DNRME Privacy and Visual Recording Devices and Systems Policy

Last reviewed: 03/04/2019 **CHC/2017/3865**
Version: 1.01

1. Purpose

The object of the *Information Privacy Act 2009* (the IP Act) is to provide for the fair collection and handling in the public sector environment of personal information as well as the general right of access to, and amendment of, personal information in the government's possession and control.

This Policy has been developed to govern the management of visual recording devices and systems where the primary purpose is to fulfil departmental functions where those functions authorise or necessitate the capture of personal information in the form of images. The Policy clarifies our responsibilities and obligations under the IP Act to provide for the appropriate collection, storage, use and disclosure of personal information captured by visual recording devices and systems. A Camera and Visual Recording Systems Guideline has been developed to support the policy and other resources and assistance is available from Privacy Services.

2. Policy

This Policy governs information privacy responsibilities for the use of visual recording devices and systems across the department where the primary purpose is to capture personal information. It is premised on complying with legislative obligations and on respect for the personal information with which the department deals.

The term 'visual recording devices and systems' means all camera technology including closed circuit television (CCTV) systems, hand held (including tablet and smart-phone), body and drone cameras. Generally, a visual recording system encompasses all forms of image recording within a coherent and regulated system. This may encompass individual devices but generally this will only be where they are part of a process or system for managing specific activities.

Resources and assistance in implementing this Policy are available from Privacy Services.

3. Principles

1. The information privacy principles (IPPs) in the IP Act apply to this Policy (summarised at section 7).

2. All areas are required to conduct a needs analysis and risk assessment before purchasing technology with visual recording capacity, if the proposed use poses a high privacy risk (see section 7).

3. Any purchase of devices and systems, which are to be used primarily for the capture of personal information in the form of images, are required to conform to the Department's Record of Procurement Activity (non-routine) process regardless of the procurement threshold.

4. Due consideration must be given to the technical capability of the system, to retention and disposal obligations under the *Public Records Act 2002* (the PR Act), and to the right of access to the information under the *Right to Information Act 2009*.

5. A Privacy Impact Assessment (PIA) must be completed for high risk uses to identify the personal information flows and privacy implications. Advice should be sought from the Privacy Officer as to whether a full PIA is necessary for individual or low risk purchases.

6. A local Procedure, based on the Cameras and Visual Recording Systems Guideline, outlining the purpose for the device or system, detailing the security, storage, use and disclosure of captured images and incorporating a periodic evaluation and review process must be developed prior to activation of any visual recording system.

7. A register of all visual recording systems, and individual devices used for high risk situations, (ie drones used for surveillance of individuals), must be maintained by the department. This is a retrospective requirement.

8. Legal advice should be sought if necessary, for example, on the impact of the *Invasion of Privacy Act 1971* where audio capture for a device or system is proposed.

4. Authority

Information Privacy Act 2009 and Office of the Information Commissioner (OIC) recommendations.

5. Scope

This Policy encompasses all visual recording devices and systems for which the primary purpose is to fulfil departmental functions where personal information is collected and applies to all:

- Permanent, temporary and casual employees, including contractors and consultants (full and part-time)
- Students, trainees and volunteers

This Policy does not cover information collected by visual recording devices and systems from which an individual's identity cannot be ascertained, for example infrastructure or vegetation information captured by a drone or hand-held camera or from individual smart devices not procured for the purpose of recording images for official purposes.

This Policy generally applies only to all new purchases or extensions to systems. However, the recording on a register of systems and individual devices, where they are routinely used for high risk purposes, is retrospective. Individual devices where they are part of a system of use do not need to be individually recorded on the register, only the system or function for which they are used. There is an expectation that the use of current visual recording devices and systems be progressively reviewed.

6. Responsibilities

Director-General is responsible for approving this Policy and departmental compliance with the IP Act.

Deputy Directors-General are responsible for:

- approving the installation of fixed visual recording systems, drone use and the use of hand-held or body cameras, where these pose a high privacy risk
- ensuring that PIAs are developed where necessary as per this policy
- communicating this policy to relevant areas of their division.

Executive Directors (or equivalent) are responsible for:

- approving lower risk uses of hand-held or body cameras
- ensuring that PIAs are developed where necessary as per this policy.

Director, Information and Reporting and the **Principal Governance Officer, Privacy Services (**the **Privacy Officer)** are responsible for:

- providing privacy advice in relation to this Policy
- reviewing PIAs to ensure compliance
- general privacy compliance in accordance with the IP Act
- complaint management in accordance with the Information Privacy Complaint Management Procedure.

Chief Counsel, In-house Legal have prime responsibility for providing legal opinion where requested by executive management on privacy-related issues and may be consulted if necessary, along with the Privacy Officer, for example, on CCTV signage.

Departmental employees are responsible for:

- ensuring their actions and practices do not contravene or are otherwise inconsistent with the privacy principles and the IP Act, including safeguarding personal information and handling it in a professional and responsible manner at all times.
- ensuring all privacy complaints are referred to PS in accordance with the Privacy Complaint Management Procedure (if necessary, through their supervisor or manager).
- ensuring PS are advised of any potential privacy breaches or issues, thus allowing appropriate action to be taken to contain the breach or address the privacy issue.
- alerting PS to any significant proposals that may involve the collection, storage, use and/or disclosure of personal information with respect to this Policy or generally (through their supervisor or manager).
- assisting PS to review systems and investigate privacy complaints as endorsed by their supervisor or manager and/or Executive Director (or equivalent).

7. Definitions and glossary of terms

Personal information: "*Information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."* Essentially, any information that can be linked to an identifiable individual is personal information and is subject to the IP Act.

High Level Risks: High level risks may arise in situations where the department:

- captures large amounts of information
- captures audio (*Invasion of Privacy Act 1971* implications)
- proposes to undertake covert surveillance
- captures any information that could cause harm, embarrassment, damage, or loss to the department or any individual if collected, used, stored or disclosed inappropriately
- proposes to capture information in circumstances where individuals, other than the intended subject of the recording, may be captured without their knowledge or consent.

Greater scrutiny should be applied to personal information that would cause embarrassment, loss or hurt to a person if it was inappropriately dealt with or exposed. Risk levels should be assessed in accordance with the department's risk management process.

IPPs: the Information Privacy Principles. In summary:

Collection IPPs 1-3

- *We may only collect personal information for a lawful purpose that is directly related to our functions and it must not be collected in a way that is unlawful or unfair.*
- *When asking an individual for their personal information we must ensure they are aware of our purpose, our authority and any likely disclosure, that the information is relevant, up to date and complete and that the collection does not intrude to an unreasonable extent upon the personal affairs of the individual.*

Storage and Security IPP 4

- *We must ensure that there are reasonable safeguards against loss, unauthorised access, use, modification and disclosure and any other misuse of the personal information.*

Access and Amendment IPPs 5-7

- *We will take all reasonable steps, unless prohibited, to ensure awareness of the personal information we hold and how individuals can access and amend their personal information.*

Accuracy IPP 8

- *We will take reasonable steps to ensure that any personal information we use is accurate, current and complete.*

Use and Disclosure IPPs 10-11

- *In general, we must use personal information only for the purpose for which it was collected and disclose the information only if the person is reasonably aware of the disclosure or has expressly consented to the disclosure. We may use or disclose the personal information if we seek the approval of the individual prior to use or disclosure or where it is required or authorised by law.*

PR Act: *Public Records Act 2002*
RTI Act: *Right to Information Act 2009*

Visual Recording Device: any individual device which records a visual image from which an individual's identity is apparent or can be reasonably ascertained.

Visual Recording System: all forms of recording within a coherent and regulated system, for example, CCTV systems, from which an individual's identity is apparent. It may include individual visual recording devices where they are part of a process or system for managing specific activities.

8. References

The following references provide guidance and assistance and should be read in conjunction with this Policy:
Bring Your Own Device (BYOD) Policy
Cameras and Visual Recording Systems Guideline (in development)
Capturing and managing surveillance and monitoring records
Code of Conduct for the Queensland Public Service
Information Standard 18 (Information Security)
Information Standard 31 (Retention and Disposal of Public Records)
Information Standard 40 (Recordkeeping)
ISO31000:2009 Risk Management: Principles and guidelines

ICT-as-a-Service risk assessment guideline
Non-routine procurement process
OIC Camera Surveillance and Privacy
OIC Overview of the privacy impact assessment process
Privacy Complaint Management Procedure
Privacy Impact Assessment Toolkit
Risk Management Policy
Standards Australia (AS4806 for CCTV standards)
Use of Internet, Email and Other ICT Facilities and Devices Policy and Procedure

9. Review

This policy will be reviewed within two years of the effective date.

10. Approval

Signed: *B Parker*

Brenda Parker
Deputy Director-General
Business and Corporate Partnerships
Department of Natural Resources, Mines and Energy

Date: 3/04/2019

Keywords

Privacy and Visual Recording Devices and Systems Policy; Privacy; Visual Recording; Devices; Systems; camera; phone