Privacy Policy

Department of Logistics and Infrastructure

Commitment

The Department of Logistics and Infrastructure, (the Department) values and respects the privacy of the members of the public that interact with the agency.

The Department is committed to protecting privacy and ensuring that personal information is collected and handled in a manner that the public should reasonably expect and in accordance with the *Information Act 2002* (NT). Specifically, the Information Privacy Principles, and, where applicable, the Australian Privacy Principles in the *Privacy Act 1988* (Cwth).

Purpose

This policy describes how the Department will collect, use, disclose and manage personal information and maintain the quality and security of personal information.

Scope

This policy applies to all Departmental employees, contractors and agents that collect and handle personal information in the performance of their role.

Information Collected

The Department collects a range of personal information necessary for, or directly related to, the conduct of various functions and activities. This includes, but is not limited to:

- public roads monitoring
- public submissions and community consultations
- urban public and school bus and public transport
- vehicle registration and driver licensing
- remote and urban social housing
- commercial passenger vehicle industry
- road and marine safety, and
- procurement.

The personal information routinely collected to deliver these functions and activities includes:

- an individual's name, date of birth, signature, address and phone number
- photograph / video image or footage
- sensitive information, e.g. criminal record, health or genetic information
- some aspects of biometric information (facial biometric data)
- financial, banking or credit information
- employee record information
- internet protocol (IP) addresses, or
- location information from a mobile device.

Also see the DLI website for more information.

Some of the personal information collected is required by legislation, see Schedule 1 for further information. Other information we collect may indirectly identify a person and is also considered personal information under this policy.

There are limits and additional requirements associated with the collection of sensitive information (i.e. medical records) that requires either the consent of the person, legal authority or other grounds listed in IPP 10.

Information Privacy Principles

The Department is committed to the right of individuals to have their personal information collected, used, disclosed and managed in accordance with the Information Privacy Principles (IPPs).

The IPPs – represented by a ✓ – are set out below and are available online at Schedule 2 the *Information Act 2002*.

Collection of personal information:

The Department will:

- ✓ only collect personal information if it is necessary for the functions or activities of the Department
- ✓ inform individuals of the purpose for collection, any relevant laws requiring the personal information, and the consequences of not providing the information
- ✓ collect directly from the person, if that is reasonable and practicable, and
- ✓ collect in a lawful, fair and not unreasonably intrusive way.

Use and disclosure:

Personal information can be used or disclosed for the purpose for which it was collected. The IPPs limit the use and disclosure for other purposes (known as "secondary purposes").

Use or disclosure for secondary purposes may occur:

- ✓ if the person consents
- ✓ if it is required or authorised by law

Personal information: government information that discloses a person's identity or information from which a person's identity could be reasonably ascertained. It does not include identity information (name) of employees acting in an official capacity.

- ✓ for a purpose related to the primary purpose of collection and where the individual would reasonably expect the use or disclosure to occur, or
- ✓ for law enforcement and some health and safety purposes.

Management of personal information:

The Department will maintain appropriate security and control of personal information to ensure it is stored in a manner that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure. These measures include:

- ✓ ensuring that personal information is accurate, complete and up to date
- ✓ taking all reasonable steps to ensure the information is stored securely
- ✓ protecting personal information from misuse and loss and from unauthorised access, modification or disclosure, and
- ✓ destroying or permanently de-identify personal information if it is no longer needed for any purpose.

General storage and management requirements include:

- All electronic records must be stored and saved with appropriate levels of security and naming conventions that maintain privacy.
- Conversations that involve personal information, should as far as practicable, be carried out in a place and manner which limits being overheard.
- Computer screens, printing and hard copy files must be managed to ensure security and privacy of information.
- IT systems and web platforms administered by the Department will include governance structures and system controls to test, monitor, evaluate and report on privacy compliance and breaches of privacy.
- Staff must use their own individual user profile to log into IT systems. Generic or multiple-user log-in's must be carefully managed and phased out of operation as soon as possible.

Disposal:

The Department will hold personal information only for the appropriate period related to the business practice, legislation or for the historical / cultural context of the function for which the information has been collected.

The Department will take all reasonable steps to destroy or permanently de-identify personal information that is no longer needed for the purpose for which it was obtained.

Access and correction of personal information:

Any information held by the Department about an individual may be accessed by that person in accordance with IPP 6. Staff must take reasonable measures to update or correct personal information upon the request of that person (see Application to Correct Personal Information form). The Department must:

- ✓ inform individuals of the process to access their personal information held by Department, and
- ✓ take reasonable measures to update or correct personal information at the individual's request.

Identifiers, anonymity and trans-border data flow:

There are limits on transferring personal information outside the Territory and the use / disclosure of unique identifying codes (e.g. driver's licence numbers). In line with the IPPs the Department will:

- ✓ not assign or use other agencies' unique identifiers for individuals unless necessary to perform Departmental functions efficiently
- ✓ not transfer personal information outside of the NT unless required / authorised by a law or other IPP exemption, and
- ✓ where practicable, allow persons the option of dealing anonymously with the Department.

Privacy breaches, complaints and reporting:

There are various ways personal information could be compromised, for example sending an email to incorrect recipients. The public can access the Privacy Complaints form and staff may directly report any interference with privacy to Privacy.DLI@nt.gov.au.

Public and internal complaints related to suspected and/or identified privacy breaches must be referred to DIPL Privacy Complaints for action and reporting via Privacy.DLI@nt.gov.au.

The response to public complaints and notifications to the public on suspected and/or identified privacy breaches must also be coordinated through Privacy.DLI@nt.gov.au.

Louise McCormick
Chief Executive
28 October 2024