Scouts Australia Privacy Policy

Approved and updated by the authority of the Scouts Australia National Executive Committee

Date: NOVEMBER 2018

Table of Contents:

Revision History

DATE	REVISION

AUSTRALIAN PRIVACY PRINCIPLES

While the Australian Privacy Principles (APPs) are **not prescriptive**, each APP entity needs to consider how the principles apply to its own situation. This Policy outlines these Principles and describes how they pertain to Scouting in Australia. Scouts Australia's expectations against each Privacy Principle are outlined below:

APP 1 — OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

Scouts Australia expects that its Branches and sub entities will manage personal information in an open and transparent way. This requires that the national body and all its Branches are to develop and maintain a clearly expressed APP privacy policy which conforms to the national principles and this Scouts Australia Policy.

APP 2 — ANONYMITY AND PSEUDONYMITY

Scouts Australia requires that its Branches and sub entities maintain accurate records on identities of its members for the purpose. For this reason, the ability for a member to remain anonymous or utilise a pseudonym is not possible.

APP 3 — COLLECTION OF SOLICITED PERSONAL INFORMATION

Scouts Australia expects that all Branches and sub-entities will advise members that they will collect and retain solicited personal information and additionally advise of the standard that will be applied to the collection and holding of that sensitive information. Sensitive information may include personal identifiable information, medical information, custody arrangements and police record check results.

APP 4 — DEALING WITH UNSOLICITED PERSONAL INFORMATION

Scouts Australia expects that all Scout Branches and sub-entities will advise members how they will deal with unsolicited personal information.

APP 5 — NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

Scouts Australia expects that all Branches and sub-entities will advise their members when, and under what circumstances they will notify an individual of certain matters detailed below.

APP 6 — USE OR DISCLOSURE OF PERSONAL INFORMATION

Scouts Australia requires that its Branches and sub-entities clearly advise members of the circumstances in which they may use or disclose personal information that they hold.

APP 7 — DIRECT MARKETING

All Branches and sub-entities are to clearly articulate to members how they will use or disclose personal information for direct marketing purposes. Scouts Australia, its Branches and sub-entities will not provide information to any external party for direct marketing purposes without giving members an opportunity to opt-in.

APP 8 — CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

Scouts Australia requires that all members be advised of the steps that any Branch, sub-entity or related party will take to protect personal information when a situation arises that requires information to be disclosed overseas for any purpose.

APP 9 — ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

There are very limited circumstances when Scouts Australia may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual. Where these circumstances do occur, they are to be communicated to the member concerned.

APP 10 — QUALITY OF PERSONAL INFORMATION

Scouts Australia expects that all Branches and sub-entities will take reasonable steps to ensure the personal information they collect

is accurate, current, relevant and complete. Branches and sub-entities are also to take reasonable steps to ensure the personal information they use or disclose is accurate, current, complete and relevant, having regard to the purpose of that use or disclosure.

APP 11 — SECURITY OF PERSONAL INFORMATION It is the responsibility of all Branches and sub-entities to take reasonable steps to protect member information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

APP 12 — ACCESS TO PERSONAL INFORMATION All Branches and sub-entities are to outline to their members their obligations when an individual requests access to their own personal information. This advice is to include the requirement to provide access, and the time-frame it will be provided (unless a specific exception applies).

APP 13 — CORRECTION OF PERSONAL INFORMATION Scouts Australia expects that all Branches and sub-entities will develop a process through which members can request the correction of information held about them. This process is to be included in Branch and sub-entity privacy policies and conform to this Policy as a minimum standard.

1. INTRODUCTION AND CONTEXT

Scouts Australia has always respected the privacy of its members and customers and understands the importance our members place on the protection of the personal information in our care. Our commitment to protecting the privacy of our members is important to us. **For the purposes of this Policy, the term "SCOUTS AUSTRALIA" includes Scouts Australia; its State and Territory Branches; and any directly related sub-entity of the National and State organisation. For clarity, the provisions and requirements contained in this Policy are primarily the responsibility of the State or Territory Branch which has screened (as required), admitted and primarily holds, a member's record and where the member may (or may not) pay a membership fee. That entity is the 'Scout custodian' of the information.**

This Privacy Policy conforms with the provisions of the Australian Privacy Principles embodied in the "Privacy Act 1988 (Cth)". It explains the kind of information that Scouts Australia will collect from its members and how it collects, maintains, uses and discloses that information. It also describes the privacy rights of our members. Additionally, it explains how members can access the information we keep; how members can update their records; and how members can advise us of any concerns they have.

This policy presents the minimum privacy requirements for all Scout Branches and sub-entities, to reflect in their own policies (Branches as the primary custodians of member information may wish to develop their own particular and stricter requirements) and for the National Office and national functional areas as appropriate.

This policy applies to members of Scouts Australia residing within Australia. It does not extend to those members who have emigrated or are Expatriate to Australia, in particular to those jurisdictions where local Privacy laws will supersede Australian law. For example:

General Data Protection Regulations (GDPR)
Scouts Australia from time to time interacts with and collects data from individuals within the European Union (EU) who are subject to EU General Data Protection Regulations. Under European law, EU residents have the opportunity to provide their consent to their data being used by organisations outside the Union (such as Scouts Australia) for the purposes of conducting activities/events. Specifically EU residents have the right to:

- request access, correct, update or delete personal information held by Scouts Australia. EU residents may contact us directly at any time about accessing, correcting, updating or deleting their personal information by emailing us at scouts@scouts.com.au We will respond to these requests in accordance with GDPR.

- object to the processing of their personal information, ask us to restrict processing of their personal information or request portability of their personal information by contacting us at scouts@scouts.com.au
- complain to a data protection authority about our collection and use of their personal information. This complaint can be made through the national or local data protection authority.
- Opt-out at any time in the same fashion (and as easily) as they Opted-In.

Scouts Australia recognises the rights of EU Residents under GDPR legislation. However, Scouts Australia directs that for all EU residents participating in Scouts Australia activities and events that they do so on the understanding that Australian Privacy Law will apply. Potential EU participants are to be given the opportunity to consent to the above in application documentation.

2. PRIMARY PURPOSE DEFINITION

Personal information is collected and retained by Scouts Australia on past and present adult members, as well as youth members and their parents, including guardians or care-givers, for the primary purpose of operating the Scout Association in Australia.

All information collected is directly applicable to the functions and activities of Scouting and to the health, well-being and protection of its members.

This information is entered and stored in centralised databases accessible only by authorised managers of Scouting. Data may also be retained in electronic or hardcopy format by the Headquarters and at any sub-entity location (Branch, Region, District, Group level) of the organisation to which the individual member belongs.

3. COLLECTION OF DATA

Scouts Australia will only collect personal information in a fair and lawful manner. Only that information which we require to properly manage and promote our organisation and ensure the health, well-being and protection of our members is to be collected.

Scouts Australia may collect personal information from members when they apply for membership, a training course, a major Scouting event, or, at other times when we communicate with them. We may also collect personal information about members from third parties such as parents, guardians and care-givers, Scouts staff, Leaders and health care providers. During those occasions, and in the application forms that we ask members to complete, there will be statements about privacy and requests for consent. Those privacy statements should refer members to the Scouts Australia National Privacy Policy, or the Branch policy, where more detail is available on how member information may be used and disclosed. Membership application forms for Scouting must refer to the National and the Branch Privacy Policy (containing these minimum standards) and seek consent for Scouts Australia to collect, maintain, use and disclose member information that is reasonably necessary to properly manage and promote Scouting and to ensure the health, well-being and protection of our members.

4. USE OF IDENTIFIERS

When you apply to become a member of Scouts Australia, you are assigned a system generated 'scout number' by the custodian Branch or sub-entity to uniquely identify members. This number has no relationship to any identifier assigned by any other organisation. This is the main 'identifying number' that Scouts Australia uses to identify a member.

Scouts Australia Institute of Training (SAIT) captures a member's Unique Student Identifier (USI) number and uses this to track member training. The USI is a mandatory data field for reporting nationally recognised training. An 'authority' may share an 'identifier' with Scouts Australia to identify a member for a special purpose. When this occurs, Scouts Australia will protect this identifier and not share it with a third party unless lawfully required to do so.

5. TYPE OF DATA COLLECTED

"Personal information" means any information or an opinion recorded about a member to the extent where that member can be identified, or can reasonably be identified from the information.

Scouts Australia membership applications request information that identifies members such as; their full name and date of birth and contact details. Those applications will also request the name of an applicant's school or, if employed, occupation and work contacts. Application forms must also request the contact details of personal referees and seek answers to specific screening questions contained in the Scouts Australia Child Protection Policy.

The Scouts Australia adult membership application form is to specifically demand the authority for 'the Custodian Branch' to view a member's 'Personal History Information' and his/her Working With Children Certificate (WWCC) as appropriate. In applying to join Scouts a member must agree that this information can be collected and further agree that this will form the basis of our decisions about membership.

In the case of youth members, and particularly at the Branch custodian level, Scouts Australia also has a requirement to collect the names and contact details of parents, guardians and care-givers in case they need to be contacted in an emergency, or to ensure they are informed about Scouting activities, policy issues or other important matters involving their children/wards. Scouts Australia may also ask for the parents, guardians or care-givers occupation details as well as their skills/hobbies and sporting/leisure activities, as we rely on volunteering and expertise in a variety of related areas for the benefit of the delivery of our youth program.

6. SENSITIVE DATA

Scouting is a voluntary, non-political, educational movement for young people, which is open to all without distinction of origin, race or creed. The purpose of the Scout movement is to contribute to the education of young people in achieving their full physical, intellectual emotional, social and spiritual potential as individuals, as responsible citizens and as members of their local, national and international communities. In this context, Scouts Australia does not actively seek to collect sensitive information (for example; race, politics, police record or religious background) unless it is reasonably necessary to satisfy the purpose and principles of our organisation, or, is necessary for the well-being and protection of members as permitted or required by law.

The following information, which may be considered to be of a **'sensitive nature'**, can be collected by our custodian Branches:

- Member place of birth and nationality in order for us to identify any special needs of members from different cultures.
- Member gender where necessary to enable the provision of appropriate separate accommodation and ablution facilities when required (e.g. camping in the outdoors)
- Member religion/denomination (if applicable) is requested so that we can better support the needs of members from different spiritual backgrounds.
- Member marital status and partner name may be requested for the purposes of inviting partners to Scout functions and activities and to incorporate them as much as possible in the 'Scouting family'.
- Member personal history information as obtained from the authorities in accordance with the Scouts Australia Child Protection Policy.
- Member health, and medical information, including Medicare and private health fund numbers, for youth members at the time of applying for membership, as well as each time we seek parent, guardian and care-giver permission for the young person to attend a Scouting activity. Health and medical information is also sought from adult members attending major activities and events for use in medical situations. Branches may also collect health and medical information from members directly or from health care providers or from parents, guardians, care-givers, Scouts staff and leaders.

Scouts Australia will not use **sensitive information** collected from members for the purpose of any direct marketing unless they have consented to the use or disclosure of the sensitive information for that purpose.

7. CONSENT POLICY

Custodian Branches are to ensure that when a member joins Scouting, provision and statements are made in membership application forms that seek agreement for Scouts Australia to use member information to send information about Scouting and its activities and services that we feel may be of interest to them. Application forms must also seek agreement that Scouts Australia may contact members directly, from time to time to obtain their feedback about its activities and services. Those provisions must also provide

the option to Opt-Out from those provisions. It is important to indicate that should they elect to Opt-Out, Scouts Australia may not be able to provide members with all of the associated services and information they may need to be an effective member.

On joining, members must be made aware that it is a condition of membership that they agree to the collection of sensitive information for the purposes disclosed in this policy. It must be stipulated that the authority to access this information is not discretionary for any applicant. In accordance with the Scouts Australia Child Protection Policy, an application for adult membership cannot proceed without this authority. These caveats are to be contained in all Branch applications for membership.

Scouts Australia will not use personal information for any purpose that a member would not reasonably expect. In particular, at State Branch custodian level, a members information may be used to offer other products, services and activities that will enhance the Scouting-member relationship. Members must be provided with the option of Opting-Out from these provisions at any other time by informing custodian Branches in writing, that they do not wish to be contacted in this way. Scouts Australia assumes that existing members have given this consent unless they advise their custodian Branch otherwise.

8. USE AND DISCLOSURE

By signing the Branch membership application form, a member consents to his/her personal information being used in the following ways:

- To maintain a register of membership.
- To respond to requests or help us process any request for Scouting activities or services.
- To effectively administer all activities and services provided to members.
- To communicate with members about Scouting activities and services.
- To inform members of relevant internal or external activities, events, promotions or special offers that may be of interest.
- To identify 'demographic' details of our membership for the purpose of building membership.
- To ensure as best as practicable, the safety, health and well-being of all members while they participate in Scout activities.
- To carry out research, marketing or development of our products, activities and services including the surveying of members about their needs and attitudes.
- To provide contact information to enable communication between members (approved at Branch HQ level)
- To assess the suitability of adult members for membership.
- To provide information and/or to report to the relevant authorities when necessary.
- To direct membership inquiries to Scout sub-entities.
- To direct inquiries to Scout managers regarding the use or hire of Scout property or services.
- To assess, process and investigate claims made under any insurance products that Scouting maintains.

We will share certain information with the authorities where it is legally our responsibility to do so, and, when we decide that this is necessary in the interests of child protection and/or member safety. Scouts Australia may also share information with an authority for the purpose of screening its members and where disclosure is required or authorised for law enforcement or regulatory purposes.

Members may specifically require that their personal contact details (including home phone number) NOT be provided to any other Scout member for the purpose of communication between members by advising custodian Branches in writing of this requirement. Branches are to make provision for this option and communicate this to their members.

Scouts Australia will give proper and responsible consideration to privacy issues associated with the introduction of new marketing methods or technology and it will not knowingly disclose member personal information to overseas recipients, unless the member has provided consent.

9. DATA QUALITY AND INTEGRITY

Scouts Australia relies on the accuracy of the information that members provide. Members should be reminded of the requirement to notify their custodian Branches promptly if there are changes to the personal information held by them.

10. DATA ACCESS AND CORRECTION

Branches are to ensure that members can, at any time, request access to their personal information. Branches should process a request of this nature within a reasonable time (usually 10 business days). Branch policies should provide advice to members as to how they can examine and request amendment of their personal information. Before giving a member access to their records, either in person or over the phone, Branches should seek proof of identity before release.

Scouts Australia, from time to time, will update member personal information based on the information received as members apply for training courses, attend events or complete application forms other than those completed on joining. If for any reason Scouts Australia (custodian Branches) declines to give a member access to their personal information or declines to amend a member's personal information, they are to provide the member with written notice (within 10 business days) that sets out the reasons for the decline and the mechanism available to complain about the decline.

The provisions contained in Section 10 pertain to a member's information only and not to any other information that the Scouts Branch or entity may hold.

11. ACCESS TO DATA BY MEMBERS

Scouting is essentially a 'volunteer' organisation. Communication between members is of primary importance for the organisation's operations and therefore the provision of contact details to members to allow them to make contact with other members is most important. Additionally, the provision of some personal information about members to other members (whose role may be to supervise and in some cases assess the performance of those members) is also essential to our program.

Some personal information, may be shared with other members at Branch level consistent with the primary purpose (section 2). Staff of the organisation, including event staff and member volunteers, may have access to health and medical information for the purpose of ensuring the health, well-being and protection of the organisation's members. Information may be provided to another member of Scouting for these bona fide purposes.

Scouts Australia may also publish from time to time, a contact list showing personal contact details for a select list of senior adult members. This list is provided to all those on the list and to other adult members for contact purposes. As above, you may specifically require that your personal contact details (including home phone number) NOT be included on these lists by advising Scouts Australia or the custodian Branch in writing.

12. ACCESS TO DATA BY NON-MEMBERS

Access to personal information by non-members, except custodial parents, guardians, care-givers and authorised volunteer adults in Scouting is not permitted, subject to other provisions of this policy and as set out in this paragraph. Personally identifiable data is not provided to external parties except where Scouts Australia has a duty to disclose that information, or where disclosure is required or authorised for law enforcement or regulatory purposes (as above).

Healthcare staff such as doctors, nurses, paramedics and first aid staff at events may have access to or be provided with health and medical information of members for the purpose of ensuring the health, well-being and protection of the organisation's members. Where it is an emergency or, in the organisation's view withholding the information could severely endanger a member's life, health or safety or pose a serious threat to public health or safety, a member's health and medical information may be released to another health care provider without seeking consent beforehand. Branches and host Branches of major events are to ensure that this privacy provision is made known to members as appropriate.

International Scouting Activities. Scouts Australia collects information from members through an application process for all international Scouting activities. The collection of this data provides Scouts Australia with the information required to effectively manage participation in these activities.

Scouts Australia transfers this data to the host organisation for the respective event. Data includes personal details for co-ordinating resources, medical details for welfare/health support, job preferences for service roles etc. The management of data at this point is the responsibility of the host organisation and its Privacy Policies.

13. DATA SECURITY

Scouts Australia takes all reasonable steps to protect the personal information of members from misuse, interference, loss, unauthorised access, modification or disclosure.

Scouts Australia expects that all levels of Scouting have physical, electronic and procedural safeguards in place to protect member information. For example, member personal information in the form of original or copies of paper forms are to be stored in secured containers in secured premises. Certain information may also be held by authorised voluntary adults at lower levels than the Branch Headquarters. In these cases, the senior volunteer or staff adults are accountable for the security and privacy of member data at that location. In all location circumstances, and at all levels, the security measures to be adopted should include regularly changing passwords; encryption and off-site duplication and storage.

The custodian Branch Headquarters in each State and Territory is the sole location of the State consolidated electronic membership databases. Access to information stored electronically is to be restricted to authorised personnel who require that level of access only, including restrictions on the nature of that access such as Read-Only or Edit access.. All authorised personnel must require logins and passwords for access to this information. Scouts Australia requires that all volunteers and staff are to maintain the confidentiality of customer and member information and ensure appropriate security of all usernames and passwords used to access Scout membership systems.

Each custodian Branch is to ensure that their member databases are secured and backed-up on a regular basis to a secure off-site location.

Any visitor, to any Scout premises containing member data and information is required to be signed-in and out (at a Scout HQ) and/or accompanied or observed at all times by a member of staff or an authorised volunteer adult while on the premises.

Custodian Branches are to destroy or de-identify any personal information such as reports as soon as the information is no longer required by Scouting. Branches may retain physical and electronic information pertaining to past members for specific purposes in their membership databases and historical archives.

14. DATA BREACH

Although Scouts Australia takes all reasonable steps to secure member data, the example Data Breach Response Plan at ANNEX A details the steps that are to be taken in the event of a data breach.

15. COMMERCIAL USE OF DATA AND MARKETING

There are occasions when external organisations or individuals wish to offer a product or service which we consider would be beneficial or of interest to Scouts Australia members. Subject to Scouts Australia's assessment and approval of the external organisation and its material, the agreement of the specific custodian Branches and a signed agreement with the external organisation, the Custodian Branch may provide a mailing service for that external organisation. Scouts Australia does not provide membership information directly to an external party without approval from the Custodian Branch or as prescribed in this policy.

At times Scouts Australia relies on third party suppliers to conduct specialised activities such as bulk mail outs, data processing, printing etc. These agents act on behalf of Scouts Australia and are not permitted to use any information in the process for their own commercial benefit. While member personal information may be provided to these agents to enable them to perform their agreed tasks, such information remains the property of Scouts Australia and its custodian Branches at all times and the service providers are to be bound by specific confidentiality, non-disclosure agreements and data disposal protocols.

16. PHOTOGRAPHS AND IMAGES

Photographs of persons may be used for marketing purposes in accordance with the Scouts Australia and Branch Marketing and PR Plans. Scouts Australia and its sub-entities are to use suppliers and partners who are signatories to the Australian Direct Marketing Association (ADMA) Code of Ethics in relation to all direct marketing and electronic marketing to members. Custodian Branches are to ensure that their membership application forms contain an approval for the above marketing purposes. Members are to be given the opportunity to specifically Opt-Out in those forms. Members are to be given the opportunity to Opt-Out at other times by:

- contacting the National/Branch responsible membership manager
- 'unsubscribing' from email marketing messages, which are always to include an unsubscribe option
- attending or sending written advice to the relevant Scout offices and requesting to be removed from any email and/or postal marketing

17. WEBSITE AND ONLINE SERVICES

Scouts Australia does not collect any personal information via our web sites except when members knowingly provide it. If members have elected to be a 'registered user' Scouts Australia may use member information to send to a member various promotional offers, Scout program information, special events or other marketing communications that may be of interest to the member. Whenever we send a member an email or message for a commercial purpose, that correspondence is to provide an option to 'unsubscribe'.

Scouts Australia takes reasonable steps to ensure that member information online is secure from any unauthorised access or disclosure. We have incorporated security procedures and practices that we consider are consistent with Australian industry practice. We review our security procedures from time to time and update them when we deem necessary. The use of information that a member decides to provide to a third party on the internet (outside our website and its levels of protection) falls outside this statement. Scouts Australia cannot assume responsibility and makes no warranties or representations regarding the information practices of third-party sites where a member is able to access their sites through ours. We encourage Scout users to review each site's privacy policy before disclosing any personally identifiable information.

Members may elect to use an e-commerce section of Scouts Australia websites to purchase products and to pay for those products using a debit/credit card. Scouts Australia mandates that these transactions (at all levels) are to use an industry standard encryption code. Scouts Australia and its sub-entities do not retain member credit card details.

For statistical purposes Scouts Australia may collect non-personalised information on website activity (such as the number of users who visit the website and navigation patterns) through the use of tracking technology. In order to collect statistics we may anonymously log information, and identify categories of users by items such as domains and browser types.

18. MEMBER RIGHTS

All members are to be advised that they are not bound to provide certain personal information. However, without that information, Scouts Australia may not be able to process an application, fulfil a request to become a member or provide members with an appropriate level of service including member health, safety and medical needs.

Members are entitled to request their own personal information records held by Scouts Australia, its Branches and sub-entities at any time for correction or checking, and, members may at any time choose to cancel or opt-out of any Scout service or mailing. Members may also elect to advise that their phone numbers are to be marked 'silent' in which case Scouts Australia will not release or publish them in any form, and members may also withdraw permission to use their information or image for marketing purposes. Custodian Branches are to advise members of these privacy rights.

As per Section 10 comment. The provisions contained in Section 18 pertain to a member's information only and not to any other information that the Scouts Branch or entity may hold.

19. COMPLAINTS RESOLUTION

Custodian Branches are to ensure that members are advised about their right to make a complaint about Scouts Australia's collection, use or security of their information and about how to make that complaint. Generally, this should include the contact details of the 'responsible officer' as well as the privacy regulator (the OAI Commissioner). An example text is as follows:

"If you lodge a complaint about the handling of your personal information, the Branch Chief Executive Officer will respond to you as soon as possible. We will aim to deal with your complaint at the source of the complaint. If you are not satisfied with the response you receive, please let us know and our Branch Chief Executive Officer will investigate further and respond to you.

After an initial complaint, if you are unsatisfied with our resolution, and in accordance with the Privacy Act, you may escalate your complaint to the Office of Australian Information Commissioner (OAIC) after 30 days have passed from when you informed us of your complaint. Complaints to the OAIC must be made in writing, preferably using the online Privacy Complaint Form which can be found at http://www.oaic.gov.au/privacy/making-a-privacy-complaint. The OAIC can also be contacted via its enquiries line on 1300 363 992. The specific address for the OAIC is: GPO Box 5218, Sydney NSW 2001 (Email: enquires@oaic.gov.au).

Note: The Federal Government has proposed the abolition of the OAIC and if this ultimately occurs complaints can be made to the Privacy Commissioner instead of the OAIC."

20. PRIVACY POLICY AMENDMENT

The information contained in this Policy relates to the Scouts Australia current privacy standards. Scouts Australia may vary it's privacy standards from time to time.

Amendments to this policy are only to be authorised by the Scouts Australia National Executive Committee.

RESPONSIBILITY

A DATA BREACH occurs when personal information that we hold is subject to unauthorised access or disclosure, or is lost. Importantly, the faster we respond to a breach the better our ability will be to contain the breach, assess the ramifications, notify individuals and the regulator where required and to review the situation, and our own systems and performance to prevent a similar occurrence. Some examples of a Data Breach are:

- A computer containing personal information is stolen from a Scout Hall
- The Branch HQ is subject to a break-in or cyber-attack which accesses our membership systems
- Scout member information is inadvertently shared with a third party without consent

As an organisation which highly values the safety and wellbeing of our members, we all share a responsibility to protect personal information at every level. Whereas the custodian Branch CEO/Responsible Officer ultimately carries the responsibility for data and personal security at the Branch level, all adults who have been given access to and management of personal information (custodians) have the responsibility to the Branch for the security of that information, and, for the reporting of any breaches to the Branch HQ.

We have established robust systems and procedures which are designed to limit access to and provide a measure of security for the information that we hold. These systems are regularly reviewed and updated to ensure they perform as expected. Importantly, every Branch Scout entity (National Office; custodian Branch; Region/District/Group/Major & Minor Event Contingent/Business unit and Scout premises manager) is responsible for the security of personal information it holds of our members and clients. We recognise that systems can be inadvertently or intentionally breached and that physical and cyber security measures will not always be perfect. To this end, the **DATA BREACH RESPONSE PLAN** below has been designed to ensure that if and when a breach occurs, our response is in accordance with our responsibilities, and that it is swift and efficient.

DATA BREACH RESPONSE PLAN

1. **When we suspect, know or are advised of a data breach – immediate action**
   Where we discover that there has been an unauthorised access; unauthorised disclosure; or loss of retained personal information, we will commence an assessment of that breach (suspected or known) **immediately.** Our Branch Membership Manager and the CEO will conduct this initial assessment. Our immediate actions on discovery are:
   a. **Pre-discovery: We mandate that all suspected or known Data Breaches are to be reported to the Branch Membership Manager (or the Branch HQ) as they are found or discovered.**
   b. **The Branch Membership Manager will immediately investigate and determine the location, persons involved, how the breach occurred, and an initial understanding of the severity of the Breach. This initial information will be reported to the CEO or the Branch GM Operations. A record of the breach, actions taken / planned will be recorded in the Data Breach Register. All further updates, resolutions, etc will be recorded against this entry and this register will be made available to the OAIC should it be called upon.**
   c. **The CEO may take an immediate decision to advise the affected person(s) by phone and email depending on the nature of the breach (and an initial assessment of potential harm).**
   d. **The CEO will decide if the matter is to be referred to a 'Data Breach Response Team' or continue to be managed by the Branch Membership Manager.**
   e. **The core 'Data Breach Response Team' will consist of the CEO, the Branch Membership Manager; the Branch Volunteer Support Manager; the Branch Risk & Compliance Manager; the volunteer or staff manager of the site/location/event/activity/Scout hall; and the PA to the Chief Commissioner. External support from our IT and Business Systems partners will also form part of the Data Breach Response Team as required.**
   f. **Notwithstanding the decision at sub para 1d, the CEO may take any immediate action possible that may reduce the impact of the breach.**
   g. **The CEO may also alert the Branch marketing staff, the Branch insurance partners and our external IT and Business Systems partners as required.**

h. **Once the CEO has received an initial report (1 to 3 days) they will make a decision whether to advise the affected person(s) and or make a report through the NDB Scheme.**

2. **We will contain the breach**

During the assessment phase, we will also take all steps possible to contain and minimise any harm that may develop as a result of the breach. This may include changing passwords, retrieving information, shutting down certain information systems, and directing containment at the breach site. Methods of containing a breach will vary on a case-by-case basis. These could comprise:

a. **Advising the affected person(s) regardless of the potential need to report to the Privacy Commissioner so that that affected person(s) can take their own containment action;**
b. **Centrally restricting access to certain information systems;**
c. **Retrieving records (physically and or electronically);**
d. **Securing premises and preventing further entry;**
e. **Requesting potential unintended recipients to ignore/delete if appropriate;**
f. **Changing Passwords and/or restricting access to hardware;**
g. **Reporting a matter to the Police or other security agency;**
h. **Requesting our IT; business system and security partners to investigate and report on the breach for subsequent security action or sharing with the authorities; and**
i. **Advise the affected person(s) of our actions.**

3. **We will fully assess the breach (within 30 days)**

The Branch CEO will consider whether the data breach is likely to result in **serious harm** to any person. We will also gather information to determine if our remedial action was able to prevent the likely risk of serious harm. From this assessment, we will make an evidence-based decision about whether serious harm is likely or unpreventable. If this is the case, the matter will be reported to the Privacy Commissioner. The resultant written assessment by the Data Breach Response Team (if used) or the CEO's determination as well as the containment and preventative measures taken, will be reported to the Board (BEC) on every occasion.

4. **We will notify**

The Branch CEO will notify an affected person(s) regardless of the need to notify the Privacy Commissioner. Where serious harm has occurred or is likely, and our preventative measures have not prevented that harm, the Branch CEO will prepare and send a statement for the Privacy Commissioner that contains:

a. **The identity of Scouts Australia and our contact details**
b. **A full description of the breach**
c. **The actual information that was breached**
d. **Our recommendations for the persons concerned**

We will share the contents of the above statement with the following (as appropriate):

a. **Only those persons at direct risk of harm, and/or**
b. **With persons we believe should know, and/or**
c. **Publish relevant contents of the statement on the custodian Branch website and Leader updates and communications' so that all Scout custodians can learn from the breach.**

5. **We will engage**

We will directly engage with any person who has been affected by the breach and will take pro-active action to mitigate any harm. We will offer further assistance as and if required to the person(s) affected and take action to ensure we strengthen our systems where weaknesses are identified.

6. **We will review**

We will conduct a full review of the breach and our response (including surveying the persons concerned) in an effort to prevent future breaches. This review will include:

a. **An assessment of the recommendations of the investigation conducted.**
b. **The development of a prevention plan for future breaches.**
c. **Conducting regular audits to ensure the plan is working.**
d. **Updating our security where required and monitoring the areas of weakness.**
e. **Reviewing our Privacy Policy and other security arrangements.**
f. **Communicating with and upskilling custodians with the lessons learned.**
g. **Closure and approval of the data breach item as recorded in the data breach register.**