

# Privacy Policy

## Purpose of this Policy

**SIDS and Kids South Australia** is committed to providing quality services to you and this policy outlines our ongoing obligations to you in respect of how we manage your Personal Information.

We have adopted the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) (the Privacy Act). The APPs govern the way in which we collect, use, disclose, store, secure and dispose of your Personal Information.

A copy of the Australian Privacy Principles may be obtained from the website of The Office of the Australian Information Commissioner at [www.aaic.gov.au](http://www.aaic.gov.au)

## What is Personal Information and why do we collect it?

Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect include: names, addresses, email addresses, phone and facsimile numbers.

This Personal Information is obtained in many ways including correspondence, by telephone and by email, via our website [www.sidssa.org](http://www.sidssa.org), from your website, from social media, publications, from other publicly available sources.

We collect your Personal Information for the primary purpose of providing our services to you, providing information to our clients and marketing. We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. You may unsubscribe from our mailing/marketing lists at any time by contacting us in writing.

When we collect Personal Information we will, where appropriate and where possible, explain to you why we are collecting the information and how we plan to use it.

## Sensitive Information

Sensitive information is defined in the Privacy Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political

association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information.

Sensitive information will be used by us only:

- For the primary purpose for which it was obtained
- For a secondary purpose that is directly related to the primary purpose
- With your consent; or where required or authorised by law.

## **Third Parties**

Where reasonable and practicable to do so, we will collect your Personal Information only from you. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party.

## **Disclosure of Personal Information**

Your Personal Information may be disclosed in a number of circumstances including the following:

- Third parties where you consent to the use or disclosure; and
- Where required or authorised by law.

## **Security of Personal and Sensitive Information**

Your Personal and Sensitive Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorized access, modification or disclosure.

When your Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your Information. However, most of the Information is or will be stored in client files which will be kept by us for a minimum of 7 years.

## **Access to your Personal Information**

You may access the Personal Information we hold about you and to update and/or correct it, subject to certain exceptions. If you wish to access your Personal Information, please contact us in writing.

SIDS and Kids SA will not charge any fee for your access request. In order to protect your Personal Information we may require identification from you before releasing the requested information.

## **Maintaining the Quality of your Personal Information**

It is an important to us that your Personal Information is up to date. We will take reasonable steps to make sure that your Personal Information is accurate, complete and up-to-date. If you find that the information we have is not up to date or is inaccurate, please advise us as soon as practicable so we can update our records and ensure we can continue to provide quality services to you.

## **Privacy Breach**

SIDS and Kids SA takes reasonable steps to protect the **Personal and Sensitive Information** we hold from misuse, interference, loss, unauthorised access, modification or disclosure.

We will take seriously and deal promptly with any accidental or unauthorised disclosure of personal or sensitive information. All employees are made aware of their obligations to handle personal or sensitive information in accordance with the Privacy Act. Our practices and procedures are regularly reviewed to ensure ongoing compliance.

Where an accidental or unauthorised use or disclosure occurs, SIDS and Kids SA will act quickly to rectify and remedy the situation. Refer Appendix 1 for our Data Breach Response Plan.

Any employee, Board member or volunteer of SIDS and Kids SA identified as breaching this policy will be subject to appropriate action. For employees, that may include termination of employment.

## **Privacy Policy Complaints and Enquiries**

If you have any queries or complaints about our Privacy Policy please contact the CEO of SIDS and Kids SA on 08 8332 1066 or [ceo@sidssa.org](mailto:ceo@sidssa.org).

## Data Breach Response Plan

1. On identification of a suspected privacy breach, a SIDS and Kids SA staff member must immediately notify the CEO of the time and date the suspected breach was discovered, the type of information involved, the cause and extent of the breach, and the context of the affected information and the breach.
2. The CEO will assess the details of the suspected breach and determine whether a data breach has occurred. If the CEO has any suspicion that a breach has occurred, they must immediately notify the President of the Board of Directors of SIDS and Kids SA (or an authorised delegate).
3. In some instances, a minor breach may be able to be dealt with at the director level. In such case, the following details must be recorded:
  - a) a description of the breach or suspected breach;
  - b) action taken by the Director, CEO or SIDS and Kids SA staff member to address the breach or suspected breach;
  - c) outcome of that action;
  - d) sign off from the Director that no further action is required; and
  - e) confirmation that the incident has been recorded in the SIDS and Kids SA Data Breach Incident Log.
4. In the case of a serious breach, it must immediately be escalated to the Data Breach Response Team comprising the CEO, Board President, Legal Officer and an IT Representative (where electronic data involved).
5. The Data Breach Response Team will undertake the following process:
  - Step 1: Contain the breach and do a preliminary assessment
  - Step 2: Evaluate the risks associated with the breach
  - Step 3: Notify affected individuals or entities or third parties, as appropriate
  - Step 4: Prevent future breaches