PRIVACY POLICY

10 Vincentia Street, Marsfield 2122
Post: PO Box 1653, North Ryde 2113
Phone: 9887 2299 | Fax: 9878 4564
ABN: 11 850 625 970 | CFN: 21669

Minimbah Challenge Inc

Privacy Policy

Contents

Introduction

Minimbah Challenge Inc is bound by the Privacy Act 1988 (Privacy Act). Any personal information we collect will be handled in accordance with the Australian Privacy Principles (APPs) outlined in the Privacy Act and any applicable state or territory legislation.

Privacy law is regulated by the Australian Information Commissioner. Further information about privacy legislation can be obtained from the Office of the Australian Information Commissioner website at: www.oaic.gov.au

Purpose

This privacy policy sets out how Minimbah Challenge Inc complies with its obligations under the Privacy Act regarding the collection, use, disclosure, storage, security and access of the personal information of clients, donors, members, volunteers, job applicants and staff.

Policy

1. We respect your privacy - Minimbah Challenge Inc is committed to maintaining the privacy of your personal information. This policy sets out how we collect, use and manage personal information in accordance with the Privacy Act and APPs contained therein.

2. Collection of personal information - The Privacy Act defines personal information as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." Minimbah Challenge Inc will only collect personal information necessary to deliver our services and conduct the business activities that support this. We may collect the following types of personal information: contact details; details for next of kin or emergency contact; NDIS records; job applications; payment details and other information relevant to the relationship of the individual with Minimbah Challenge Inc. We may also collect sensitive information such as details of a medical information where supplied; incidents reports; complaint; racial or ethnic origin; health information where relevant to the supports to be provided to clients.

3. Information collected on our website - In common with many websites we may collect aggregated information which tells us about visitors to the Minimbah Challenge Inc site but not the identity of those visitors. For example, we may collect information about the date, time and duration of visits and which pages of the Minimbah Challenge Inc website are most

commonly accessed. This information is used by us to help to administer and improve the Minimbah Challenge Inc website. The Minimbah Challenge Inc website may use 'cookies'. Cookies are small files which are stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client and website, and can be accessed either by the web server or the client computer. This allows the server to deliver a page tailored to a particular user, or the page itself can contain some script which is aware of the data in the cookie and so is able to carry information from one visit to the website (or related site) to the next. Cookies may also be used to manage security and store information about the type of browser being used. With most internet browsers, users can erase cookies from their computer, block all cookies, or receive a warning before a cookie is stored. However, some parts of the Minimbah Challenge Inc site may not function fully for users that disallow cookies.

4. Methods of collecting personal information - Minimbah Challenge Inc collects personal information through a variety of methods including electronic or face to face interactions; interaction with our website; requests for information; and provision of goods and services. We collect personal information directly from individuals or their authorised representatives; through referrals from other service providers; donations; or information shared with your permission.

5. Use of personal information - Minimbah Challenge Inc uses personal information to provide supports and services. We may also use personal information to notify individuals of information and opportunities they may be interested in. De-identified data may be used to meet regulatory and funding requirements or for the purposes of internal reporting and improvement of services. Where not previously requested, and in accordance with Privacy legislation, we may use personal information to communicate with individuals through newsletters or direct marketing. All such communications will provide an option to opt out or unsubscribe.

6. Security of personal information - Minimbah Challenge Inc will take reasonable steps to protect personal information from misuse, interference and loss, unauthorised access, modification or disclosure. Personal information held by Minimbah Challenge Inc is stored electronically in secure databases, or where retention of hard copy documents is required, in secure filing systems. Only authorised Minimbah Challenge Inc personnel are provided with access to individuals' personal information. Where personal information is no longer required by the Minimbah Challenge Inc, or where required by law, Minimbah Challenge Inc will take reasonable steps to securely destroy or de-identify information in accordance with legal requirements for retention and disposal.

7. Data Breach Notification – Minimbah Challenge Inc accepts its obligation to keep personal information safe and is open and transparent in how data is handled. In the event that personal data systems are breached, data is misused or lost, then Minimbah Challenge Inc will take all reasonable and practicable means to contact individuals whose personal information is involved. Minimbah Challenge Inc will advise such individuals of the extent of the data breach (if known) and advise individuals of the most appropriate means of regaining control of their information, in an effort to limit the personal impact of the breach. If appropriate, Minimbah Challenge Inc will also report any breach of data to the Office of the Australian Information Commissioner (OAIC).

8. Access and correction - Individuals may request access to the personal information Minimbah Challenge Inc holds about them. Where reasonable and practicable to do so, and in accordance with the provisions of the Privacy Act, Minimbah Challenge Inc will provide supervised access to an individual's personal information. Requests to access personal information must be made in writing, either by email or hard copy. In the event access to records requires a significant allocation of resources, we may charge a reasonable administration fee to cover costs. Corrections or updates to personal information supplied by clients or their authorised representatives must be made by the individual or their authorised representative. In all cases, Minimbah Challenge Inc staff must be satisfied changes are authorised by the individual in question. Requests to change personal information supplied by clients or their authorised representative will be actioned as a priority.

9. Disclosure of personal information overseas - Minimbah Challenge Inc will generally disclose an individual's personal information to an overseas entity where an individual or their authorised representative explicitly requests disclosure of their personal information to the overseas entity to enable the individual to receive services in that country. Minimbah Challenge Inc strives to ensure all that all participant information is stored on Australian servers. Where local services are unavailable, however, or cost prohibitive, Minimbah Challenge Inc will take reasonable steps to ensure that the overseas recipient does not breach the APPs. Countries in which we may engage providers to complete this type of activity include China, Hong Kong, Singapore and India.

10. Use, adoption or disclosure of government related identifiers - Except in relation to a clinical referral to another agency on behalf of the client, Minimbah Challenge Inc will not use, adopt or disclose an identifier assigned to an individual by a Commonwealth agency unless required to by law or where reasonably necessary and in accordance with the APPs.

11. Anonymity and pseudonymity - Where practical, individuals may deal with Minimbah Challenge Inc anonymously or using a pseudonym. The majority of our services, however, will require collection of personal information to enable Minimbah Challenge Inc to provide the appropriate goods, services or response.

12. Review and improvement - Minimbah Challenge Inc may update this Privacy Policy from time to time to reflect changes to legislation or internal process improvements. An up to date copy of this policy is freely available on request by contacting Reception or reception@minimbah.org.au .

13. Complaints and enquiries - Minimbah Challenge Inc takes all complaints seriously and confidentially. To lodge a complaint, either contact the CEO on (02) 9887 2299; or the Minimbah President at president@minimbah.org.au. Requests or enquiries regarding this privacy policy or personal information held by Minimbah Challenge Inc can be made by email: admin@minimbah.org.au or by phoning our Marsfield office on (02) 9887 2299.

Definitions

Australian Privacy Principles (APPs): principles pertaining to the handling of personal information as set out in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) (Reform Act).

Client: Any person and/or their nominated representative, who engages the services of Minimbah Challenge Inc.

Donors: All persons who participate in or support revenue generation activities for Minimbah Challenge Inc.

Identifier: A number or code assigned by Minimbah to an individual to identify uniquely the individual for the purposes of the Minimbah's operations that is not identifiable with any number or code assigned to that individual by the Commonwealth.

Individual: a client, donor, family member, volunteer, job applicant, or staff member of Minimbah Challenge Inc.

Sensitive information: a subset of personal information. Includes information or an opinion about an individual's racial or ethnic origin, political opinions, memberships, religious beliefs, sexual orientation, health information, criminal record or genetic information.

Staff: All paid and unpaid persons undertaking work for Minimbah Challenge Inc, including employees, volunteers, individuals on work experience, student placements, secondments and contractors.

OAIC: Office of the Australian Information Commissioner. The OAIC is responsible for Privacy, Freedom of Information and information policy.

Cross References

- Privacy Act 1988 & Australian Privacy Principles
- Applicable state and territory health and information privacy legislation

Authorised by
Wayne Newell, Chief Executive Officer

Document control

Original Document Date: June 2010
Effective reviewed date: 8 January 2020
Prepared by: Minimbah Challenge Inc CEO/Privacy Officer

Approved by: Minimbah Challenge Inc Committee of Management
Document identifier: Minimbah Challenge Inc Privacy Policy

Next review*: January 2023

* Unless otherwise indicated, this policy will still apply beyond the review date.

Data Breach Procedure and Response Plan

This procedure sets out the processes to be followed by Minimbah staff in the event that Minimbah experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

---

1. Introduction

This Procedure is governed by the Minimbah Challenge Inc (**Minimbah**) *Privacy Policy*.

Minimbah is committed to managing personal information in accordance with the *Privacy Act 1988 (Cth)* (the Act) and the Minimbah Privacy Policy.

This document sets out the processes to be followed by Minimbah staff in the event that Minimbah experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, personal information.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (NDB Act) established a Notifiable Data Breaches (NDB) scheme requiring organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

Accordingly, Minimbah needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether it is likely to result in serious harm and whether it constitutes an NDB.

Adherence to this Procedure and Response Plan will ensure that Minimbah can contain, assess and respond to data breaches expeditiously and mitigate potential harm to the person(s) affected.

This Procedure and Response Plan has been informed by:

- The Office of the Australian Information Commissioner's *"Guide to developing a data breach response plan*"
- The Office of the Australian Information Commissioner's *"Data breach notification guide: a guide to handling personal information security breaches*"
- NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)

This document should be read in conjunction with *Minimbah's Privacy Policy*.

2. Process where a breach occurs or is suspected

2.1 Alert

Where a privacy data breach is known to have occurred (or is suspected) any member of Minimbah staff who becomes aware of this must, within 24 hours, alert the CEO or Care Manager in the first instance.

The Information that should be provided (if known) at this point includes:

a) When the breach occurred (time and date)
b) Description of the breach (type of personal information involved)
c) Cause of the breach (if known) otherwise how it was discovered
d) Which system(s) if any are affected
e) What information may be impacted
f) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

2.2 Assess and determine the potential impact

Once notified of the information above, the CEO or Care Manager ***must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.***

2.2.1 Criteria for determining whether a privacy data breach has occurred

a) Is personal information involved?
b) Is the personal information of a sensitive nature?
c) Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

2.2.2 Criteria for determining severity

a) The type and extent of personal information involved
b) Whether multiple individuals have been affected
c) Whether the information is protected by any security measures (password protection or encryption)
d) The person or kinds of people who now have access
e) Whether there is (or could there be) a real risk of serious harm to the affected individuals
f) Whether there could be media or stakeholder attention as a result of the breach or suspect breach

With respect to 2.2.2(e) above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation.

Having considered the matters in 2.2.1 and 2.2.2, the CEO or Care Manager must notify the Privacy Officer within 24 hours of being alerted under 2.1.

2.3 CEO/Privacy Officer to issue pre-emptive instructions

Following 2.2, the CEO/Privacy Officer will take a preliminary view as to whether the breach (or suspected breach) may constitute an NDB. Accordingly, they will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Minimbah Committee of Management. This will depend on the nature and severity of the breach.

2.3.1 Data breach managed at the local level

Where the CEO/Privacy Officer instructs that the data breach is to be managed at the local level, the Care Manager must:

a) ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system); and
b) submit a report via the Privacy Coordinator within 48 hours of receiving instructions under 3.3. The report must contain the following:

- Description of breach or suspected breach;
- Action taken;
- Outcome of action;
- Processes that have been implemented to prevent a repeat of the situation; and
- Recommendation that no further action is necessary.

The CEO/Privacy Officer will be provided with a copy of the report and will sign-off that no further action is required.

2.3.2 Data breach managed by the Minimbah Committee of Management

Where the CEO/Privacy Officer instructs that the data breach must be escalated to the Minimbah Committee of Management, they will convene a meeting of the Committee of Management, through the President, as soon as is practicable.

2.4 Primary role of the Minimbah Committee of Management in relation to a data breach

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Committee of Management (as appropriate):

a) Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
b) evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined in sections 2.2.1 and 2.2.2 above.
c) Call upon the expertise of, or consult with, relevant staff in the particular circumstances.

d) Engage an independent cyber security or forensic expert as appropriate.
e) Assess whether serious harm is likely (with reference to section 2.2.2 above and section 26WG of the NDB Act).
f) Make a recommendation to the CEO/Privacy Officer whether this breach constitutes an NDB for the purpose of mandatory reporting to the OAIC and the practicality of notifying affected individuals.
g) Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media.

The Minimbah Committee of Management must undertake its assessment within 48 hours of being convened.

The CEO/Privacy Officer will provide periodic updates to the Minimbah President as deemed appropriate.

2.5 Notification

Having regard to the Minimbah Committee of Management's recommendation in 2.4 above, the CEO/Privacy Officer will determine whether there are reasonable grounds to suspect that an NDB has occurred.

If there are reasonable grounds, the CEO/Privacy Officer must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

A template can be found at **Annexure B**.

If practicable, Minimbah must also notify each individual to whom the relevant personal information relates. Where impracticable, Minimbah must take reasonable steps to publicise the statement.

2.6 Secondary Role of the Minimbah Committee of Management in relation to a data breach

Once the matters referred to in 2.4 and 2.5 have been dealt with, the Minimbah Committee of Management should turn attention to the following:

- Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training.
- Prepare a report for submission to Senate.
- Consider the option of an audit to ensure necessary outcomes are affected and effective.

3. Updates to this Procedure

In line with continuous improvement, this procedure is scheduled for review every five years or more frequently if appropriate.

4. Revisions made to this Procedure

Date	Major or Minor Revision	Description of Revision(s)
18 May 2018	Original approved copy	Completed

5. Contact details

Contact for all matters related to privacy, including complaints about breaches of privacy, should be directed as follows:

CEO/Privacy Coordinator

E: ceo@minimbah.org.au

T: 02 9887 2299

P: PO Box 968, North Sydney NSW 2059

Policy applies to	All Staff and volunteers
Policy Status	Revised Policy
Approval Authority	CEO
Governing Authority	Minimbah Committee of Management
Responsible Officer	CEO
Effective Date	10/01/2020
Date of Last Revision	Not Applicable
Date of Policy Review *	10/01/2023

* Unless otherwise indicated, this policy will still apply beyond the review date.