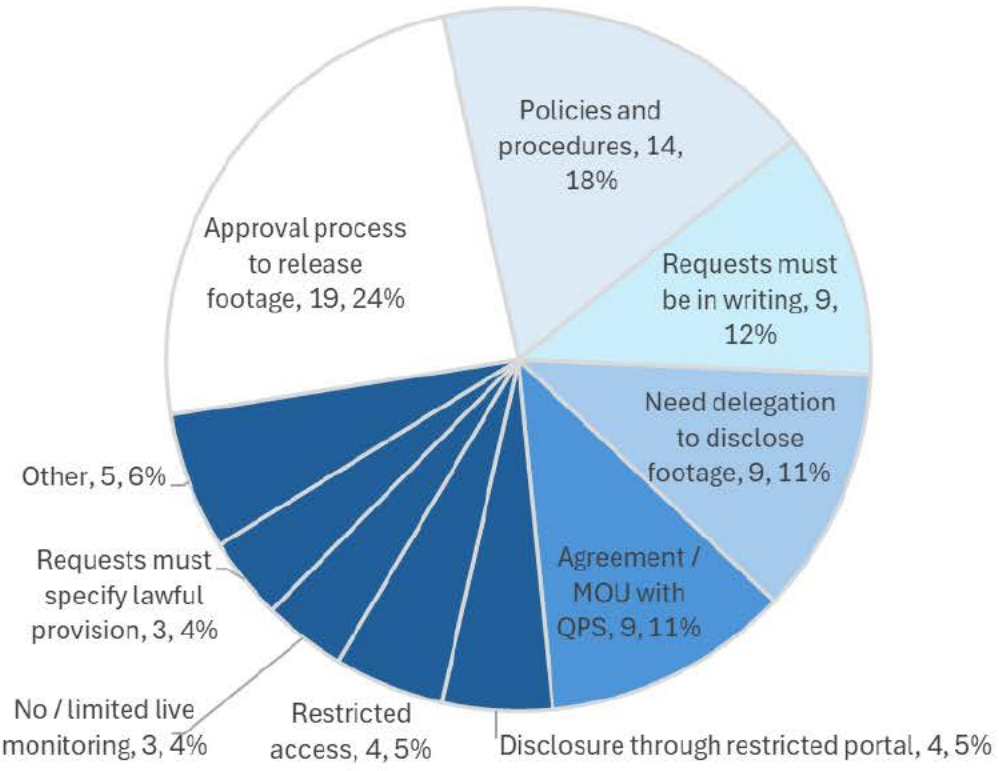
Other common methods were to:

- only use footage in accordance with policies and procedures (16 out of 63 reported methods, 25%)
- ensure cameras were visible to promote safety and deter crime (7 out of 63 reported methods, 11%)
- ensure any usage was authorised (6 out of 63 reported methods, 10%).

Disclosure of footage

Local governments reported a range of methods to manage disclosure, as depicted in Figure 9.

Figure 9
Methods for managing disclosure



Source: Office of the Information Commissioner Questionnaire, 2025.
'MOU' stands for Memorandum of Understanding, a written agreement as to the way in which information will be shared and used.

A common theme was managing requests from the Queensland Police Service. Nine local governments reported having a formal Memorandum of Understanding (**MOU**) or agreement with the Queensland Police Service for disclosure of footage. This is an effective strategy. Another nine local governments reported having a structured procedure for the Queensland Police Service to request footage as part of their description of approval processes, policies and procedures, delegations or requiring requests in writing. Eight local governments mentioned Queensland Police Service requests, but did not describe an access or information sharing policy or procedures.

Retention and disposal of footage

The most common method reported for managing retention and disposal of footage was automatic deletion or overwriting of footage after a fixed period of time (27 out of 46 responses, 59%). The reported time periods varied from five days to three months. Five local governments had different time periods for retaining footage depending on the type of footage.

The second most common method reported was a reference to reliance on policies and procedures (15 out of 46 responses, 33%).

Other comments

Local governments reported additional methods of managing privacy impacts:

- a regime of audit, staff training and other governance controls
- being mindful of the location of cameras
- masking parts of the captured images
- a drone use policy.

Privacy policy

Regardless of whether the local government operated camera surveillance, all 50 local government respondents answered the question about whether they had a privacy policy.

43 local governments (86%) reported having a privacy policy.

Seven local governments (14%) said they did not have a privacy policy. Two of these said other policies covered privacy, and one said they had a privacy policy in draft to be considered by Council. The Information Privacy Act requires all agencies to have a QPP Privacy Policy, containing prescribed information, and available to the public free of charge and in an appropriate form (for example on an agency website).[19]

Although the majority of local governments have the required policy, there is a shortfall. An assessment of agency compliance with this is out of scope for this Review.

[19] QPP 1.3, 1.4 and 1.5.

Of the 43 local governments reporting a privacy policy:

- 21 local governments said their privacy policy contained a policy about camera surveillance.
- 18 local governments reported having a separate camera surveillance policy.
- Four local governments were updating their policies about camera surveillance, three in their privacy policy and one in a standalone camera surveillance policy.

13 local governments made additional comments, the majority (eight comments) being about their intention to update the camera surveillance system or the policies governing the system.

4.6 Limited use of privacy impact assessments

20 out of 50 respondent local governments reported conducting a PIA for their camera surveillance (3 Shire, 13 Regional and 4 City councils). Two other local governments advised that a PIA was in progress, or they had identified the need to conduct a PIA.

Having 20 local governments conduct a PIA is an improvement compared to past OIC audits. The follow-up audit conducted in 2015-16, reported one local government conducting a PIA:

> *Privacy impact assessments were not commonly conducted for camera surveillance introductions or expansions in 2011 or 2015.* [20]

However, there is still work to do to achieve general acceptance of the usefulness of conducting PIAs.

[20] *Camera surveillance and privacy – follow-up review: Review of agency adoption of recommendations made under the Information Privacy Act 2009 (Qld)*, Report No. 1 of 2015-16 to the Queensland Legislative Assembly, page 18.

One local government queried the need for a PIA, saying:

Local government did not expect to consider privacy in public places

No. The agency has not used the Commission's template to assess Privacy impacts of CCTV cameras.

The primary driver behind the purchase and installation has been the greater good / public benefit and responding positively to community calls for enhanced security or improved performance from Council in maintaining fit for purpose services, facilities and assets that have been harmed, targeted or damaged by bad actors who the community wants to discourage, deter and identify and hold to account. ***It is unexpected to learn that there is an expectation of privacy in public places and on properties that the person depicted does not own or control and has opted into visiting despite warning notices.*** **[highlighting added]**

Source: Local Government response to Office of the Information Commissioner Questionnaire, 2025

This comment indicates that not all local governments fully understand the operation of the Information Privacy Act. Queensland Privacy Principle 5 states that if an agency collects personal information, it must take reasonable steps to notify individuals about the collection. Agency awareness of this obligation is an opportunity for improvement.

Three local governments conducted a PIA before installing the camera surveillance, 10 reported conducting a PIA before installing the cameras and afterwards, and nine reported conducting a PIA only after installation. Two of these related to a local government reporting they conducted elements of a PIA or were going to conduct a forthcoming PIA.

Regardless of whether they answered 'yes' or 'no', some local governments reported taking some steps towards conduct of a PIA, as depicted in Figure 10.

Although not reporting conduct of a PIA, all local governments with camera surveillance reported taking steps to address privacy issues.

Figure 10
Privacy impact assessment activities

Activities	Number of local governments reporting		
	PIA conducted	PIA: • not conducted • in progress • identified	TOTAL
	YES	NO	
Full PIA	12	1 (in progress)	13
Elements of a PIA	4	2	6
Checked legislation	3	2	5
Considered privacy		2	2
Identified a PIA was required		1	1
No description	1	19	20
TOTAL	**20**	**27**	**47**

Source: Office of the Information Commissioner Questionnaire, 2025

5 Review of six privacy impact assessments

Twenty local governments advised in their survey responses that they had conducted a PIA of camera surveillance in public spaces.

As part of this Review, OIC selected six local governments for closer examination, taking into account:

- the type of council in order to examine a mixture of City, Regional and Shire councils
- use of AI (selecting local governments that reported using AI).

This chapter reports findings about this sample of six local governments' PIAs.

The assessment was based on OIC's guideline for conducting PIAs.[21] The assessment criteria are at **Appendix 3**.

5.1 Summary of findings

Combined, the six sampled local governments operate a total of nearly 7,000 cameras.[22] The PIAs reviewed by OIC either represent good practice or contain elements of good practice. There were also opportunities for improvement.

Five themes emerged from the assessment of the PIAs. The local governments:

- identified privacy risks and strategies
- did not conduct PIAs for all camera holdings (they conducted PIAs for 44.8% of their camera holdings on average, and half that for new technologies such as mobile cameras, body worn cameras or drones)
- did not consider all the project parameters in their PIAs (All the PIAs were detailed and at a level appropriate for the project, although three of the local government PIAs had missing elements, for example binding contracted service providers to the privacy principles)

[21] OIC's guidelines are available at www.oic.qld.gov.au.
[22] 5,957 fixed cameras, 441 mobile cameras, 326 body worn cameras and 18 drones, a total of 6,852 cameras.

- have generally not used external consultation to inform the PIA (Only one local government alluded to consulting external stakeholders to assist in identifying privacy risks and risk mitigation strategies.)
- have been using AI without considering its privacy impacts (All of the sampled local governments reported using AI in their camera surveillance. None of the sampled local governments reported an ethical risk assessment of the use of AI for camera surveillance.)

5.2 Case study of good practice

One local government had a strong approach to assessing the privacy impacts of camera surveillance. This is presented here as one example of good practice.

Case study – Moreton Bay City Council

Moreton Bay City Council (the **Council**) is the third largest local government in Australia. Over 520,000 people live in its urban, rural and coastal areas, just north of Brisbane.

Case study – Moreton Bay City Council

The Council operates over 2,000 surveillance cameras in its public places. These cameras are either fixed, mobile, drones, or automated number plate recognition cameras. They are used to deter and resolve crime, promote public and staff safety, and protect property.

The Council has a suite of documents addressing privacy in camera surveillance, including comprehensive project documentation for the camera surveillance systems and four PIAs.

The main PIA is titled '*City of Moreton Bay CCTV Program*'. It covers all camera surveillance systems. This PIA effectively identifies and describes:

- reasons for camera surveillance
- the flow of information about surveillance, in easy-to-read diagrams
- how the privacy principles apply to camera surveillance
- strategies to pinpoint, assess and manage privacy risk
- how Council will engage with the public about the cameras.

The three other PIAs add information about specific projects – drones, targeted surveillance at customer service centres and weighbridges, and automated number plate recognition. These PIAs identify project-specific risks and strategies.

Council supports its staff to assess privacy risks with a pre-deployment checklist. This is completed before the installation of any new fixed cameras.

These documents are clear, detailed and thorough. They show that Council has carefully considered privacy impacts and documented its approach well.

Case study – Moreton Bay City Council

Council is innovating to improve its management of privacy. For example, Council advises it is:

- affixing QR Codes to all its portable and fixed assets to assist members of the public to access public-facing information about the asset and request further information
- trialling a governance support tool to record deployments and analyse data about the deployments, for example, to profile sites applying privacy masks and activating analytic functions.

Source Office of the Information Commissioner Questionnaire, Examination of Privacy Impact Assessment, 2025

Creative Commons or Public Images: https://commons.wikimedia.org/wiki/File:MoretonBayRegion-QldLGA.svg, https://www.moretonbay.qld.gov.au/Home

5.3 Privacy impact assessments identified privacy risks and strategies

At the heart of a PIA is the identification of a project's privacy risks and the development of strategies to mitigate or manage those risks.

A comprehensive PIA:

- assesses whether a project gives effect to the Information Privacy Act
- supports good governance and informed decision making
- allows potential problems and risks to be identified early, when addressing them is easier and cheaper
- recognises and addresses community privacy concerns, which can build trust in the agency's information handling practices.

All of the local government PIAs adopted a comprehensive suite of strategies to mitigate or manage privacy risks.

Five of the six local government PIAs identified privacy risks and developed risk mitigation strategies tailored to identified risks. The sixth used a suite of documents to identify privacy risks and risk mitigation strategies, including the PIA.

5.4 Privacy impact assessments did not cover all camera holdings

Agencies should conduct PIAs for all of their camera surveillance holdings.

The six local governments' responses to the questionnaire reported they operate 6,852 cameras in total.

They conducted PIAs for 3,073 (44.8%) cameras. These were predominantly for the fixed cameras and to a lesser extent mobile cameras. One of the local governments reported conducting a PIA for body worn cameras. One local government conducted a PIA for one drone as a trial and now operates 10 drones.

These results are depicted in Figure 11.

Figure 11
Camera surveillance covered by PIAs by six sampled local governments

	Fixed cameras	Mobile cameras	Body worn cameras	Drones	Totals
Number of cameras	5,957	551	326	18	6,852
Number of cameras considered in a PIA	2,870	154	48	1	3,073
Percent of cameras considered in a PIA	48.2%	27.9%	14.7%	5.6%	44.8%

Source: Office of the Information Commissioner Questionnaire and responses to specific questions, 2025

This means the six sampled local governments operate 55.2% of their cameras without using a PIA.

For cameras other than fixed cameras, such as mobile cameras, body worn cameras and drones, only 22.7% of cameras have been considered by a PIA, leaving 77.3% of the newer technology cameras operated without undertaking a PIA to consider privacy risks.

5.5 Privacy impact assessments did not consider all project parameters

A good PIA starts with a clear understanding of the project's purpose and outcomes. PIAs are scalable, with the level of required detail depending on the size and complexity of the project, and the nature of the personal information to be collected by an agency.

All of the PIAs reviewed by OIC were detailed, at a level appropriate for the project, although three had missing elements, such as:

- project responsibilities (one local government)
- a detailed description of achievements, deliverables and benefits (two local governments)
- overseas transfer of personal information (two local governments)
- binding contracted service providers (two local governments)
- a map of the flow of information (two local governments)
- linking privacy risks to the Information Privacy Act (three local governments).

Omissions in a PIA run the risk that the assessment will not fully identify privacy risks and strategies to mitigate or manage those risks. In particular, agencies need to take care when outsourcing services that the contractor is aware of and meets their privacy obligations.

5.6 Privacy impact assessments not based on thorough consultation

Consultation with stakeholders is essential to a PIA process. It allows people to identify privacy impacts and solutions based on their experience or expertise.

Project managers conducting PIAs should consider consulting:

- internal stakeholders - such as the information technology, privacy, legal, procurement and records management business areas, customer facing staff who will put the project into practice, and employees whose privacy may be impacted by the project
- external stakeholders – such as other government agencies, third party contracted service suppliers, clients, non-government organisations, advocacy groups and members of the public.

External consultation often involves seeking the views of the people whose personal information will be affected by the project. There are five main aims:

- enabling the agency to understand the concerns of those individuals
- informing the public of their rights
- improving transparency and openness through public awareness
- using community engagement and participation to strengthen government practices and decision making
- building community confidence in government.

Three local governments described stakeholder consultation in their PIAs, largely with internal stakeholders. Only one local government alluded to consulting external stakeholders to assist in identifying privacy risks and risk mitigation strategies. Three local governments conducted partial external consultation:

- with a supplier but not the community
- by advising rather than consulting
- by identifying a need to consult but not consulting.

Agencies will make informed decisions if they consult people affected by a project:

- Community members may have local knowledge relevant to the success of the project, for example, regarding sections of road that are accident-prone or regarding incursions onto council property.
- People with expertise relevant to their project can inform the agency about privacy risks and risk mitigation strategies from a technical or expert perspective.
- An agency outsourcing a service should consult the third party contractor about privacy as standard practice. Third party contractors may have experience in practical privacy issues affecting their service. The consultation also strengthens project management of the outsourced service by raising the contractor's privacy obligations for discussion.

Gaps in the PIAs miss the opportunity to identify privacy risks and risk mitigation strategies. They also miss the opportunity to build trust in the community about local government transparency and safeguarding of personal information.

5.7 Use of AI without considering privacy impacts

The Queensland Government requires government agencies to consider risk when implementing AI. This requirement is contained in its *Artificial intelligence governance policy*.[23] The purpose of this policy is to ensure that agencies take a '*structured and consistent approach when evaluating AI solutions for transparency, accountability and risk*'. The policy is mandatory for departments and statutory bodies, and describes good practice for other sectors, including local governments.

[23] *Artificial intelligence governance policy*, Queensland Government Enterprise Architecture, viewable at https://www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/artificial-intelligence-governance-policy.

In September 2025, the Auditor-General recommended that all public sector entities:

> *implement ethical risk assessment processes for AI systems in use or under development to more comprehensively identify and manage ethical risks* [Recommendation 7][24]

The *Artificial intelligence governance policy* requires agencies to use a consistent and evidence-based process which incorporates an ethical framework to evaluate transparency, accountability, and risk associated with the AI lifecycle.

To assist agencies in finding and using a framework to conduct an evaluation, the policy refers agencies to the *Foundational AI risk assessment Framework* (**FAIRA Framework**) and the *National Framework for the Assurance of AI in Government*.[25]

As a starting point, agencies need to determine whether they are using AI. The *Foundational artificial intelligence risk assessment guideline*[26] acknowledges that there can be ambiguity as to whether a product uses AI.

The guideline:

- provides three different definitions of AI from the OECD, an ISO standard, and under the Queensland Government Enterprise Architecture
- describes how risks for AI overlap with risks for a human-machine interface using non-AI automated technology or software
- identifies automated decision making as a possible AI use.

'Automated decision making' is a term covering a range of automated functions, including systems that make a decision, recommend a decision, automate fact-

---

[24] *Managing the ethical risks of artificial intelligence*, Queensland Audit Office, tabled 24 September 2025.

[25] *National framework for the assurance of artificial intelligence in government*, viewable at https://www.finance.gov.au/government/public-data/data-and-digital-ministers-meeting/national-framework-assurance-artificial-intelligence-government.
Foundational artificial intelligence risk assessment framework, viewable at https://www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/faira-framework.

[26] *Foundational artificial intelligence risk assessment guideline*, viewable at https://www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/foundational-artificial-intelligence-risk-assessment-guideline.

finding such as data matching, or provide interactive or non-interactive guidance to decision makers.

Regardless of definitions, the guideline encourages agencies to take a broad approach to automation projects and use the FAIRA Framework to identify risks and communicate with stakeholders in any project involving AI, automated decision making or decision-assistance technology.

Local governments should conduct an ethical risk assessment for all these projects, including an assessment of the privacy impacts of any AI component of the project.

All six local governments assessed reported using AI in their camera surveillance, with one reporting use of facial recognition.

When queried further, two of the local governments changed their report, and stated that specific systems did not involve AI, for example automated number plate recognition or thermal imaging.

There is recognised ambiguity around whether systems like this are AI systems. However, good practice takes a broad view and conducts an ethical risk assessment of any system with a component of AI, automated or assisted decision making technology.

None of the six local governments assessed reported an ethical risk assessment of the use of AI for camera surveillance.

6 Appendices

Appendix 1 – Survey respondents and non-respondents

Local government	Respondent
Aurukun Shire Council	No
Balonne Shire Council	Yes
Banana Shire Council	Yes
Barcaldine Regional Council	No
Barcoo Shire Council	Yes
Blackall-Tambo Regional Council	Yes
Boulia Shire Council	No
Brisbane City Council	Yes
Bulloo Shire Council	Yes
Bundaberg Regional Council	Yes
Burdekin Shire Council	Yes
Burke Shire Council	Yes
Cairns Regional Council	Yes
Carpentaria Shire Council	Yes
Cassowary Coast Regional Council	Yes
Central Highlands Regional Council	Yes
Charters Towers Regional Council	Yes
Cherbourg Aboriginal Shire Council	No
Cloncurry Shire Council	Yes
Cook Shire Council	Yes
Croydon Shire Council	Yes
Diamantina Shire Council	Yes
Doomadgee Aboriginal Shire Council	No
Douglas Shire Council	Yes
Etheridge Shire Council	No
Flinders Shire Council	Yes
Fraser Coast Regional Council	Yes

Local government	Respondent
Gladstone Regional Council	Yes
Gold Coast City Council	Yes
Goondiwindi Regional Council	Yes
Gympie Regional Council	No
Hinchinbrook Shire Council	No
Hope Vale Aboriginal Shire Council	Yes
Ipswich City Council	Yes
Isaac Regional Council	Yes
Kowanyama Aboriginal Shire Council	No
Livingstone Shire Council	Yes
Lockhart River Aboriginal Shire Council	No
Lockyer Valley Regional Council	Yes
Logan City Council	Yes
Longreach Regional Council	Yes
Mackay Regional Council	Yes
Mapoon Aboriginal Shire Council	No
Maranoa Regional Council	No
Mareeba Shire Council	Yes
McKinlay Shire Council	No
Moreton Bay City Council	Yes
Mornington Shire Council	No
Mount Isa City Council	No
Murweh Shire Council	Other *
Napranum Aboriginal Shire Council	No
Noosa Shire Council	Yes
North Burnett Regional Council	Yes
Northern Peninsula Area Regional Council	No
Palm Island Aboriginal Shire Council	Yes
Paroo Shire Council	No
Pormpuraaw Aboriginal Shire Council	No

Local government	Respondent
Quilpie Shire Council	No
Redland City Council	No
Richmond Shire Council	No
Rockhampton Regional Council	Yes
Scenic Rim Regional Council	Yes
Somerset Regional Council	Yes
South Burnett Regional Council	Yes
Southern Downs Regional Council	Yes
Sunshine Coast Regional Council	Yes
Tablelands Regional Council	Yes
Toowoomba Regional Council	Yes
Torres Shire Council	Yes
Torres Strait Island Regional Council	No
Townsville City Council	No
Weipa Town	No
Western Downs Regional Council	Yes
Whitsunday Regional Council	Yes
Winton Shire Council	Yes
Woorabinda Aboriginal Shire Council	No
Wujal Wujal Aboriginal Shire Council	Yes
Yarrabah Aboriginal Shire Council	No

** Murweh Shire Council submitted a late response, which was not included in the analysis.*

Appendix 2 – Questionnaire

Questionnaire – Privacy and camera surveillance in public spaces

Name of your Agency	
Contact officer – name	
Contact officer – position	
Contact officer – email	
Contact officer – phone	

Question	**Please advise**	**Agency response**
1	The number of cameras operating in your agency's public spaces. (Please only include cameras in public spaces, and do not include cameras operating inside agency premises, for example, for workplace health and safety reasons. If your agency does not operate any camera surveillance, please advise 'none' in response to each option in Question 1 to complete your response to the questionnaire.)	
	fixed cameras	
	mobile cameras	
	body worn cameras	
	drones	
2	Does your agency's CCTV surveillance system or any other type of camera have facial recognition capability?	
	If so, please describe.	
3	Does your agency use any other types of artificial intelligence in the operation of its CCTV surveillance system?	

Question	Please advise	Agency response
	If so, please describe.	
4	Has your agency conducted a privacy impact assessment for any aspect of its CCTV surveillance system or type of camera?	
	If yes, was the privacy impact assessment conducted:	
	• **before** the CCTV surveillance system or type of camera was installed?	
	If so, please describe.	
	• **after** the CCTV surveillance system or type of camera was installed, for example if the system was upgraded or as a regular review?	
	If so, please describe.	
5	Regardless of whether or not your agency has conducted a privacy impact assessment of its CCTV surveillance system or other type of camera, has it taken any other steps to manage the privacy impacts of operating CCTV surveillance systems?	
	If so, please outline what your agency has done.	
	For example:	
	• notifying the community about the operation of the camera surveillance system or type of camera	
	• data storage and security	
	• use of footage	
	• disclosure of footage	
	• retention and disposal of footage	

Question	Please advise	Agency response
	• any other steps?	
6	Does your agency have a privacy policy?	
	If so, does it refer to your agency's use of CCTV surveillance systems?	
	Further comments (optional)	

Appendix 3 – Review criteria for privacy impact assessments

These are the criteria used to assess each privacy impact assessment. For example, the description of a 'Threshold Privacy Impact Assessment' was used as the basis for assessing any threshold privacy impact assessments provided.

CRITERIA

Criteria - Overview

Use of camera surveillance in public spaces (number and type of cameras, sourced from questionnaire responses)

Consideration of privacy impacts when operating camera surveillance (threshold PIA, plan for a PIA, PIA)

Does the agency's PIA process represent good practice?

If applicable, has the agency undertaken an ethical risk assessment of use of artificial intelligence

Threshold Privacy Impact Assessment *(see OIC tool – Threshold Privacy Assessment 'At a Glance', and OIC Guideline Step-by-step guide to Privacy Impact Assessments)*

A Threshold Privacy Assessment is a tool that agencies can use to determine whether a PIA is required for new projects or projects that change the way personal information is handled. If an agency is unsure whether to complete a PIA, they can complete a Threshold assessment which is a series of screening questions that indicates whether a PIA should be completed.

A PIA should be conducted if a proposed project collects, stores, uses or discloses personal information.

An agency should undertake a PIA early in the development of a project so that its findings can influence its design. Undertaking a PIA early will prevent unnecessary

effort being expended on design options that are not compliant with the Information Privacy Act.

Privacy Impact Assessment Plan (*see OIC Guideline Step-by-step guide to Privacy Impact Assessments)*

Generally, if a Threshold Privacy Assessment indicates a PIA is required, the OIC would expect to see that the agency has considered:

- what aspects of the project will be assessed
- where the PIA will fit in the overall project plan and timeframes
- who will conduct the PIA and what resourcing is available
- the extent and timing of stakeholder consultations
- the steps that will need to be taken after the PIA, such as implementation of recommendations and arrangements for ongoing monitoring.

How detailed should the PIA process be? (*See OIC's template Privacy Impact Assessment Report*)

How detailed a PIA needs to be will depend on the scale and complexity of the project. For simple projects, the PIA process can be quick, and the PIA report may be quite short. Complex projects will involve a more formal and intensive exercise. The level of detail will be influenced by:

- the nature of the personal information involved in the project
- whether new or innovative technology will be used to collect or store the information
- whether the provision of personal information will be mandatory
- whether the project involves data-matching
- whether information will be shared with another agency; and/or
- the likely community and/or media interest in the project.

Camera surveillance captures images (and sometimes audio) of individuals. This is collected without consent, although a collection notice would inform people of the collection, and potentially allow them to avoid collection by avoiding that area.
If artificial intelligence is used, that would require additional consideration, particularly if that enables data matching.

The information may be shared with other agencies, for example, the Queensland Police Service.
There will be a level of community and media interest, as camera surveillance is seen as a community safety strategy.
The OIC would expect to see a PIA of reasonable breadth and depth to address these issues.

Does the agency's Privacy Impact Assessment describe the project?
(*See OIC Guideline Privacy impact assessments – consultation)*
Having a clear understanding of what the project intends to achieve provides context for the rest of the PIA process. A PIA will help identify the most privacy respectful way of achieving that aim.
This information could include:

- who is responsible for the project
- what the project will deliver
- what it will achieve
- the benefits to the agency or the community; and
- whether the project is part of a program of related projects.

Does the agency's Privacy Impact Assessment include consultation with stakeholders? (*See OIC Guideline – Privacy impact assessments – consultation)*

Consultation with stakeholders who will be affected by the project, or who have an interest in the project, is essential to the PIA process.

The aim is to take reasonable steps to facilitate as much communication about the project as possible so that its privacy impacts and risks can be identified and discussed.

Who an agency should consult will depend on the nature of the project, but may include:

- internal stakeholders – are critical as they can answer questions about likely information flows, governance structures, technical architecture, legislation under which the agency operates and recordkeeping requirements. They may also be able to suggest potential actions to address the identified privacy issues or provide advice on what option is the most appropriate.
- external stakeholders – involves seeking the views of the people whose personal information will be affected by the project. It will allow the agency to understand the concerns of those individuals and improves transparency by making people aware of how their personal information will be used.

Consultation is not necessarily a separate step as it can be useful to consult throughout the PIA process.

Effective consultation

Effective consultations should follow these principles:

- Timely – at the right stage and allow enough time for responses.
- Clear and proportionate – in scope and focused.
- Representative – ensure those likely to be affected have a voice.
- Asks objective questions and present realistic options.
- Ensure that those participating get feedback at the end of the process.

Does the agency's Privacy Impact Assessment map the flow of personal information? (*example from the Office of the Victorian Information Commissioner's Privacy Impact Assessment Guide*)

It is important to describe what personal information is involved in the project and how it will flow through the agency's systems and processes to deliver the output desired by the project.

Clearly mapped information flows will assist agencies to identify privacy risks and impacts.

The OIC would expect to see personal information mapping include:

- what personal information is collected, its source and how it will be collected
- how it will be stored, what safeguards will be in place and who will have access to it
- what the personal information will be used for and by whom
- whether the personal information will be routinely disclosed and if so, to whom will it be given and for what purpose
- how individuals will be able to access and amend their personal information
- how long the information will be retained.

Does the agency's Privacy Impact Assessment identify privacy impacts and risks? (*See OIC Guideline - Privacy impact assessments - risk considerations)*

A privacy risk is a potential adverse event that a particular practice or activity associated with the collection, handling and management of personal information will fail to meet individuals' reasonable expectations of privacy.

It involves considering the cause and consequences of the risk, and the likelihood of it occurring. To identify privacy risks, an agency can check the project's handling of personal information against the Information Privacy Act, for example, the requirement to take all reasonable steps to bind contracted service providers to the privacy principles.

Using a risk matrix helps prioritise risks according to how likely it is that the risk will materialise and the severity of its potential consequence.

Even where an act or practice complies with the Information Privacy Act, individuals may be uncomfortable with their information being involved in the act or practice. Consultation with the community is an effective way to assess whether a project is seen as privacy intrusive.

Does the agency's Privacy Impact Assessment identify options to address privacy risk? (*See OIC Guideline - Privacy impact assessments - risk considerations*)

An agency can minimise privacy risks by:

- implementing physical measures (limiting access, providing lockable storage, reducing the use of hard copy documents)
- implementing technical solutions (auditing systems, managing devices, minimising data collection, passwords)
- implementing privacy positive policies or procedures (training, communication strategies)

Does the agency's Privacy Impact Assessment report on the outcome of the PIA? (*See OIC Guidelines - Privacy impacts assessments - tips for PIA report drafting, PIA report template*)

In finalising a report on the outcome of the PIA for approval by the Project Executive, Steering Committee etc, the report, at a minimum, should:

- describe the information flows involved in the project
- provide a summary of the analysis against the privacy principles to show what the privacy impacts are
- make recommendations to remove or mitigate privacy risks
- set out consultation processes undertaken
- identify whether the PIA should be reviewed during the project.

Does the agency's Privacy Impact Assessment respond to recommendations in the report and implement them? (*See OIC Guideline - Undertaking a Privacy Impact Assessment*)

It is important that actions are taken to implement the recommendations made in the report, and to continue to review and update the PIA, even after the project's completion.

Agencies should document what the Project Executive/Steering Committee/senior management agreed to. That is:

- what recommendations will be implemented
- any recommendations that will not be implemented, and the rationale for this decision.

Publishing the PIA report

Publishing a PIA report and the agency's response demonstrates a commitment to openness and transparency and that the project has been designed with privacy in mind. If detailed information about the project cannot be published due to security or commercial concerns, consider publishing a summary or redacted version of the PIA report.

A PIA report is a living document. It should be revisited and updated if changes to the design of the project create new privacy impacts that were not previously considered.

Similarly, a PIA does not end on delivery of the project. Reassessing the privacy impacts of the system or process after it is in operation, for example when updates are deployed or new features are released, will help ensure that the agency continues to approach privacy as a 'design feature' of its processes and activities.

If applicable, has the agency undertaken an ethical risk assessment of use of artificial intelligence?

If the project involves AI, the agency has considered the privacy risks of AI.

A resource document is the Queensland Government's *Artificial intelligence governance policy*.

While Local governments are **not required** to comply with this policy, as per the *Financial and Performance Management Standard 2019*, see section 9(2)(c) FAA – *Financial Accountability Act 2009,* the policy describes **good practice**.

The policy requires departments and statutory bodies to comply with these requirements:

1. Agencies must use a consistent and evidence-based process which incorporates an ethical framework to evaluate their transparency, accountability, and risk associated with the AI lifecycle
2. Agencies must establish AI governance arrangements based on ISO 38507

The policy refers to FAIRA, the framework to identify risks of AI.

It also refers to the Australian *National framework for the assurance of artificial intelligence in government* and aligns with *Australia's AI Ethics Principles*.

Australia's AI Ethics Principles at a glance

- **Human, societal and environmental wellbeing**: AI systems should benefit individuals, society and the environment.
- **Human-centred values**: AI systems should respect human rights, diversity, and the autonomy of individuals.
- **Fairness**: AI systems should be inclusive and accessible and should not involve or result in unfair discrimination against individuals, communities or groups.
- **Privacy protection and security**: AI systems should respect and uphold privacy rights and data protection and ensure the security of data.
- **Reliability and safety**: AI systems should reliably operate in accordance with their intended purpose.
- **Transparency and explainability**: There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI and can find out when an AI system is engaging with them.

- **Contestability**: When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
- **Accountability**: People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.