Procedure

Data Breach Response Plan

Issued with the authority of the Chief Commissioner
and Chief Executive Officer of Scouts Australia NSW

Chief Commissioner signature		Chief Executive Officer signature	
Sponsor	Jeanne Young		
Document type	Procedure	Date of issue	18 May 2018
Document code & no.	PRO38	Version number	1.0.0
Document title	Data Breach Response Plan	Due for review	18 November 2018

Contents

Data Breach Response Plan

Acknowledgement

The content within this document has been gathered from various official government websites as a best practise approach to data breach management.

1. Introduction

1.1 Defined terms have the meanings set out in Definitions and Acronyms section.

1.2 This document outlines the framework for responding to data breaches and suspected data breaches within the Scout Association of Australia, New South Wales Branch (**Scouts NSW**). This document has been developed in response to the Notifiable Data Breach (**NDB**) scheme under Part IIIC of the Australian Privacy Act 1998 (Cth) (**Privacy Act**).

1.3 The NDB scheme is effective 22nd February 2018 and applies to data breaches that occur on or after that date. It is not applied retrospectively.

1.4 Entities have an obligation to notify individuals, where their **personal information** is involved in a data breach, and upon assessment, it is considered likely that the breach may result in **serious harm** to the individuals.

1.5 Scouts NSW is committed to dealing with data breaches, whether actual or suspected, in a robust and timely manner.

1.6 Scouts NSW is subject to the Privacy Act and respective Australian Privacy Principles (**APP**). Scouts NSW is considered an **APP entity**.

1.7 In the course of managing our business, Scouts NSW collects **personal information** on its members (including youth members and their parents / guardians), volunteers and employees.

1.8 This response plan should be read in conjunction with our Privacy Policy (POL03). Scouts NSW is committed to protecting the privacy of its members, customers, volunteers and employees.

1.9 This response plan is binding on all staff and volunteer members as well as all formations of the organisation in NSW (from the State level down to the local Scout Group and Section).

2 Key Definitions and Criteria

2.1 The NBD scheme applies specifically to data breaches involving **personal information** that is likely to result in **serious harm** to any individual affected. These are referred to as '**eligible data breaches**'.

2.2 Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a **reasonable person** in the organisation's (Scouts NSW) position.

2.3 The criteria for an eligible data breach consists of:

2.3.1 there is **unauthorised access** to, or **unauthorised disclosure** of personal information, or a **loss** of personal information, that Scouts NSW holds

2.3.1 this is likely to result in serious harm to one or more individuals, and

2.3.1 Scouts NSW has not been able to prevent the likely risk of serious harm with remedial action.

2.4 Organisations that suspect an eligible data breach may have occurred must undertake a **reasonable** and **expeditious assessment (30 calendar days)** to determine if the data breach is likely to result in serious harm to any individual affected. The key points being:

2.4.1 If Scouts NSW has **reasonable grounds** to believe that it has experienced an eligible data breach, it must promptly notify individuals and the Office of the Australian Information Commissioner (OAIC) Commissioner about the breach, unless an exception applies.

2.4.1 If Scouts NSW **suspects** that it may have experienced an eligible data breach, it must quickly assess the situation to decide whether or not there has been an eligible data breach.

3 Purpose Statement

3.1 This data breach response plan (DBRP) sets out the procedures and escalation processes for Scouts NSW in the event of a data breach (real or suspected).

3.2 This DBRP also outlines the notification framework and processes for eligible data breaches. It is noted that any data breach needs to be considered on a case-by-case basis with a specifically tailored response.

3.3 This response plan is intended to enable Scouts NSW to contain, assess and respond to data breaches in a timely manner and to help mitigate the potential for harm to affected individuals.

3.4 Following are process outlines for staff members and volunteers to report a data breach / potential data breach, and a checklist for the Data Breach Response Committee (DBRC).

4 Data Breach Response Committee Roles and Responsibilities

4.1 The Data Breach Response Committee is to be comprised of cross-functional representatives of the organisation:

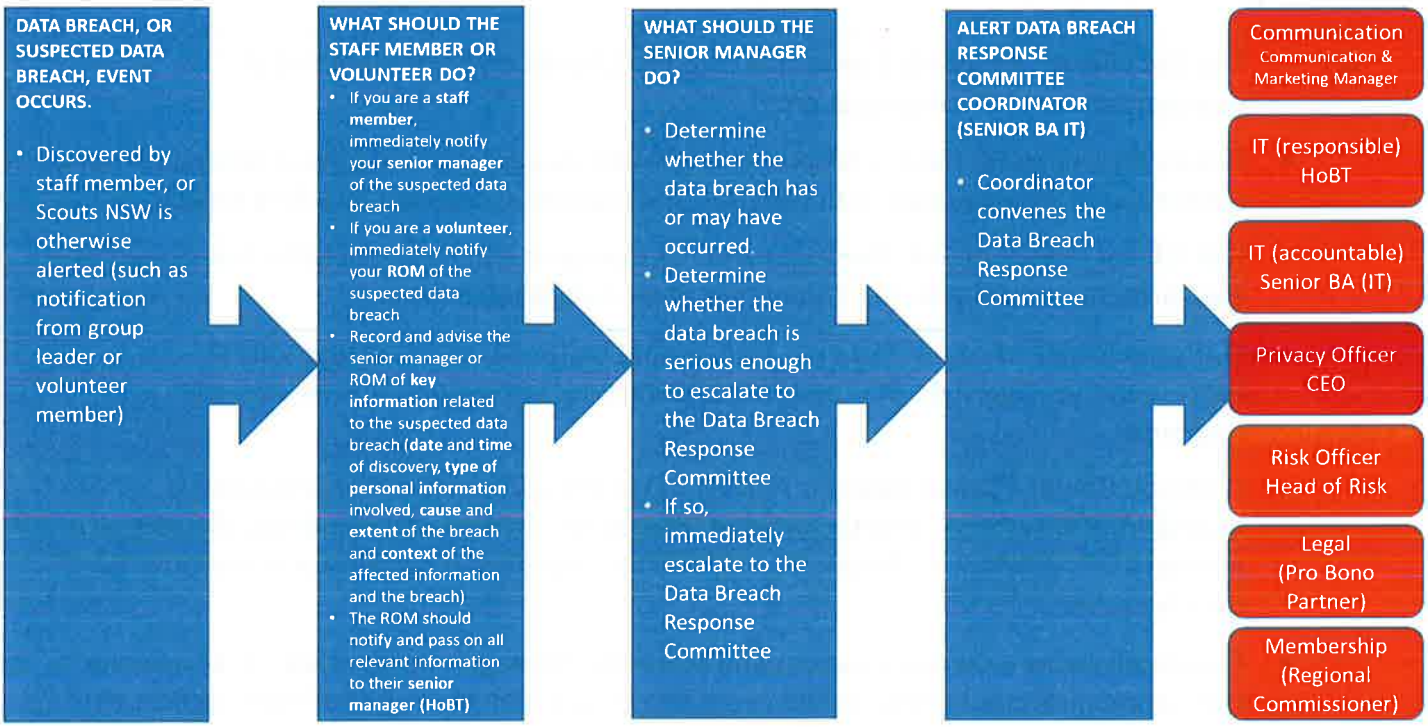
- Privacy Officer – CEO (Chair). Responsible for data stewardship and privacy related matters, authorised to communicate with the OAIC and individuals affected by a data breach.
- Risk Officer – Head of Risk. Oversight and risk management, responsible for assessment of data breaches raised with the Committee against eligibility criteria
- IT (Responsible) – Head of Business Transformation (HoBT) as the responsible IT representative. Oversight of IT systems, architecture and security (prevention and response)
- IT (Accountable) – Senior Business Analyst (IT) as the accountable IT representative. Oversight of IT systems, architecture and security (prevention and response), this role also encompasses coordinator function for convening emergency committees in response to data breaches.
- Communications – Communications and Marketing Manager. Responsible for developing the communications strategy in the event of a breach and advising the Privacy Officer and the Committee on preferred notification options.
- Legal – Pro Bono legal advisor. Oversight and legal advice to assist with assessment of data breach against eligibility criteria
- Membership – Region Commissioner level. Assistance and communication both to and from membership base, Committee can authorise this role to enact an emergency Region Commissioner forum (or similar) if the breach affected a significant number of regions / membership base.

5 Data Breach Response Committee Schedule

5.1 The Data Breach Response Committee shall meet as and when required to deal with data breaches or suspected data breaches within or relating to Scouts NSW.

5.2 Outside of the above requirement, the Committee shall meet at regular periodic intervals, such as quarterly, to review the DBRP and market best practice in terms of avoidance and response.

6 Process flow – report a data breach / suspected data breach



I. Escalation

i. Senior managers should use discretion in deciding whether to escalate to the response team.

ii. Certain data breaches may be considered minor and able to be dealt with easily within the business by the relevant manager in consultation with the Communications and Marketing Team.

iii. Consideration should be given to the following questions:

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to the affected individuals?
- Does the breach / suspected breach indicate a systemic problem in organisational processes or procedures?
- Could there be media or stakeholder attention as a result of the breach?

If the answer is 'yes', it is appropriate to notify the DBRC.

iv. If the senior manager decides not to escalate a minor data breach to the DBRC for further action, the senior manager should still send a brief email to the DBRC Coordinator outlining:

- Description of the breach / suspected breach
- Action taken to address the breach / suspected breach
- Outcome of those actions
- Senior managers view that no further action is required

These emails are to be saved in an appropriate location decided by the DBRC.

II. Data Breach Response Committee Process

i. In the event that a data breach, or suspected data breach, is escalated to the DBRC, the Coordinator (Senior BA IT) will convene the DBRC as expeditiously as possible.

ii. As there is no single method in responding to data breaches, each must be dealt with on a case-by-case basis, with a risk assessment to determine the appropriate course of action.

iii. The OAIC recommend the following four key steps are considered when responding to a breach / suspected breach:

1. Contain the breach and do a preliminary assessment
2. Evaluate the risks associated with the breach
3. Notification where required
4. Prevent future breaches

Steps 1 to 3 should be undertaken simultaneously or in quick succession.

iv. Further guidance on these steps and in reducing the risk of future breaches is available in the OAIC publications *Data Breach Notification: a guide to handling personal information security breaches* and *Guide to securing personal information* (linked in the reference section of this document).

III. Checklist and decision tree

The following checklist has been adapted from the OAIC's own Data Breach Response Plan.

STEP 1

Contain the breach and make a preliminary assessment

☐	Convene a meeting of the data breach response team.
☐	Immediately contain breach: ☐ IT to implement the *ICT Incident Response Plan* if necessary. ☐ Building security to be alerted if necessary.
☐	Inform the OAIC Executive, including the Australian Privacy Commissioner; provide ongoing updates on key developments.
☐	Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing the OAIC to take appropriate corrective action.
☐	Consider developing a communications or media strategy to manage public expectations and media interest.

STEP 2

Evaluate the risks for individuals associated with the breach

☐	Conduct initial investigation, and collect information about the breach promptly, including: ☐ the date, time, duration, and location of the breach ☐ the type of personal information involved in the breach ☐ how the breach was discovered and by whom ☐ the cause and extent of the breach ☐ a list of the affected individuals, or possible affected individuals ☐ the risk of serious harm to the affected individuals ☐ the risk of other harms.
☐	Determine whether the context of the information is important.
☐	Establish the cause and extent of the breach.
☐	Assess priorities and risks based on what is known.
☐	Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.

STEP 3

Consider breach notification

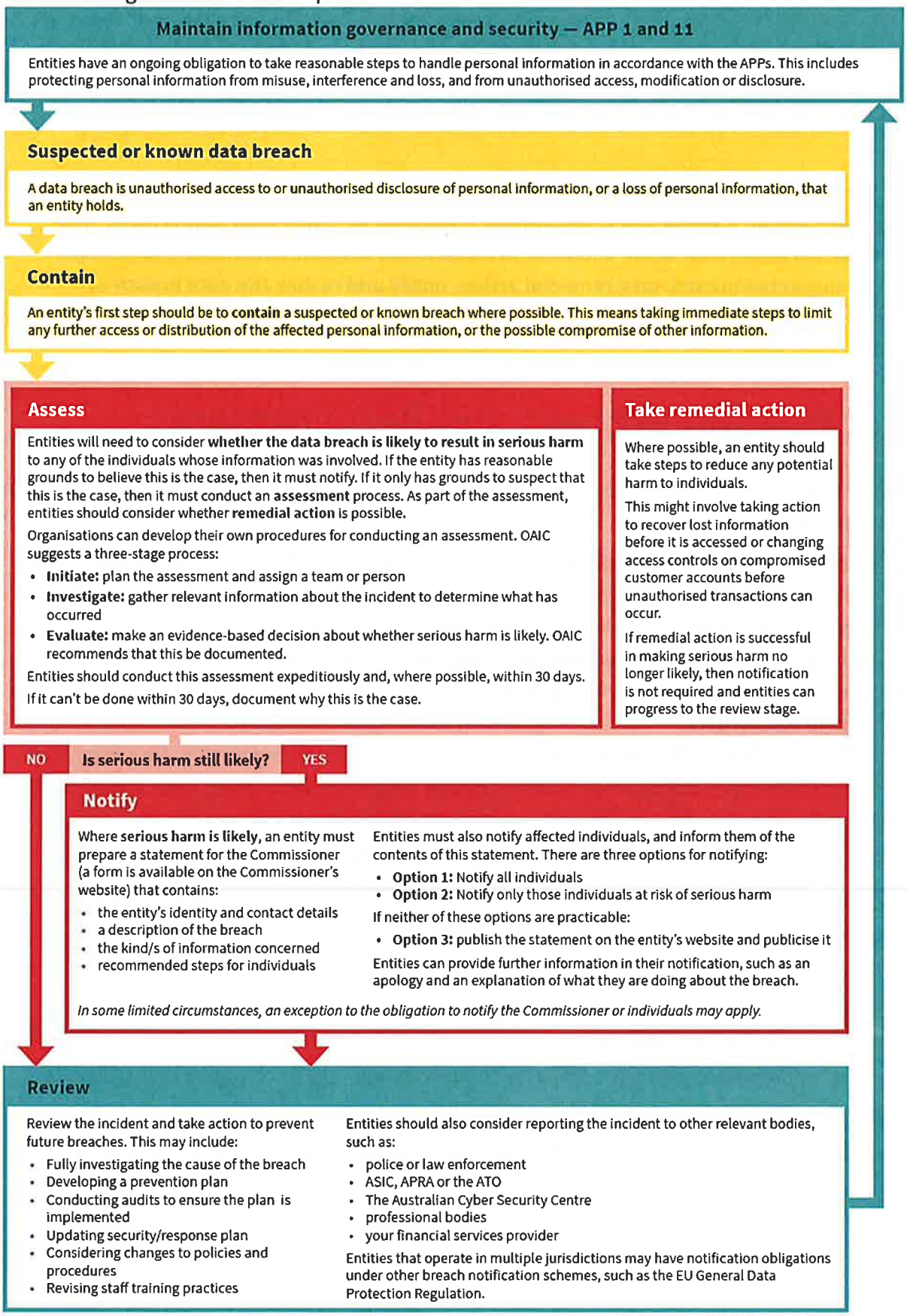
☐	Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
☐	Determine whether to notify affected individuals – is there a *real risk of serious harm to the affected individuals?* In some cases, it may be appropriate to notify the affected individuals immediately; e.g., where there is a high level of risk of serious harm to affected individuals.
☐	Consider whether others should be notified, including police/law enforcement, or other agencies or organisations affected by the breach, or where the OAIC is contractually required or required under the terms of an MOU or similar obligation to notify specific parties.

STEP 4

Review the incident and take action to prevent future breaches

☐	Fully investigate the cause of the breach.
☐	Report to OAIC Executive on outcomes and recommendations: ☐ Update security and response plan if necessary. ☐ Make appropriate changes to policies and procedures if necessary. ☐ Revise staff training practices if necessary. ☐ Consider the option of an audit to ensure necessary outcomes are effected.

The following decision tree is reproduced from the OAIC website:



IV. Processes for dealing with a data breaches within another entity

i. Where there is a data breach incident within another entity, an assessment is to be made of primary relationship. If the primary relationship is deemed to reside with Scouts NSW, then Scouts NSW will enact their DBRP and work in conjunction with the other entity to contain, assess the suspected breach, take remedial action, notify and review the data breach or suspected data breach.

7 Notification Process and Requirements

7.1 Where notification is required as a result of a data breach, there are three options available to Scouts NSW:

- **Option 1 – Notify all individuals**. If it is practicable, Scouts NSW can notify each of the individuals to whom the relevant information relates. That is, all individuals whose personal information was part of the eligible data breach.
- **Option 2 – Notify only those individuals at risk of serious harm**. If it is practicable, Scouts NSW can notify only those individuals who are at risk of serious harm from the eligible data breach.
- **Option 3 – Publish Notification**. If neither option 1 or 2 are practicable, for example, if Scouts NSW does not have up-to-date contact details for individuals, then Scouts NSW must:
  - publish a copy of the statement on its website
  - take reasonable steps to publicise the contents of the statement

7.2 Notification to affected individuals must include:

- the identity and contact details of the individual,
- description of the eligible data breach,
- the kind(s) of information concerned, and
- recommendations about the steps individuals should take in response to the breach.

Notification to the OAIC are submitted through the OAICs Notifiable Data Breach statement — Form. This process must be completed by the Privacy Officer within 30 days of the suspected data breach.

8 Definitions

8.1 **APPs:** the Australian Privacy Principles set out Schedule 1 to the Privacy Act, which apply to APP entities.

8.2 **APP entity:** has the meaning set out in section 6 of the Privacy Act, and means an agency or organisation for the purpose of the Privacy Act.

8.3 **Data breach:** means when personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Further clarification on data breaches is listed in the definitions of **unauthorised access**, **unauthorised disclosure** and **loss** of personal information.

8.4 **'Likely to occur'** and **'likely to result':** means the risk of serious harm to an individual is more probable than not (rather than possible)

8.5 **NDB**, or **NDB Scheme:** Notifiable Data Breach, Notifiable Data Breach scheme

8.6 **Personal Information:** means information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

8.7 **Privacy Act:** Part IIIC of the Australian Privacy Act 1998 (Cth)

8.8 **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.

8.9 **Scouts NSW:** Scout Association of Australia, New South Wales Branch

8.10 **Serious harm:** can 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 entity's position would identify as a possible outcome of the data breach. The test for 'serious harm' does not require that harm to be attributed to **all** affected individuals. It is satisfied if the harm would be caused to **any** individual whose relevant information has been breached.

8.11 **Unauthorised Access of Personal Information:** Personal information that the organisation holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee or an independent contractor, as well as unauthorised access by an external third party (i.e. 'hacking')

8.12 **Unauthorised Disclosure of Personal Information:** Where the organisation, intentionally or unintentionally, makes personal information accessible or visible to others outside the organisation, including an unauthorised disclosure by an employee of the organisation.

8.13 **Loss of Personal Information:** Refers to the accidental or inadvertent loss of personal information held by the organisation, where it is likely to result in unauthorised access or unauthorised disclosure.

9 References

Data Breach Notification: a guide to handling personal information security breaches

Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)

Guide to securing personal information

10 Related Group Policies and Documents

Privacy Policy

Business Continuity Plan (under development)

Cyber Security Response Plan

Data Retention Policy (under development)

Information Assets Register (under development)