BAR ASSOCIATION OF QUEENSLAND

DATA BREACH POLICY

1. Introduction

The Bar Association of Queensland (**the Association**) is committed to upholding the privacy and confidentiality of the personal information it holds. In fulfilling its statutory functions under the *Legal Profession Act 2007* (Qld) (**the LPA**), the Association primarily handles personal information necessary for barristers to obtain practising certificates and to carry out its functions under the LPA.

This Data Breach Policy details the Association's approach to managing suspected and actual data breaches. It is designed to ensure strict compliance with the *Information Privacy Act 2009* (Qld) (**the IP Act**) and the *Right to Information Act 2009* (Qld) (**the RTI Act**), as well as other pertinent legislative and regulatory requirements.

2. Purpose

The objectives of this policy are to:

- Establish a clear, structured, and compliant framework for the identification, assessment, containment, management, and response to any suspected or actual data breaches.
- Minimise the potential impact of data breaches on affected individuals and the Association's operations and reputation.
- Ensure full compliance with all relevant statutory obligations, particularly the mandatory data breach notification requirements under the IP Act, effective from 1 July 2025.
- Foster and reinforce a strong culture of privacy, data protection, and accountability across all levels of the Association.

3. Scope

This policy applies universally to all individuals associated with the Bar Association of Queensland who may have access to, or be responsible for, personal or confidential information held by the Association. This includes, but is not limited to:

- All Association staff (permanent, temporary, and casual).
- All contractors, consultants, and volunteers working on behalf of the Association.
- Any third-party service providers (including IT support) with access to Association data, regardless of where the information is stored (e.g., on Association premises, third-party cloud services) or its format (electronic or physical).

4. Definitions

For the purposes of this policy, the following definitions apply:

- **Data Breach:** An incident involving unauthorised access to, or unauthorised disclosure of, personal information held by the Association; or a loss of personal information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.
- **Eligible Data Breach:** A data breach in relation to personal information held by the Association where:
    1. There is unauthorised access to, or unauthorised disclosure of, personal information held by the Association; or personal information held by the Association is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; AND
    2. A reasonable person would conclude that the unauthorised access to, or disclosure of, the information (or the unauthorised access or disclosure that is likely to occur as a result of the loss) is likely to result in serious harm to any of the individuals to whom the personal information relates.
- **Personal Information:** As defined in section 12 of the *Information Privacy Act 2009* (Qld), 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.
- **Serious Harm:** Encompasses significant detrimental effects that could result from a data breach, including but not limited to: identity theft, significant financial loss, threats to physical safety, serious psychological harm (e.g., humiliation, severe distress), or serious harm to an individual's reputation. The assessment of serious harm considers various factors, including the sensitivity of the information, the security measures in place, and the nature of the individuals affected.
- **Chief Executive:** The designated primary individual responsible for the oversight and implementation of this Data Breach Policy, acting as the Association's Data Breach Coordinator.
- **Legal Department:** The secondary responsible party, providing critical support and expertise in managing data breaches, particularly concerning legal obligations and communications.
- **Third-Party IT Support:** External providers engaged by the Association to deliver IT infrastructure, security services, and technical support.

5. Roles and Responsibilities

The effective management of data breaches requires a coordinated effort, with clear lines of responsibility:

- **Chief Executive – Primary Responsibility:**
    - Serves as the Association's Data Breach Coordinator, holding overall accountability for the development, implementation, and adherence to this policy.
    - Makes the final determination on whether a data breach constitutes an Eligible Data Breach and on all aspects of notification to affected individuals and the OIC Queensland.
    - Oversees and approves the Association's detailed Data Breach Response Plan.
    - Ensures adequate human, financial, and technological resources are allocated to data breach prevention and response.
    - Liaises with relevant external bodies (e.g., LSC, Queensland Police Service, regulatory authorities) as necessary.
    - Leads the post-breach review and ensures implementation of corrective actions.
- **Legal Department – Secondary Responsibility:**
    - Provides expert legal advice on the interpretation and application of privacy legislation (IP Act, RTI Act), particularly concerning data breach assessments, serious harm determinations, and notification obligations.
    - Assists the Chief Executive in conducting thorough assessments of suspected data breaches.
    - Drafts and reviews all internal and external communications related to data breaches, ensuring accuracy, clarity, and legal compliance.
    - Contributes to the development and refinement of the Data Breach Response Plan and post-breach improvement strategies.
- **All Association Staff:**
    - Are personally responsible for understanding, complying with, and actively promoting this policy and all related data security procedures.
    - Must immediately report any suspected data breach, no matter how minor, to the Chief Executive upon discovery.

- Are required to participate in regular privacy and data security training provided by the Association.
- Must handle all personal and confidential information in accordance with Association policies and legislative requirements.

- **Third-Party IT Support:**
  - Must operate in strict accordance with their contractual obligations regarding data security, privacy, and incident response.
  - Are required to immediately notify the Chief Executive of any suspected or confirmed data breach impacting Association systems or data for which they are responsible.
  - Will provide technical assistance in containing, investigating, and remediating data breaches, as directed by the Chief Executive.
  - Must cooperate fully with Association investigations and adhere to all Association security protocols.

6. Data Breach Response Plan (Key Stages)

This section provides an overview of the Association's phased approach to managing data breaches.

6.1. Preparation and Prevention

Proactive measures are fundamental to minimising data breach risks:

- **Data Minimisation:** the Association will collect and retain only the personal information strictly necessary for its legislated functions, particularly under the *Legal Profession Act 2007* (Qld).
- **Robust Security Measures:** implementation and continuous maintenance of appropriate technical and organisational security controls to protect personal information. This includes:
  - **Access Controls:** restricting access to personal information on a "need-to-know" basis.
  - **Encryption:** encrypting sensitive data at rest and in transit where appropriate.
  - **Firewalls and Intrusion Detection:** deploying and maintaining network security defences.
  - **Secure Storage:** ensuring physical and electronic records are stored securely, including backup and recovery procedures.

- **Secure Disposal:** implementing processes for the secure and irreversible destruction of personal information when it is no longer required.

- **Staff Training:** regular training for all staff on privacy principles, data handling best practices, and their roles in data breach detection and reporting.
- **Third-Party Contractual Obligations:** ensuring all contracts with third-party service providers (especially IT support) explicitly detail their data security obligations, incident reporting procedures, and compliance with Queensland privacy laws.
- **Integrated Incident Response:** maintaining an overarching IT security incident response plan that integrates seamlessly with this Data Breach Policy.
- **Internal Data Breach Register:** establishing and maintaining a secure, confidential register to document all data breaches (suspected and confirmed), as required by the IP Act.
- **Policy Publication:** this Data Breach Policy will be publicly accessible on the Association website, as required by section 73 of the IP Act (Qld).

6.2. Detection and Containment (Immediate Action)

Upon becoming aware of a suspected data breach, immediate action is critical to limit potential harm:

- **Prompt Reporting:** any individual who suspects or discovers a data breach must immediately report it to the Chief Executive. Delays can significantly exacerbate the impact.
- **Initial Triage and Assessment:** the Chief Executive, involving Third-Party IT Support if technical aspects are involved, will perform an initial assessment to understand:
    - what information is potentially compromised?
    - when did the breach occur, and how was it discovered?
    - who are the potentially affected individuals?
    - what is the apparent cause of the breach (e.g., human error, system vulnerability, malicious attack)?
- **Containment Measures:** implementing immediate steps to prevent further compromise of information and mitigate ongoing harm. This may include:
    - isolating affected systems or network segments.
    - suspending or changing access credentials for compromised accounts.
    - temporarily taking affected systems offline.

- recalling or retracting misdirected communications (e.g., emails sent to incorrect recipients).
- securing physical locations or documents.
- initiating data recovery procedures if data loss has occurred.

6.3. Assessment (Within 30 Days for Suspected Eligible Data Breaches)

Following containment, a thorough investigation and assessment are conducted to determine if the breach is an Eligible Data Breach:

- **Comprehensive Investigation:** gather all relevant facts about the incident, including:
  - the exact type and sensitivity of the personal information involved (e.g., publicly available practising certificate details vs. highly confidential LSC investigation material).
  - the volume of data and the number of individuals affected.
  - the identity and characteristics of the unauthorised recipient (if any).
  - the duration and scope of the breach.
  - any remedial action taken to reduce the likelihood of harm.
- **Serious Harm Determination:** the Chief Executive, in close consultation with the Legal Department, will assess whether the breach is **likely to result in serious harm** to any affected individual. This involves a rigorous analysis of the factors outlined in the IP Act, considering the unique context of the Association's data holdings (e.g., the potential for identity theft from combined practising certificate data, or significant reputational/professional harm from confidential investigation details).
- **Documentation:** all findings, assessments, and decisions during this phase, including the rationale for determining whether it is an Eligible Data Breach (or not), will be meticulously documented in the internal Data Breach Register. The assessment process must be completed within 30 days of becoming aware of reasonable grounds to suspect an Eligible Data Breach.

6.4. Notification (If Eligible Data Breach)

If the assessment concludes there are reasonable grounds to believe an Eligible Data Breach has occurred, the Association will promptly undertake notification, unless an exemption applies.

- **Notification to the Office of the Information Commissioner (OIC) Queensland:**
  - The Chief Executive will notify the OIC Queensland as soon as practicable after becoming aware of the Eligible Data Breach, typically within 72 hours of forming a reasonable belief that an Eligible Data Breach has occurred.

- The notification will be in the form of a statement that includes:
    - the identity and contact details of the Bar Association of Queensland.
    - a clear description of the Eligible Data Breach.
    - the particular kind or kinds of personal information concerned.
    - recommendations about the steps that individuals should take in response to the Eligible Data Breach.
- Updates will be provided to the OIC if further information becomes available.

- **Notification to Affected Individuals:**
    - The Chief Executive will notify each affected individual whose personal information is part of the Eligible Data Breach as soon as practicable.
    - The notification will be direct where reasonably practicable (e.g., via email, letter, or phone call).
    - The notification to individuals will contain:
        - the Association's identity and contact details.
        - a description of the breach.
        - the types of personal information involved.
        - practical steps the individual can take to mitigate potential harm.
        - information on how to contact the Association for further assistance or information.
    - If direct notification is not reasonably practicable (e.g., due to the number of affected individuals or unknown contact details), the Association will publish a statement on its website and take reasonable steps to publicise the notification (e.g., through relevant professional channels or media).
- **Specific Considerations for Confidential Investigation Information:** in cases involving highly sensitive confidential information related to LSC referrals or disciplinary investigations, the Chief Executive will consult closely with the Legal Department and the LSC (where appropriate) to determine the most responsible and effective notification strategy, carefully balancing transparency with the need to protect the integrity of ongoing investigations or the safety of individuals. Exemptions from notification under the IP Act will be carefully considered where applicable.

6.5. Review and Improvement

Every data breach, regardless of its severity or whether it constitutes an Eligible Data Breach, will be followed by a comprehensive review to foster continuous improvement.

- **Post-Breach Analysis:** the Chief Executive, with the Legal Department and relevant IT personnel, will conduct a thorough review to:
    - identify the root cause(s) of the breach.
    - evaluate the effectiveness of the Association's response, including containment, assessment, and notification processes.
    - identify any gaps in policies, procedures, or security controls.
- **Corrective Actions:** implement necessary and proportionate remedial measures to prevent recurrence and enhance overall data security. This may include:
    - system upgrades or patches.
    - refinements to access controls.
    - updates to training modules.
    - revisions to internal procedures.
- **Documentation and Lessons Learned:** the outcomes of the review, including all corrective actions, will be documented in the internal Data Breach Register. Lessons learned will be disseminated to relevant staff and incorporated into future training.
- **Policy and Plan Review:** this Data Breach Policy and the detailed Data Breach Response Plan will be formally reviewed and updated at least annually, or more frequently if there are significant changes in legislation, technology, Association operations, or in response to a major data breach incident.

7. Data Breach Register

The Association will maintain a secure, internal Data Breach Register. This register serves as a critical record-keeping tool, capturing details of all suspected and confirmed data breaches, regardless of whether they are deemed Eligible Data Breaches. The register will include, but not be limited to:

- date and time the breach was discovered.
- a comprehensive description of the incident (what happened, how, the scope, and the types of data involved).
- the initial assessment and determination of whether it is an Eligible Data Breach (with rationale).

- details of all containment and investigation actions taken.
- decisions regarding notification (to OIC, affected individuals, and any exemptions applied).
- dates and methods of notification.
- summary of serious harm assessment (if applicable).
- identified root causes and contributing factors.
- lessons learned and a record of all corrective and preventative actions implemented.

8. Training and Awareness

To ensure the effectiveness of this policy, the Association is committed to ongoing training and awareness initiatives:

- **Mandatory Training:** all Association staff members will undergo privacy and data security training upon commencement and annually thereafter. This training will specifically cover:
    - their individual and collective responsibilities under the IP Act and this policy.
    - practical guidance on identifying, reporting, and responding to suspected data breaches.
    - best practices for secure information handling, including data minimisation, secure storage, and access control.
- **Regular Communications:** periodic reminders and updates will be circulated to reinforce data security awareness and highlight emerging threats.

9. Policy Review

This Data Breach Policy will be formally reviewed by the Chief Executive Officer and the Legal Department at least annually. Reviews will also be triggered by:

- Significant changes to privacy legislation (e.g., IP Act, RTI Act).
- Changes in the Association's functions, IT systems, or data handling practices.
- Lessons learned from internal or external data breaches.
- Guidance or recommendations from the OIC Queensland or other relevant authorities.

10. Related Documents

This policy should be read in conjunction with, and is supported by, the following Association documents and legislative instruments:

- Association Privacy Policy
- *Information Privacy Act 2009* (Qld)

- *Right to Information Act 2009* (Qld)
- *Legal Profession Act 2007* (Qld)
- Guidelines and resources published by the Office of the Information Commissioner Queensland (OIC).

Approved by:

Kelsey Rissman

Chief Executive Officer

Bar Association of Queensland

Date of Approval: 26 June 2025

Date of Next Review: 26 June 2026