LECC
Law Enforcement
Conduct Commission

Law Enforcement Conduct Commission Privacy Statement

1. Collecting personal information

We will only collect personal information if:

- it is for a lawful purpose that is directly related to one of our functions; and
- it is reasonably necessary for us to have the information.

By limiting our collection of personal information to only what we reasonably need, it is much easier to comply with our other privacy obligations. When requesting personal information on behalf of the LECC, staff should only ask for information that is reasonably necessary to the task at hand. We will especially avoid collecting sensitive personal information if we do not need it.

We will collect personal information directly from the person unless they have authorised otherwise or, in the case of health information, it would be unreasonable or impractical to obtain the information directly from the individual.

The LECC will not collect personal information by unlawful means. The LECC will not collect personal information that is excessive or intrusive and will ensure that the personal information collected is relevant, accurate, up-to-date, and complete. For example, employment at the LECC is offered only after successful completion of a rigorous probity assessment process. Potential employees are required to provide a range of personal information including declarations and details of financial interests, conflicts, and associates. The vetting documents outline the information required and provide details on the use, storage, and disposal of that information.

When collecting personal information, the LECC will take reasonable steps to tell the person:

- that the LECC is collecting and holding the information;
- what the information will be used for;
- what other organisations (if any) routinely receive this type of information;
- whether the collection of this information is required by law;
- what the consequences will be for the person if they do not provide the information; and
- how they can access their personal information held by us.

Notification is usually provided to individuals through a ‘privacy notice’ at the initial time of collection or as soon as we can afterwards. Privacy notices can be in writing or verbal.

2. Safeguards to protect personal information

We will put in place reasonable security safeguards to protect personal information from

loss, unauthorised access, use, modification, or disclosure, and against all other misuse. We will ensure personal information is stored securely, not kept longer than necessary for lawful purposes, and disposed of appropriately.

We will enable anyone to know, on request to the LECC:

- whether we hold their personal information;
- the nature of the personal information;
- the main purposes for which we use their personal information; and
- their entitlement to access their personal information.

The publication of this Plan promotes accountability and increases the transparency of our information handling practices. This Plan will be accessible on our website and available to download and print.

We will allow people to access their personal information and must do so without excessive delay or expense. We will allow people to update or amend their personal information, to ensure it is accurate, relevant, up-to-date, complete, and not misleading. We will only refuse access or a request to amend personal information where authorised by law, and we will provide written reasons, if requested.

3. Use of personal information

Before using personal information, we will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading. For example, if investigating a workplace grievance, we will give the person the subject of the complaint an opportunity to correct the information relied upon before a final decision is made.

We may use personal information for:

- the primary purpose for which it was collected;
- a directly related secondary purpose within the reasonable expectations of the person;
- another purpose permitted by law, such as where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health; or
- another purpose for which the person has consented.

4. Disclosure of personal information

We may disclose personal information if:

- the disclosure is directly related to the purpose for which the information was collected, and we have no reason to believe that the person concerned would object to the disclosure;
- the person has been made aware in accordance with a privacy notice under s 10 of the PPIP Act that information of the kind in question is usually disclosed to the intended recipient; or
- another purpose if the person has consented.

We can generally only disclose sensitive personal information when the person has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health. We may disclose health information if:

- the person has consent to the disclosure;
- the disclosure is directly related to the purpose for which it was collected, and the individual would reasonably expect us to disclose the information for that purpose; or
- we reasonably believe that the recipient of the information is subject to a law or binding scheme equivalent to the HPPs; or
- we have bound the recipient by contract to privacy obligations equivalent to the HPPs.

We will not transfer personal or health information outside of NSW or to a Commonwealth agency except in limited circumstances permitted by law.

5. Suspected data breaches

Amendments to the PPIP Act have introduced the Mandatory Notification of Data Breach (MNDB) Scheme. An 'eligible data breach' will have occurred where there is unauthorised access to, or disclosure of, personal information that is likely to result in serious harm to an individual. The breach may occur:

- within the LECC; or
- between public sector agencies; or
- by an external person or entity accessing LECC data.

When an eligible data breach is suspected to have occurred, we are required to make all reasonable efforts to immediately contain the data breach and assess whether the data breach is an eligible data breach. Factors that may be considered in this assessment include the sensitivity of the personal information, and the nature of the harm that may occur.

If found to be an eligible data breach, we will notify both the Privacy Commissioner and the individuals affected by the data breach.

Christina Anderson
Chief Executive Officer

29 February 2024