LECC
Law Enforcement
Conduct Commission

1.17 LECC Data Breach Policy

The Law Enforcement Conduct Commission (LECC) is required by s 59ZD of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) to prepare and publish a Data Breach Policy.

In carrying out its functions, the LECC collects personal and health information. The LECC is committed to ensuring the timely identification, assessment, containment, management, notification and prevention of suspected and/or confirmed data breaches in accordance with the PPIP Act.

LECC
Law Enforcement
Conduct Commission

Document Control

Policy title	1.17 Data Breach Policy
Responsible business unit	Corporate Services
Sponsor	Chief Executive Officer
Approval	Executive Committee
Date of approval	November 2023
Security Classification	OFFICIAL
DLM	None
Review period	12 months
Next review	November 2024

Version History

Version	Date	Reason for amendment
V0.1	11 November 2023	Draft document
V1.0	28 November 2023	Approved for publication

Printed copies and e-copies on personal drives may not be up to date.
Check the LECC website to ensure you have the latest version of this document.

LECC
Law Enforcement
Conduct Commission

Contents

LECC
Law Enforcement
Conduct Commission

1. Definitions

Assessor	The Employee appointed to carry out the assessment about whether the data breach is, or there are reasonable grounds to believe the data breach is, an *eligible data breach*.
CEO	Chief Executive Officer
LECC	Law Enforcement Conduct Commission.
Employees / Officer / Staff	Persons working with or on behalf of the LECC, including ongoing, temporary or term-basis employees and senior executives.
Collection	The way in which the LECC acquires personal or health information, including written or online form, a verbal conversation, a voice recording or photograph/image.
Eligible data breach	Occurs when there is unauthorised access, disclosure, or loss of personal information held by the LECC and a reasonable person would conclude that that the access or disclosure of that personal information would be likely to result in serious harm to an individual to whom the information relates. See s 59D of the PPIP Act for the full definition.
Health information	Information or opinion about a person's physical or mental health or disability, or information provided or generated in the delivery of a health service. See s 6 of the HRIP Act for the full definition.
Personal information	Information or opinion that identifies or could reasonably identify an individual. See s 4 of the PPIP Act for the full definition.
Privacy principles	The Information Protection Principles set out in Division 1, Part 2 of the PPIP Act and the Health Principles set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Lawful exemptions are provided.

2. About the LECC

The LECC was established in 2017 as a permanent independent investigative commission to provide oversight of the NSW Police Force and NSW Crime Commission.

The LECC strengthens law enforcement integrity, by preventing, detecting and investigating misconduct and maladministration within law enforcement in NSW. The LECC does this by detecting and investigating misconduct and corruption, and overseeing complaint handling.

The LECC also aims to understand and assist in the prevention of officer misconduct.

More detailed information about the role and functions of the LECC can be obtained by visiting the LECC website at: *www.lecc.nsw.gov.au*.

3. Introduction to the Data Breach Policy

Part 6A of the PPIP Act establishes the NSW Mandatory Notification of Data Breach (MNDB) Scheme.

The MNDB Scheme requires every NSW public sector agency bound by the PPIP Act to:

- prepare and publish a Data Breach Policy (DBP) for managing and responding to data breaches.
- notify the Privacy Commissioner and affected individuals of eligible data breaches.
- establish, maintain, and publish a public register of eligible data breaches.
- establish and maintain an internal register of eligible data breaches.

4. Purpose

This Policy sets out how the LECC will respond to a suspected or confirmed data breach involving personal information.

The Policy sets out:

- the roles and responsibility of LECC staff in relation to identifying, reporting, assessing, and managing a breach.
- what an eligible data breach is under the PPIP Act.
- the steps the LECC will follow when a data breach occurs.
- the systems and processes in place at the LECC to prevent data breaches.

5. Roles and responsibilities

5.1 Employees

All LECC employees are required to comply with:

- the PPIP Act.
- the HRIP Act.
- the LECC's Privacy Management Plan.
- this DBP.

All LECC employees must immediately notify their manager after becoming aware of a suspected or confirmed data breach in accordance with this policy.

5.2 Contractors, Consultants, and Third-party Service Providers

All LECC contractors, consultants and third-party service providers are required to:

- comply with this DBP.
- immediately notify their LECC contact after becoming aware of a suspected or confirmed data breach in accordance with this policy.

5.3 Managers and Directors

Managers and Directors are responsible for ensuring that:

- their staff are aware of and understand their obligations under the PPIP and HRIP Acts.
- their staff comply with this DBP and the LECC's Privacy Management Plan.
- they notify the Chief Executive Officer (CEO) of any suspected or confirmed data breach within one business day after receiving notice from their staff, or becoming aware of, a suspected or confirmed data breach.

5.4 Executive

The Executive is responsible for:

- approving the DBP**.**
- ensuring that the annual review of this **DBP** is completed.

5.5 CEO

The CEO is responsible for implementing this Policy, appointing and overseeing the Assessor, and causing all notifications and actions for eligible data breaches to be completed.

5.6 The Appointed Assessor

The Assessor is responsible for assessing and investigating data breaches, preparing a Report for the CEO, and completing the Post Incident Review and preparing a Post Incident Review Report.

6. Scope

This Policy applies to all LECC employees, contractors, consultants, and third-party service providers and covers all personal information and personal health information collected, received, and held by the LECC.

7. Key concepts and definitions

7.1 What is a data breach?

A 'data breach' occurs when personal information held by an agency (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

This can involve:

- disclosure of personal information external to the LECC, or publicly.
- unauthorised access to personal information by a LECC employee.
- unauthorised sharing of personal information between teams within the LECC.

It may occur due to:

- malicious or criminal cyber attack/inicdent.
- system failure.
- human error.
- Loss/theft of data or equipment.
- employee misconduct.

7.2 What is 'personal information'?

'personal information' for the purposes of the MNDB Scheme includes both 'personal information' as defined in section 4 of the PPIP Act and 'health information', as defined in section 6 of the Health Records and Information Privacy Act 2002 (HRIP Act). Therefore 'personal information' means:

- any information or opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion; and
- any information about an individual's physical or mental health, disability, and information connected to the provision of a health service.

7.3 What is 'serious harm'?

The term 'serious harm' is not defined in the PPIP Act. The Information Privacy Commission has provided some information on this, noting that:

Serious harm occurs where the harm arising from the data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance, or inconvenience.

Harms that can arise as the result of a data breach are context-specific and will vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk.
- the level of sensitivity of the personal information accessed, disclosed, or lost.
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach.
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm).
- the circumstances in which the breach occurred.
- actions taken by the agency to reduce the risk of harm following the breach.

Harm to an individual includes physical harm; economic, financial, or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the LECC's position would identify as a possible outcome of the data breach.

8. What is an Eligible Data Breach?

The MNDB Scheme applies only where an 'eligible data breach' has occurred. A data breach is an 'eligible data breach' where the below two tests are satisfied.

First, there is:

- an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information.

AND

Secondly:

- a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

The scheme does not apply to data breaches that do not involve personal information, or to breaches that are not likely to result in serious harm to an individual.

LECC
Law Enforcement
Conduct Commission

9. What happens if it is not an Eligible Data Breach?

If the data breach does not satisfy the test in paragraph 8 above, then it is not considered an 'eligible data breach', and the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is not triggered.

This means the LECC is not required to notify individuals or the Privacy Commissioner of the breach.

However, the LECC will still take action to respond to the data breach, minimise potential harm, and mitigate any risk of future breaches. This may include providing a voluntary notification to individuals impacted by the breach where appropriate.

10. What happens if it is an Eligible Data Breach?

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered.

There are four elements of the notification process:

1. The CEO, as the head of the LECC, must immediately notify the Privacy Commissioner after an eligible data breach is identified using the approved *form*.

2. Determine whether an exemption applies: If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, the LECC may not be required to notify affected individuals.[1]

3. Notify affected individuals (unless an exemption applies) or their authorised representative as soon as reasonably practicable.

4. Provide further information to the Privacy Commissioner. The LECC may be required to provide additional information to the Privacy Commissioner, if they have been unable to provide complete information in their initial notification, if they have made a public notification, or if they are relying on an exemption.

Notification should be undertaken promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves.

The MNDB Scheme requires an agency to take reasonable steps to notify affected individuals as soon as practicable.

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as practical issues such as having contact details for the affected individuals/organisations.

[1] The IPC has produced guidance to agencies on exemptions from notification. This can be reviewed *here*.

Where all individuals affected by an eligible data breach cannot be notified, the LECC will consider issuing a public notification on its website.

11. How the LECC will respond to a Data Breach

When a data breach is reported by a staff member to their manager, the manager must as soon as practicable, but no later than one business day, notify the LECC's CEO.

When a data breach is reported by a contractor or third-party to any LECC staff member, that staff member must as soon as practicable notify the LECC's CEO

The CEO must be informed of any data breach to ensure the application of this policy, including making notifications to the Privacy Commissioner for eligible data breaches and affected individuals.

There are five key steps required in responding to a data breach. They are:

- initial report and triage.
- contain the breach or suspected breach.
- assess the breach and implement any additional actions identified to mitigate risks.
- Notify the appropriate parties (if applicable).
- review (post incident).

Each step is set out in further detail below. The first four steps should be carried out concurrently where possible.

The fifth and final step provides recommendations for longer-term solutions and prevention strategies.

11.1 Initial report and triage

Once the CEO is notified of a suspected or confirmed data breach, the CEO will consider the circumstances and promptly appoint an Assessor.

Alternatively, the CEO may also consider convening a Data Breach Response Team, where a data breach involves highly sensitive information, has a high risk of harm to individuals and affects a significant number of individuals and/or organisations.

11.2 Contain the breach or suspected breach

Containing the breach is to be prioritised by the LECC.

All necessary steps possible must be taken to contain the breach and minimise any resulting damage.

For example, steps should be taken to:

- recover the personal information.

- shut down the system that has been breached.
- suspend the activity that led to the breach.
- revoke or change access codes or passwords.

If a third-party is in possession of the data and declines to return it, it may be necessary for the LECC to seek legal or other advice on what action can be taken to recover the data. When recovering data, the LECC will make sure that copies have not been made by a third party or, if they have, that all copies are recovered. This can include receiving written confirmation from a third-party that the copy of the data that they received in error, has been permanently deleted.

11.3 Assess the breach and mitigate risks

To determine what other steps are needed, the appointed Assessor will provide a report expeditiously[2] to the CEO, setting out:

- their assessment of the incident. In assessing the incident, the Assessor must consider:
    - who is affected by the breach, and whether any of the individuals have personal circumstances which may put them at particular risk of harm.
    - the type or types of personal information involved in the data breach.
    - the circumstances of the data breach, including its cause and extent.
    - the nature of the foreseeable harm to affected individuals/organisations, and if this harm can be removed through remedial action.[3]
    - Have regard to the guidelines prepared by the Privacy Commissioner, about the process for carrying out an assessment. They can be reviewed *here*.
- whether it is an eligible data breach under the MNDB Scheme (see paragraph 8 above)[4]. If so, the draft report should further detail what notifications need to be made and identify which registers need to be updated.
- an action plan, which details any further steps to be taken to prevent harm and/or reduce any harm already done.

The CEO will then decide if an eligible data breach has occurred, or if there are reasonable grounds to believe the data breach is an eligible data breach.

The CEO will be responsible for causing the implementation of the proposed actions and recommendations.

[2] This is subject to a statutory time frame of 30 days. See section 59E of the PPIP Act.
[3] Section 59H of the PPIP Act sets out factors the Assessor may consider.
[4] The IPC has developed a Data Breach Self-assessment Tool for Mandatory Notification of Data Breach to assist NSW public sector agencies to determine whether a data breach is an eligible data breach under the MNDB Scheme. It is recommended that the Assessor uses this tool to assist with this step. It can be accessed *here*.

11.4 Notify the appropriate parties (if applicable)

If an eligible data breach has occurred, the notification process under Division 3 of the MNDB Scheme (Part 6A of the PPIP Act) is triggered (see paragraph 10 above).

Privacy Commissioner

The CEO must ensure that the Mandatory Data Breach Reporting Form is appropriately completed and provided to the Privacy Commission as required by s 59M of the PPIP Act.

Affected Individuals/organisations

If an exemption does not apply, the LECC must notify all affected individuals/organisations or their authorised representative as soon as practicable. The notification:

- should be done directly. That is by telephone, letter, email or in person.
- must include the information as set out in s 59O of the PPIP Act. That is:
    - the date the breach occurred.
    - a description of the breach.
    - how the breach occurred.
    - the type of breach that occurred.
    - the personal information included in the breach.
    - the amount of time the personal information was disclosed for.
    - actions that have been taken or are planned to secure the information, or to control and mitigate the harm.
    - recommendations about the steps an individual should take in response to the breach.
    - information about complaints and reviews of agency conduct.
    - the name of the agencies that were subject to the breach.
    - contact details for the agency subject to the breach or the nominated person to contact about the breach.

A public notice in a newspaper, or a media release by the LECC will only occur where the contact information of affected individuals/organisations is unknown, or where direct notification is prohibitively expensive, could cause further harm, or is not reasonably practicable.[5]

A record of any public notification of a data breach will be published on the LECC's website and recorded on the Public Data Breach Register for a period of 12 months (see paragraph 13 below).

Other Notifications

The LECC will also consider whether notification of external stakeholders (in addition to the Privacy Commissioner) is required by contract or by other laws or administrative arrangements where a data breach occurs.

[5] See s 59N and s 59P of the PPIP Act for further guidance in relation to public notifications.

11.5 Review (post incident)

Once the incident response is finalised and any applicable notifications complete, the Assessor will be responsible for conducting a Post Incident Review and preparing a Post Incident Review Report.

The Post Incident Review Report should:

- further investigate the circumstances of the breach to determine all relevant causes.
- Make recommendations about what short or long-term measures could be taken to prevent any reoccurrence.
- reflect on any improvements that could be made to this policy, or action taken by the LECC, to improve our response to a future data breach.

The Post Incident Review Report must be sent to the CEO for their consideration and comment.

12. Systems and processes

The LECC has established a range of systems and processes for preventing and managing data breaches. This includes:

1. Ensuing that all LECC staff complete mandatory cyber security training.

2. Ensuring that LECC information is held on Information Communication and Technology facilities in a way that maintains the confidentiality, integrity and availability of the information. Further detailed information about the LECC's storage and security of personal information is set out in our LECC Privacy Management Plan.

3. Internal LECC policies and procedures concerning the manner in which information is dealt with. This included the following:
    - The Code of Ethics and Conduct sets out the general standards of conduct expected of LECC officers, including the use and protection of personal information.
    - The Employee Induction Procedure provides procedures which ensure all officers newly employed at the LECC are notified of internal policies and procedures, including responsibilities regarding the confidentiality of information.
    - The IT Conditions of Use Policy identifies the principles for proper use of the LECC Information Communication and Technology facilities and systems, along with the responsibilities of all employees of the LECC.
    - The Information Security Policy provides guidelines to ensure that information within the LECC is treated with the appropriate levels of security.
    - The Records Management Policy provides for the management of records within the LECC including the capture, creation, control and maintenance of electronic and physical records.
    - The Security Vetting and Clearance Policy and Procedure establishes the

guidelines for the security clearance and pre-employment checks to be undertaken in respect of all staff and contractors prior to commencement of duties at the LECC. This includes the way personal information may be collected and dealt with for such purposes.

- The Physical Security (Personnel & Premises) Procedure outlines procedures to ensure the security of the LECCs working environment, including maintaining the physical security of confidential information.

4. All external contractors and consultants engaged by the LECC are notified of relevant policies and procedures when engaged by the LECC.

5. Presentations and training have been provided to the LECC staff on the MNDB Scheme

13. Public Data Breach Register

Section 59P of PPIP Act requires the LECC to maintain a Public Notification Register.

The LECC will maintain a public notification register on the LECC website. This will be used to provide public notifications of eligible data breaches where the LECC is unable to notify, or it is not reasonably practicable to notify, affected individuals.

The LECC's public data breach register can be viewed here.

14. Internal Data Breach Register

The CEO will maintain an internal register of all eligible data breaches impacting the LECC.

15. Privacy complaints and applications for an internal review

A person who is dissatisfied about the manner in which the LECC has dealt with their personal information can make a complaint to the LECC in writing. The LECC will consider the issues raised by the complainant and respond in writing as soon as is reasonably possible (but not later than 60 days after receipt of the complaint). Complaints should be addressed to the CEO at the address below.

Requests for review must be made in writing and include a postal address by which the LECC can send a response. The request should be addressed to:

The Chief Executive Officer
Law Enforcement Conduct
Commission GPO Box 3880
SYDNEY NSW 2000

Applications for review should generally be made within six months of the person becoming aware of the conduct which forms the subject of the application. The LECC may decline to deal with applications which are made after this time.

Upon receipt of any application for review, the LECC will notify the Privacy Commissioner of the application as per s 54 of the PPIP Act. The LECC will keep the Privacy Commissioner informed of the progress of the application and the ultimate outcome.

All requests for review and the LECC's responses to such requests are to be recorded on the LECC's internal document management systems.

The LECC will process the application for review in accordance with Part 5 of the PPIP Act.

The LECC will acknowledge receipt of a request for internal review within seven days and complete the review within 60 days. It is noted, that if any application for review is not completed within 60 days from the day of its receipt, the applicant is entitled to make an application under s 55 of the PPIP Act to the Civil and Administrative Decisions Tribunal (NCAT) for a review of the relevant conduct. Further information about making an application to the tribunal can be found on their website *www.ncat.nsw.gov.au*.

As soon as possible after the completion of the review (but not longer than 14 days), the LECC will notify the applicant in writing of the outcome of the review, the actions proposed to be taken by the LECC (and the reasons for those actions) and the rights of the applicant, including the right to have those findings and the proposed action reviewed by the NCAT.

16. Complaints to the Privacy Commissioner

An individual can make a compliant to the Privacy Commissioner about a breach of their privacy by the LECC. More information about the role of the Information and Privacy Commission (IPC) in handling complaints can be found on the IPC website *www.ipc.nsw.gov.au*.

17. Other legislative requirements

LECC officers should be aware that the obligations under the PPIP Act and HRIP Act may be only some of those applicable to the information they are dealing with and a number of other pieces of legislation regulate the manner in which information is dealt with.

Section 180 of the LECC Act is of particular significance and is applicable to both current and former officers of the LECC. Section 180(2) of the LECC Act holds that a person to whom the section applies must not:

> *(2) ... directly or indirectly, except for the purposes of this Act or otherwise in connection with the exercise of the person's functions under this Act -*
>
> *(a) make a record of any information, or*

(b) disclose or communicate to any person any information,

being information acquired by the person by reason of, or in the course of, the exercise of the person's functions under this Act.

Other legislation that may be relevant to the treatment of personal information includes:

- *Government Information (Public Access) Act 2009*
- *Health Records and Information Privacy Act 2002*
- *Surveillance Devices Act 2007*
- *Workplace Surveillance Act 2005*
- *State Records Act 1998*
- *Crimes Act 1900*
- *Criminal Records Act 1991*
- *Public Interest Disclosures Act 1994*
- *Telecommunications (Interception and Access) (New South Wales) Act 1987*
- *Telecommunications (Interception and Access) Act 1979* (Cth)

18. Related Guidance

The Information and Privacy Commission has produced useful guidance that may further assist the LECC to respond to a data breach. These guides include:

- *Guide to managing data breaches in accordance with the PPIP Act.*
- *Guide to Preparing a Data Breach Policy*
- *Fact Sheet - Mandatory Notification of Data Breach Scheme: Exemptions from notification requirements*
- *Guidelines on the assessment of data breaches under Part 6A of the PPIP Act*