Data Breach Policy & Response Plan

St Johns Park Bowling Club Limited

ACN: 823 421 682

Contents

1. Definitions and Interpretation 4
2. Responsibility 5
3. What is a Data Breach? 6
4. Responding to a Data Breach 6
5. Review and Prevention 9
Annexure "A" 10
Annexure 'B' 11

This policy is made on 19 February 2018 and will be reviewed biennially.

Introduction

This policy provides guidance regarding management of Personal Information held by the St Johns Park Bowling Club Limited (**Club**) and a plan for responding to a data security breach of such information held by the Club.

The policy provides guidance for staff for managing a data breach including:

- how staff may conduct an assessment and investigate a potential data breach;

- evaluation as to whether the data breach is an 'eligible data breach'; and

- if an eligible data breach occurs, steps in responding to the eligible data breach and considerations regarding parties that must be notified.

This policy has been developed to supplement the Club's Privacy Policy and in accordance with the *Privacy Amendment (Notifiable Data Breaches) Act* 2017 (**Act**). The Act is an amendment to the *Privacy Act* 1988 (Cth) (**Privacy Act**) and is referred to as the Notifiable Data Breach (**NDB**) scheme.

The NDB scheme requires regulated entities to notify individuals, organisations and the Commissioner where an 'eligible data breach' occurs, as outlined in this policy. Regulated entities include businesses and not-for-profit organisations with an annual turnover of $3 million or more. Accordingly, the Club is a 'regulated entity'.

The Club acknowledges the guidance provided by publications of the Office of the Australian Information Commissioner.

1. Definitions and Interpretation

1.1 Definitions

Act means the *Privacy Amendment (Notifiable Data Breaches) Act* 2017.

Assessment means a *'reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach'*, in accordance with s26WH of the Act.

Data Breach refers to the matters set out in clause 3 of this Policy.

Eligible Data Breach will arise where the following three criteria have been met:

(a) There is unauthorised access or unauthorised disclosure of personal information, that an entity holds; and

(b) This is likely to result in Serious Harm to one or more individuals; and

(c) The entity has not been able to prevent the likely risk of Serious Harm with remedial action.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

Relevant Matters are set out in s26WG of the Act as a non-exhaustive list of considerations as to whether a reasonable person would conclude that access to or disclosure of information would be likely or would not be likely to result in serious harm and include:

(c) The kinds of information;

(d) The sensitivity of the information;

(e) Whether the information is protected by one or more security measures;

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

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

(h) 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 the information, or 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;

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

(i) The nature of the harm;

(j) Any other relevant matters.

Remedial Action is where an entity takes action regarding a data breach and as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual, in accordance with s26WF (2) of the Act.

Serious Harm is determined having regard to the type of Data Breach but could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the organisation's position would identify as a possible outcome of the data breach.

Statement about an eligible breach means a statement complying with s26WK of the Act, a template to which is provided at Annexure A and will be modified depending upon the circumstances of the breach in conjunction with legal advice.

2. Responsibility

2.1 The Board and management of the Club has overall responsibility for the implementation of the Club's policies and facilitating staff training in relation to such policies.

2.2 The Club acknowledges it must take reasonable steps to protect Personal Information it holds from misuse, interference, loss, unauthorised access, duplication, publication or disclosure.

2.3 The Club ensures that any external third-party providers of information storage also take steps to protect Personal Information and requests copies of their Data Breach Policy and Response Plan. In circumstances where the Club is not satisfied with an external third-party Data Breach Policy and Response Plan, the Club will request that the agreement between it and the third party be amended to include the clauses set out in **Annexure 'B'** to this policy.

3. What is a Data Breach?

3.1 A Data Breach occurs when Personal Information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of such a breach may include, but are not limited to:

(a) Accidental loss of a portable device such as a USB, laptop or phone;

(b) When Personal Information is inadvertently sent to the wrong person or entity;

(c) A compromised user account by accidental disclosure of user login details through phishing, hence allowing unauthorised access to Personal Information; or

(d) Equipment failure or malware infection where an unauthorised party gains access to the Club's systems.

4. Responding to a Data Breach

4.1 The Club's Board and management must be notified of any Data Breach as soon as possible after the Data Breach has been identified.

4.2 The Club's Board and management must then act in accordance with this Policy and in particular the provisions of this clause 4 in responding to the Data Breach including assisting in responding to enquiries made by the public and managing complaints that may be received as a result of the breach.

4.3 Keys steps in responding to a Data Breach

There are four key steps to responding to a Data Breach;

(a) Contain the Data Breach;

(b) Assessment of the Data Breach and associated risks involved;

(c) Consider notifying affected individuals and the Commissioner;

(d) Review the Data Breach and identify and implement measures to prevent future Data Breaches.

4.4 Contain the Data Breach

Once a Data Breach has been identified, the Club must firstly take steps to contain the Data Breach. This involves taking immediate steps to limit any further access or distribution of the affected Personal Information, or the possible compromise of other information.

The actions required in containing a Data Breach will depend on the circumstances of the Data Breach, for example it may involve shutting down a system, revoking access to a system or changing access codes or passwords in conjunction with an Information and Communication Technology (**ICT**) provider.

4.5 Assessment of the Data Breach and risks involved

(a) **Plan:** The CEO is responsible for, and has authority to coordinate, the assessment of a Data Breach and may undertake this internally by assigning a team to assist in the process, depending on the potential magnitude of the breach or undertake the assessment through an external provider;

(b) **Insurance:** If the Club has an insurance policy in relation to Data Breaches the CEO will ensure that the insurer is notified of the Data Breach and seek input from the insurer as to its desire to be involved in the response.

(c) **Assess, Investigate & Evaluate:** The CEO and person or persons responsible for the assessment must immediately investigate the Data Breach by gathering the relevant information about the incident to determine what has occurred and evaluate whether Serious Harm is likely to occur or has occurred as a result. Questions that may be asked include:

(i) **Who is affected by the Data Breach?** Determine the data involved and who this may affect. Is it Personal Information and which individuals or organisations will it affect?

(ii) **What caused the breach?** Was this a targeted attack or through oversight of the Club or any of its employees? Determine the kind or kinds of persons who may have access to the data.

(iii) **What is the risk of harm?** For example, has access been gained to Personal Information such as financial details and may this lead to financial harm? Is there an ongoing risk regarding further disclosure? What steps have been taken to contain the Data Breach? Was the data recovered and was it protected by security measures? Which system/s does it affect?

The Definitions section of this policy sets out a non-exhaustive list of **Relevant Matters** to consider.

(d) If this assessment is concluded and the person/s undertaking the assessment find that there was a Data Breach, that Serious Harm is likely to result from the Data Breach and the Club has not been able to prevent the likely risk of Serious Harm with remedial action, then the Data Breach will constitute an ‘Eligible Data Breach’, and notification is necessary.

An exception may apply to the obligation to notify the Commissioner or individuals where remedial action is taken and the Data Breach would not be likely to result in Serious Harm. An example of this is provided by the Office of the Australian Information Commissioner (**OAIC**), whereby an employee leaves their smartphone on public transport on the way to work. They realise once they arrive at work, however due to the security measures on their phone the IT support staff are confident that its contents could not have been accessed in the short period when it was lost and when its contents were deleted. This incident would therefore not require notification. However, the circumstances of whether there is an obligation to notify following each Data Breach must be considered on once the assessment of the Data Breach has been undertaken.

(e) Once again, it is important to note that the primary role of the CEO and response team is to firstly contain the breach and minimise any further disclosure or potential disclosure of Personal Information.

4.6 Notification

The CEO and management of the Club will manage the notification process.

If the Club finds an 'Eligible Data Breach' has occurred, it must notify the Commissioner as soon as practicable. This will vary depending upon the circumstances, however prompt notification is expected. The OAIC provides an online form for reporting of Eligible Data Breaches or a Microsoft Word version may be sent to enquiries@oaic.gov.au. The OAIC may request supplementary information.

Notification to the Commissioner is not required before the notification to individuals and the process will depend upon the circumstances. However, the Commissioner expects to be notified expeditiously.

The Club must notify individuals affected by the Eligible Data Breach. Once again, prompt notification is necessary to avoid or reduce the potential damage by enabling the individual or organisation to take steps to protect themselves if possible. This may require notification by email, phone or by publicising a statement on the Club's website, or a combination of these notifications.

If the Club does not have up to date contact details for individuals or organisations it will publish a copy of the statement on their website and take steps to publicise the contents of the statement.

A template of the type of details that should be included can be found at Annexure A. However, the statement will be tailored where possible to incorporate an explanation of the circumstances giving rise to the Eligible Data Breach. The statement should be made by the CEO.

The CEO and management will coordinate the communications plan depending upon the circumstances of the Eligible Data Breach and will consider contacting external stakeholders such as Police, ASIC, The Australian Cyber Security Centre,

professional bodies or financial service providers. The CEO will have authority to seek external support as necessary such as legal support in drafting notices, Information and Communication Technology (**ICT**) support if the Eligible Data Breach requires investigation of the ICT systems and HR Support if the breach was due to the actions of a Club employee.

5. Review and Prevention

5.1 Once the Data Breach has been managed the Club will ensure it reviews the breach and develops a prevention plan. This may involve:

(a) Updating a security/response plan;

(b) Considering changes to policies and procedures;

(c) Revising staff training and/or access requirements to ICT systems;

(d) Review of contractual obligations with third party service providers.

The review and prevention plan will depend upon the circumstances of the Data Breach and necessary steps in accordance with such breach.

Annexure "A"

Statement
(This statement should be approved by the Club's insurer prior to being sent to any recipient)

St Johns Park Bowling Club Limited
PO BOX 403
BONNYRIGG NSW 2177
Contact: Chief Executive Officer – Mr David Marsh

(addressed to individuals affected)

Dear xxx,

I am writing to information you of a recent data breach that occurred on (date/or date range), and it was detected on (date).

(a) A brief description of what occurred

(b) Description of data that was inappropriately accessed, collected, used or disclosed (ie. Was it financial information, the kind of information disclosed)

(c) Risk/s to individuals or organisations/who has obtained or is likely to have obtained access to the information (usually it would be sufficient to state 'external third party' or 'former employee' for example.

(d) Steps taken by the Club

(e) Steps recommended to individuals, for example, if the breach involves financial information you may suggest the individual contact their financial institution to change their credit card number

(f) A brief description of what the Club is doing to investigate, control or mitigate the harm to individuals or organisations and protect against further breaches.

Please phone me with any questions or concerns you may have about the data breach.

We have established a section on the Club website (insert link), with updated information and links to resources that offer information about this data breach and take our role in safeguarding your data very seriously.

Please be assured we are doing everything we can to rectify this situation and put further measures in place to prevent any future breach.

Annexure 'B'

Agreement with Third-Party providers

We have included clauses below, which may be included in Agreements with third-party providers in relation to their management of Personal Information on behalf of the Club.

CONFIDENTIAL INFORMATION

The Contractor acknowledges that:

(a) that all rights, title and interest in the Confidential Information remains at all times, with the Club;

(b) the Confidential Information is confidential to the Club;

(c) whilst performing the Services, the Contractor will come into possession or be in a position to acquire Confidential information;

(d) any Personal Information forming part of the Confidential Information must be handled and protected in accordance with the requirements of the Privacy Act and the APP's.

The Contractor undertakes that during the term of this Agreement, it will:

(a) take reasonable steps to protect Confidential Information from misuse, interference and loss, as well as unauthorised use, access, modification, duplication, publication or disclosure; and

(b) not disclose, orally or otherwise, any Confidential Information to any person or entity other than its employees, contractors, agents, officers and advisers (or those of its related bodies corporate) who require access to the Confidential Information strictly for the purpose of allowing the Contractor to provide the Services or any other purpose expressly agreed to in writing by the Club (in its absolute discretion), and subject always to the Contractor obtaining written undertakings from any such employees, contractors, agents, officers and advisers (or those of its related bodies corporate), that they will take all reasonable steps protect the Confidential Information to at least the same standard required of the Contractor under this Agreement;

(c) put in place and maintain security measures to protect Confidential Information from misuse, interference and loss, as well as unauthorised use, access, modification, duplication, publication or disclosure including by its employees, contractors, agents, officers and advisers (or those of its related bodies corporate);

(d) take reasonable steps to destroy or de-identify all Confidential Information it holds once it is no longer needed for the purpose of providing the Services or upon expiry or termination of this Agreement;

(e) immediately notify the Club of any suspected misuse, interference and loss, as well as unauthorised access, modification, duplication, publication or disclosure of any of the Club's Confidential Information in accordance with this Agreement; and

(f) immediately take all reasonable steps to stop any suspected misuse, interference and loss, as well as unauthorised access, modification, duplication, publication or disclosure of any of the Club's Confidential Information and notify the Club of such steps.

The Contractor agrees that, prior to entering into this Agreement, it will develop policies, practices and procedures to ensure compliance with the Privacy Act and the APP including:

(a) documenting the internal practices, procedures and systems that the Contractor will use to protect Confidential Information, including Confidential Information security measures such as:

(i) date and time stamped access records in relation to Confidential Information;

(ii) ceasing the use of generic usernames and passwords, to the extent they are used for remote access to the Contractor or Club systems for the purpose of viewing the Confidential Information; and

(iii) immediately removing system privileges of former employees of the Contractor, contractors, agents, officers and advisers upon their cessation of their services to the Contractor,

(b) making available to the Club on request, copies of any individual data access records;

(c) documenting the security choices the Contractor has made about its security profile, including the reasons why it has or has not adopted specific Confidential Information security measures;

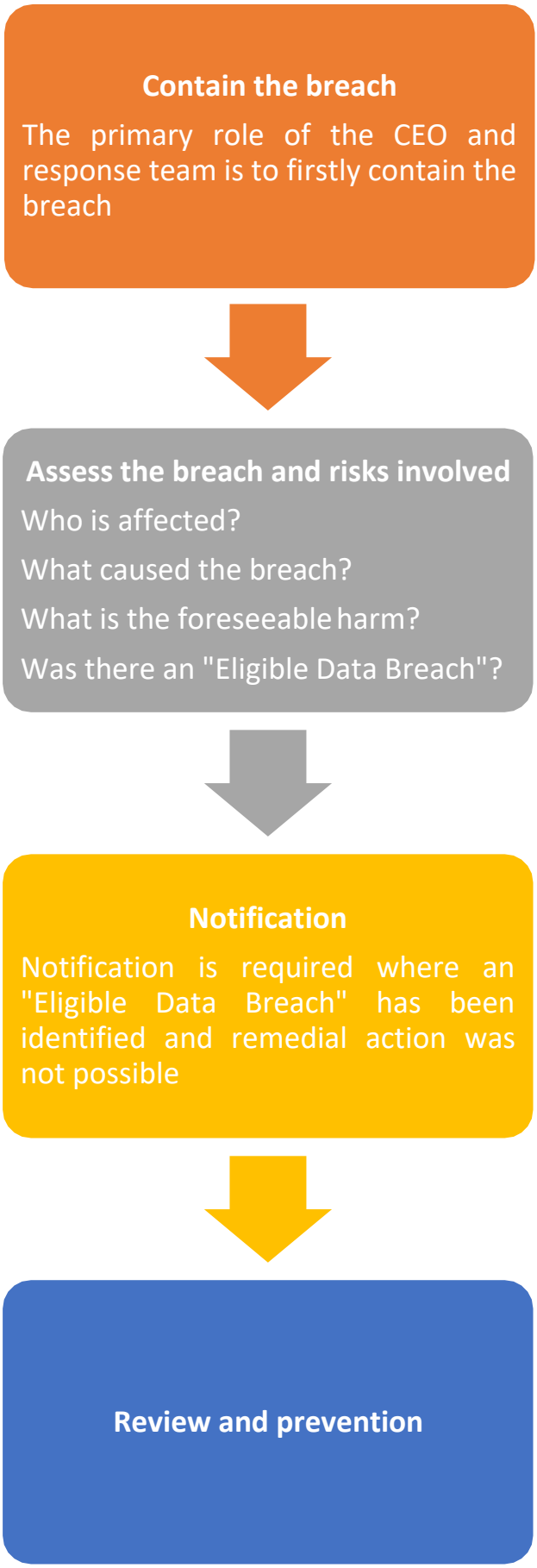
(d) ensuring that all employees, contractors, agents, officers and advisers (or those of its related bodies corporate), are trained in and are familiar with the policies, practices and procedures developed by the Contractor.

This clause does not apply to Confidential Information which:

(a) is required by law to be disclosed;

(b) is ordered to be disclosed in the course of legal proceedings; or

(c) falls into the public domain other than through an act or omission of the Contractor, its officers, employees, agents or contractors.


Contain the breach
The primary role of the CEO and response team is to firstly contain the breach
Assess the breach and risks involved
Who is affected?
What caused the breach?
What is the foreseeable harm?
Was there an "Eligible Data Breach"?
Notification
Notification is required where an "Eligible Data Breach" has been identified and remedial action was not possible
Review and prevention