BA Data Breach Response Plan

Date adopted by *BA* Board 11th August 2018

Date Policy Effective 11th August 2018

BA Limited (ACN: 072 484 998) trading as Basketball Australia

BASKETBALL AUSTRALIA LIMITED

DATA BREACH RESPONSE PLAN

BACKGROUND

1. Basketball Australia (ABN 57 072 484 998) (**Basketball Australia**, **we** or **us**) collects, holds, uses and discloses personal information relating to various individuals in the course of operating the peak body of basketball in Australia.

2. We are bound by the provisions of the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APP**) in our collection, security, storage, use and disclosure of personal information.

3. This Data Breach Response Plan sets out the procedures to be followed by all staff employed by Basketball Australia in the event that we experience a data breach, or suspect that a data breach has occurred. This policy also applies to all contractors, students, volunteers and agency personnel engaged by Basketball Australia, as well as external organisations who have been granted access to Basketball Australia's Information and Communication Technology infrastructure or data. References in this policy to an "employee" include all of the above entities.

WHY DO WE NEED A RESPONSE PLAN?

4. This Data Breach Response Plan is a tool for managing and mitigating the impact of a data breach. The faster we respond to a breach, the more likely we are to effectively limit any negative consequences resulting from the breach.

5. Also, there are now laws which require mandatory notification of "eligible data breaches".

6. Failing to implement adequate information security and failing to notify the Australian Information Commission (**Commissioner**) and affected individuals of "eligible data breaches" can lead to penalties of up to $2.1 million under the Privacy Act.

WHAT IS A DATA BREACH?

7. A data breach occurs when there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information.

8. "Personal information" is information about an identified individual, or an individual who is reasonably identifiable.

9. A data breach may be caused by malicious action (by an internal or external party), human error, or a failure in information handling or security systems. Examples of data breaches include:

    (a) loss or theft of physical devices (such as laptops, smartphones, storage devices);

    (b) paper records stolen from offices, archives, insecure recycling or garbage bins;

    (c) employees accessing or disclosing personal information outside of the requirements or authorisation of their employment;

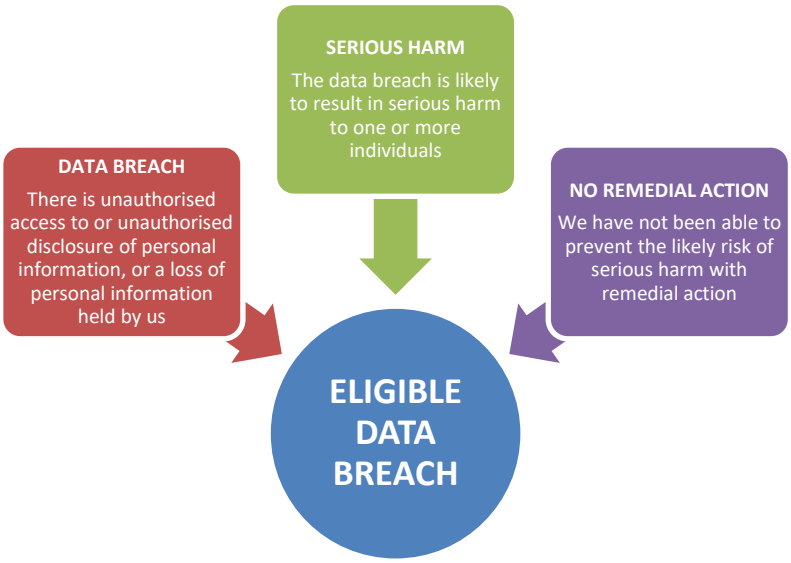
(d) inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person;

(e) databases containing personal information (eg. The Basketball Network) being hacked into or otherwise illegally accessed by individuals outside of Basketball Australia; and

(f) disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

REPORTABLE DATA BREACHES

10. Not all data breaches are notifiable. Under the Privacy Act, we are required to notify particular individuals and the Commissioner about ***eligible*** data breaches. A data breach is an "eligible data breach" where "a reasonable person would conclude that there is a ***likely*** risk of ***serious harm*** to any of the affected individuals as a result of the unauthorised access or unauthorised disclosure".



WHAT IS SERIOUS HARM?

11. "Serious harm" is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. Examples of harm include:

(a) significant financial loss by the individual caused by financial fraud including unauthorised credit card transactions or credit fraud;

(b) identity theft causing financial loss or emotional and psychological harm;

(c) threats to an individual's physical safety, including family violence;

(d) humiliation, damage to reputation or relationships;

(e) workplace or social bullying or marginalisation; and

(f) physical harm or intimidation.

12. The Privacy Act contains the following non-exhaustive list of relevant matters that should be considered when assessing whether an individual is susceptible to serious harm:

(a) the kind or kinds of information;

(b) the sensitivity of the information;

(c) whether the information is protected by one or more security measures;

(d) if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome;

(e) the persons, or the kinds of persons, who have obtained, or who could obtain, the information;

(f) if a security technology or methodology:

(i) was used in relation to the information; and

(ii) was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information,

the likelihood that the persons, or the kinds of persons, who:

(iii) have obtained, or who could obtain, the information, and;

(iv) have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates,

have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;

(g) the nature of the harm; and

(h) any other relevant matters considered appropriate.

WHAT DOES "LIKELY" MEAN?

13. The next step involves deciding whether, from the perspective of a reasonable person, the data breach would be ***likely*** to result in serious harm to an individual whose personal information was part of the data breach.

14. In this context, a 'reasonable person' means a person in the entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach.

15. 'Likely' means that the risk of serious harm to an individual is more probable than not (rather than merely possible).

CAN SERIOUS HARM BE PREVENTED WITH REMEDIAL ACTION?

16. If we take positive steps to address a data breach in a timely manner, we can possibly avoid the need to notify. If we take remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach. Examples of remedial action include:

(a) ***employee leaves a smartphone on public transport:*** IT support staff remotely delete information on the smartphone; and

(b) ***email sent to incorrect person:*** the sender realises the error and contacts the recipient to ensure that the email has not been accessed and to request its deletion from the recipient's server.

RESPONDING TO A DATA BREACH

17. The processes outlined in the table below and the **Appendix** must be followed when an employee discovers a data breach or suspects that a data breach has occurred.

Step	Responsible person	Actions required
Discovery of data breach or suspected data breach by an employee	Employee	Where an employee discovers a data breach or suspects that a data breach has occurred, the employee must immediately notify the **Database and Digital Project Manager** (or equivalent) of the suspected data breach and attempt to remediate the breach if it is within their authority. The **Database and Digital Project Manager** (or equivalent) should be advised in writing of the following matters: • time and date that the suspected data breach was discovered; • the type of information involved; • the cause and extent of the suspected data breach; and • the context of the affected personal information and the suspected data breach.
Assessment by GM – Community and Stakeholder Relations (or equivalent)	**GM – Community and Stakeholder Relations (or equivalent)**	The **GM – Community and Stakeholder Relations (or equivalent)** must assess and determine whether a data breach has occurred. If the **GM – Community and Stakeholder Relations (or equivalent)** suspects that a data breach has occurred, the matter must be notified to the **CEO** to assess seriousness and potential reportability.
Escalation to CEO	**CEO or COO**	The **CEO or COO** must assess the seriousness of the suspected data breach. It will either be considered 'minor' or 'major' and then be handled as follows. **Minor breaches:** Minor breaches should be able to be dealt with by the **GM – Community and Stakeholder Relations (or equivalent)** The following details must be considered by the **GM – Community and Stakeholder Relations (or equivalent)**: • the nature of the breach or suspected breach; • action taken by relevant people within Basketball Australia to address the breach or suspected breach; and • the outcome of the action taken. If the **CEO** deems that the breach will not result in serious harm to an individual, then no further action is required.

Step	Responsible person	Actions required
		Potentially serious or major breaches: Where a data breach is deemed as being potentially serious or major, the **CEO** must undertake the processes outlined in the **Appendix** to this Response Plan, which include undertaking the following key steps: • **Step 1: Contain** the data breach to prevent any further compromise of personal information. • **Step 2: Assess** the data breach by gathering facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm. • **Step 3: Notify** individuals and the Commissioner if required. • **Step 4: Review** the incident and consider what actions can be taken to prevent future breaches. The steps highlighted in red in the process map contained in the **Appendix** are required by the Privacy Act under the Notifiable Data Breaches Scheme. Once the **CEO** has undertaken actions described above, the details of the matter must be recorded in accordance with Basketball Australia's record keeping practices.

RESPONSIBILITY FOR REPORTING

18. Affected individuals must be notified of data breaches promptly in order to better protect their personal information. In the event that the data breach is caused by an external organisation, Basketball Australia still retains the responsibility for notifying the affected individuals and the Commissioner of eligible data breaches. This is because Basketball Australia has the most direct relationship with the affected individual.

APPENDIX - DATA BREACH RESPONSE PROCESS MAP

Maintain information governance and security - APP 1 and 11

We have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds. If a data breach is suspected or discovered by an employee, the matter should be immediately remediated by the employee if it is within their authority and notified to the [insert appropriate title/position]. If the [insert appropriate title/position] suspects that a data breach has occurred, he or she must notify the [insert appropriate title/position].

Contain

The [insert appropriate title/position] will **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

The [insert appropriate title/position] will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If there are reasonable grounds to *believe* this is the case, then notification will be required (see below).

If there are grounds to only *suspect* that this is the case, then the [insert appropriate title/position] must conduct an **assessment** process. As part of the assessment, the [insert appropriate title/position] should consider whether **remedial action** is possible.

The responsibilities of the [insert appropriate title/position] are to:
- **Initiate**: plan the assessment and assign a team or person
- **Investigate**: gather relevant information about the incident to determine what has occurred
- **Evaluate**: make an evidence-based decision about whether serious harm is likely. The OAIC recommends that this be documented.

The [insert appropriate title/position] should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, the [insert appropriate title/position] must document why this is the case.

Take remedial action

Where possible, the [insert appropriate title/position] should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and the [insert appropriate title/position] can progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where **serious harm is likely**, the [insert appropriate title/position] must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:
- the entity's identity and contact details;
- a description of the breach;
- the kind/s of information concerned; and
- recommended steps for individuals.

The [insert appropriate title/position] must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:
Option 1: Notify all individuals.
Option 2: Notify only those individuals at risk of serious harm.
Option 3: Publish the statement on our website and publicise it.

The content of any notification must be reviewed by the CEO. The [insert appropriate title/position] should also consider whether it is appropriate to notify other relevant bodies such as the police or other law enforcement bodies.

If the data breach affects personal information of EU residents, the [insert appropriate title/position] will consider its obligation to notify under the EU General Data Protection Regime.

Review

The [insert appropriate title/position] must review the incident and take action to prevent future breaches. This may include:
- fully investigating the cause of the breach;
- developing a prevention plan;
- conducting audits to ensure the plan is implemented;
- updating security/response plan;
- considering changes to policies and procedures; and
- revising staff training practices.