st george community

Privacy and Confidentiality Policy

Policy Statement

The Service will conform to both state and commonwealth privacy legislation requirements regarding the collection, use and protection of personal information of our Consumers and Team Members.

Policy Protocols

Confidentiality refers to the obligation of non-disclosure by this agency of personal information unless it has the consent of the person concerned.

The Service will ensure privacy and confidentiality by:

- Collecting only the information required for service delivery;
- Informing people of the purpose for collecting the information;
- Providing individuals with access to their information held by the Service;
- Disclosing personal information to 3rd parties only with the written consent of the individual;
- Securely storing Consumers personal information; and
- Destroying information in accordance with the Archives Act 1983.

In the following circumstances there is an obligation to report:

- a crime or intended crime;
- where the person is suicidal, safety is at risk, personal harm or being harmed (abused) by another; and
- warn a third party who is in danger.

Agencies and organisations regulated under the Australian Privacy Act 1988 (Privacy Act) are required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach.

The Australian Privacy principles (APP's) apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (amends the Privacy Act 1988) outlines the 13 APP's:

APP1 – Open and Transparent Management of Personal Information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 – Anonymity and Pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 – Collection of Solicited Personal Information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing With Unsolicited Personal Information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of The Collection of Personal Information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use or Disclosure of Personal Information

Outlines the circumstances in which an APP entity may use of disclose personal information that it holds.

APP 7 – Direct Marketing

An organization may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-border Disclosure of Personal Information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 - Adoption, Use or Disclosure of Government Related Identifiers

Outlines the limited circumstances when an organization may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 – Quality of Personal Information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of Personal Information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorized access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to Personal Information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of Personal Information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

Adapted from APP-a summary for APP entities, Office of the Australian Information Commissioner. www.oaic.gov.au

National Data Breach Scheme

The National Data Breach Scheme applies from the 22 February 2018 to all agencies and organisations with existing personal information security obligations under the Privacy Act. It was established by the passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017.

The scheme includes an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. The Australian Information Commissioner must be notified of eligible data breaches. Notifications should be lodged through the Notifiable Data Breach form which is available at;

https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

Section 6 of the Privacy Amendment (Notifiable Data Breaches) Act 2017 says that the scheme applies to incidents where personal information is subject to unauthorised access or disclosure, or lost, following the scheme's commencement.

Examples of data breaches include:

- a device containing customer's personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person

Data breaches can cause significant harm in multiple ways. Individuals whose personal information is involved in a data breach may be at risk of serious harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of harm include:

- Financial fraud including unauthorised credit card transactions or credit fraud
- Identity theft causing financial loss or emotional and psychological harm
- Family Violence
- Physical harm or intimidation

In some circumstances the data breach is not reportable:

- If an entity takes action quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm.
- In some circumstances, if the data breach involves more than one entity
- An enforcement body does not need to notify individuals about an eligible data breach is some circumstances
- Exceptions to notifying individuals or the Commissioner may apply where a Commonwealth law prohibits or regulates the use or disclosure of information (a secrecy provision).
- In some circumstances, the Commissioner may declare by written notice that an entity does not need to comply with the National Data Breach Scheme notification requirements in relation to specific eligible data breach.

Related Documentation

- doc_055 Team Member Orientation
- doc_313 Service User Information Provision
- doc_138 Consumer User Rights and Responsibilities
- doc_280 Privacy and Confidentiality Procedure

Relevant Standards

Aged Care Quality Standards

1. Consumer Dignity and Choice
4. Service and Supports for Daily Living

NDIS Practice Standards

1. Rights & Responsibilities
6. Provider Governance and Operational Management