POLICY NO: CORPO-011	**VERSION NO: 6.0**
DATE OF IMPLEMENTATION: 22 May 2019	**REVIEW DATE: 22 May 2022**

Privacy Policy

Contents

Purpose

This Privacy and Confidentiality Policy defines the way in which ConnectaAbility Australia personal and other confidential information is to be protected.

Scope

This policy applies to all engaged with the ConnectAbility Australia community. This extends to our people, both paid and unpaid, in the delivery of engagement on behalf of ConnectAbility Australia. The policy outlines the minimum requirements and is compulsory.

Definitions

Term	Definition
Australian Privacy Principles (APP)	Australian Privacy Principles (APP): • legally binding principles which are the cornerstone of the privacy protection framework in the Privacy Act, • set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information, • apply to most Australian Government agencies and some private sector organisations — collectively referred to as APP entities. The APPs are grouped into five parts to reflect the personal information lifecycle: • Part 1 — Consideration of personal information privacy (APPs 1 and 2) • Part 2 — Collection of personal information (APPs 3, 4 and 5) • Part 3 — Dealing with personal information (APPs 6, 7, 8 and 9) • Part 4 — Integrity of personal information (APPs 10 and 11) • Part 5 — Access to, and correction of, personal information (APPs 12 and 13).
corporate information	Any non-public information pertaining to ConnectAbility Australia business.
data breach	A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.
de-identified information	Is information that is no longer about an identifiable individual or an individual who is reasonably identifiable. Generally, de-identification includes:

	1. removing personal identifiers, such as an individual's name, address, date of birth or other identifying information 2. removing or altering other information that may allow an individual to be identified, for example, a unique characteristic of the individual. De-identification may not altogether remove the risk that an individual can be re-identified.
government identifier	A number, letter or symbol, or a combination of any or all of those things, used to identify the individual or to verify the identity of the individual.
ConnectAbility Australia community	All persons involved in all current, and future and new business operations under the direction of ConnectAbility Australia.
NDB Scheme	Notifiable Data Breach Scheme
personal information	Any information or an opinion about an identified individual, or an individual who is reasonably identifiable. Personal information collected by ConnectAbility Australia may include: an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and/or employment details. Personal information that has been de-identified will no longer be considered personal information.
reasonable steps	The responsibility of ConnectAbility Australia is to be able to justify that reasonable steps were taken.
sensitive information	Part of personal information about an individual. Sensitive information collected by ConnectAbility Australia may include: racial or ethnic origin, religious beliefs, health information or criminal record. Sensitive information is generally afforded a higher level of privacy protection than other personal information. Inappropriate handling of sensitive information can have adverse consequences for an individual; it may cause humiliation, embarrassment or undermine an individual's dignity.

Policy

Personal information – ConnectAbility Australia is committed to protecting the privacy and confidentiality of personal information which the organisation collects, holds and administers about various stakeholders including, but not limited to, employees (both paid and unpaid) and customers. Personal information will not be disclosed to any unauthorised third party without the consent of the individual.

All personal information, including sensitive information, collected by ConnectAbility Australia, is collected in accordance with the Privacy Act 1988 and the Australian Privacy Principles (Privacy Amendment (Enhancing Privacy Protection) Act 2012) and the Privacy Amendment (Notifiable Data Breaches) Act 2017 . This policy also ensures compliance with the National Disability Service Standards, NDIS Quality and Safeguards Practice Standards and Article 22 of the United Nations Convention of the Rights of Persons with Disabilities.

Corporate information – ConnectAbility Australia is committed to protecting the confidentiality of commercially sensitive information regarding its business activities.

Confidential information must never be used for personal gain.

ConnectAbility Australia takes reasonable steps to protect any personal or corporate information received from customers, families, employees, volunteers or other service providers. These steps apply to the way the organisation collects, stores, uses or discloses these types of information. The type of information we collect, and the way we use this will depend on the individual's relationship with ConnectAbility Australia (e.g. as a customer, family member/carer, employee, volunteer or other service provider).

All ConnectAbility Australia people must comply with the standards detailed in this policy and must not release personal or confidential information without proper authorisation.

In brief, the Privacy policy explains:

- the kinds of personal information collected by the organisation
- how the organisation keeps personal information secure
- the ways the organisation collects personal information
- the purposes for which personal information is collected, held, used and disclosed
- how individuals can access, update or correct their personal information
- how an individual can make a complaint if they feel ConnectAbility Australia has breached the Australian Privacy Principles.

A breach of this policy by an employee may result in disciplinary action up to and including termination of employment, or for non-employees, other appropriate sanctions, including legal action.

Procedure

Application of Australian Privacy Principles within ConnectAbility Australia.

Part 1 — consideration of personal information privacy (APPs 1 and 2)

Open and transparent management of information

1. ConnectAbility Australia has a clearly expressed and up-to-date Privacy Policy detailing how we manage personal information.
    a. our policy statement is available on the ConnectAbility Australia website
    b. a copy of the Privacy Policy can be downloaded directly from the website, alternatively a hard copy can be sent, free of charge, on request.
2. ConnectAbility Australia has procedures for dealing with privacy related inquiries and complaints.

a. ConnectAbility Australia has practices, procedures and systems to ensure the organisation complies with the APPs and any binding registered APP code.

Anonymity and pseudonymity

3. Where it is not unlawful or impracticable, individuals have the option of remaining anonymous or using a pseudonym when dealing with ConnectAbility Australia.
    a. ConnectAbility Australia is not required to provide those options where:
        i. the organisation is required or authorised by law or a court or tribunal order to deal with identified individuals, or
        ii. it is impracticable for the organisation to deal with individuals who have not identified themselves.

Part 2 — Collection of personal information (APPs 3, 4 and 5)

Collection

4. ConnectAbility Australia may only collect personal information that is reasonably necessary for, or directly related to, one or more of ConnectAbility Australia functions or activities.
5. ConnectAbility Australia must solicit and collect personal information:
    a. by lawful and fair means
    b. directly from the individual, unless:
        i. the individual consents to the collection of the information from someone other than the individual; or
        ii. ConnectAbility Australia is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or
        iii. it is unreasonable or impracticable to do so.
6. ConnectAbility Australia may only collect sensitive information where:
    a. the individual has consented to the collection of that information and the information is reasonably necessary for ConnectAbility Australia' to carry out one or more of its' functions or activities, or
    b. the collection of information is required or authorised by or under Australian law or a court/tribunal order,
    c. ConnectAbility Australia reasonably believes the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

Unsolicited information

7. Where it receives unsolicited personal information, ConnectAbility Australia must decide within a reasonable period of time whether that personal information about an individual could have been lawfully collected by ConnectAbility Australia itself, and:
    a. If so, the information will be dealt with in accordance with the treatment of solicited information documented in this Privacy Policy, or,
    b. If not, and the information is not contained within a Commonwealth record, ConnectAbility Australia will, as soon as practicable, but only if lawful and reasonable to do so, destroy the information or ensure the information is de-identified.

Notification of collection

8. At or before the time ConnectAbility Australia collects personal information from an individual, or as soon as practicable after that, the organisation will take reasonable steps to ensure the individual is aware:
    a. ConnectAbility Australia is the collector of the personal information
    b. of contact details, telephone number and email address, for the person responsible for handling enquiries and requests relating to the Privacy Act
    c. how, when and from where the personal information was collected
    d. whether the collection is required or authorised by law
    e. the purposes for which the information has been collected
    f. the consequences if all or part of the personal information is not collected by ConnectAbility Australia
    g. the organisations (or the types of organisations) to which ConnectAbility Australia usually discloses personal information of the kind being collected
    h. they can access their personal information and seek correction of this, if required
    i. whether the personal information will be transferred overseas, and if practicable or known, to which countries
9. If an individual is concerned about how ConnectAbility Australia handles their personal information or that they have breached the APP they can make a complaint:
    a. directly to ConnectAbility Australia through the ConnectAbility Australia website or our internal complaints mechanism
        i. the organisation manages all complaints in line with our complaints procedure, a copy of which is available on request
        ii. the CEO or their delegate is responsible for handling enquiries, requests, complaints relating to the Privacy Act
    b. to the Office of the Australian Information Commissioner (OAIC). Further information is available on their website: http://www.oaic.gov.au/privacy/privacy-complaints

Part 3 - Dealing with personal information (APPs 6, 7, 8 and 9)

Use and disclosure

10. ConnectAbility Australia can only use or disclose personal information for a purpose for which it was collected (the 'primary purpose').
11. Where the information is sensitive information, ConnectAbility Australia may only use that information for a primary purpose or a directly related purpose the individual has consented to.
12. ConnectAbility Australia may sometimes use or disclose personal information about an individual for a 'secondary purpose'. However, ConnectAbility Australia will only use or disclose personal information about an individual for a secondary purpose in limited circumstances. ConnectAbility Australia will, wherever reasonably possible, seek consent from individuals before using their personal information for a secondary purpose.
13. ConnectAbility Australia may use personal information about an individual for a secondary purpose if
    a. the individual has consented to a secondary use or disclosure
    b. the individual would reasonably expect ConnectAbility Australia to use or disclose the information for the secondary purpose, and that secondary purpose is:

i. if the information is personal information, it is related to the primary purpose of collection, or,
ii. in the case of sensitive information, it is directly related to the primary purpose
iii. the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order

14. Some special situations set out in the Law allow the use or disclosure of personal information without consent. In each case, if it does this, ConnectAbility Australia will comply with the relevant Australian Privacy Principle or Rules made by the Privacy Commissioner. Some of these special situations are:
    a. where ConnectAbility Australia reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety;
    b. ConnectAbility Australia has reason to suspect an individual may have done something unlawful or engaged in serious misconduct that relates to ConnectAbility Australia functions or activities, and ConnectAbility Australia needs to disclose the information so that it can take appropriate action; or
    c. ConnectAbility Australia reasonably believes that the use or disclosure is reasonably necessary to assist another person to locate a person reported as missing, or
    d. ConnectAbility Australia reasonably believes that the use or disclosure of the information is reasonably necessary for an enforcement body's enforcement related activities
        i. ConnectAbility Australia will make a written note that ConnectAbility Australia has used the information for that purpose.
    e. A complete list of these special situations is contained in law.
15. Whether or not an individual has consented to the use or disclosure, in the case of any obligation ConnectAbility Australia has under a Commonwealth contract, ConnectAbility Australia is entitled to comply with a requirement under that Commonwealth contract to disclose personal or sensitive information to the Commonwealth agency funding the activity.

Direct marketing

16. ConnectAbility Australia may only use personal information about an individual for direct marketing where an exception applies under the Law. In every situation where ConnectAbility Australia is permitted to use or disclose personal information for direct marketing, ConnectAbility Australia will allow the individual to 'opt out' and will act on the individual's request to 'opt out'.
17. ConnectAbility Australia may use personal information (other than sensitive information) about an individual for direct marketing if:
    a. ConnectAbility Australia collected the information from the individual:
        i. and the individual would reasonably expect ConnectAbility Australia to use or disclose the information for direct marketing; and
        ii. ConnectAbility Australia has provided a simple means so the individual can easily request not to receive direct marketing communications from ConnectAbility Australia; and
        iii. the individual has not made a prior request to ConnectAbility Australia to not receive direct marketing communications from ConnectAbility Australia.
    b. ConnectAbility Australia collected the information from someone other than the individual and:

i. either the individual has consented to the use or disclosure for the purpose, or it is impracticable to obtain the individual's consent; and
ii. in each direct marketing communication with the individual, ConnectAbility Australia includes a prominent statement that the individual can ask not to receive further direct marketing communications from ConnectAbility Australia; or
iii. ConnectAbility Australia otherwise draws the individual's attention in some other way to the fact that the individual may make that request; and
iv. the individual has not made a request asking ConnectAbility Australia to stop sending direct marketing communications.

18. If ConnectAbility Australia uses or discloses personal information about an individual for:
    a. direct marketing, an individual may ask ConnectAbility Australia to stop sending direct marketing communications from ConnectAbility Australia and ConnectAbility Australia must do that within 14 days after receiving the request unless exceptional circumstances apply; or
    b. where the personal information is used for the purpose of facilitating direct marketing by other organisations on behalf of ConnectAbility Australia, an individual may request ConnectAbility Australia not to use or disclose the individual's information for direct marketing by other organisations and ConnectAbility Australia must act on that request within 14 days after receiving the request (unless exceptional circumstances apply).
19. The individual may request ConnectAbility Australia to provide details of where his or her personal information came from (e.g. which other organisation) and ConnectAbility Australia must do so within 14 days after receiving the request (except in exceptional circumstances) unless it is impractical or unreasonable to do so.
20. ConnectAbility Australia will not charge any individual for the making of, or to give effect to, these requests.

Cross border disclosure

21. ConnectAbility Australia will only send information overseas if it has taken reasonable steps to ensure the transferred information, will be held, used or disclosed by the recipient organisation consistent with the APP. Further details on these steps can be found in the law.

Adoption use or disclosure of government identifiers

22. ConnectAbility Australia will not adopt a government related identifier of an individual as its own identifier of the individual unless the adoption of the government related identifier is required or authorised by law or a court/tribunal order.
23. ConnectAbility Australia will not use or disclose a government related identifier of an individual unless:
    a. the use or disclosure of the identifier is reasonably necessary for ConnectAbility Australia to verify the identity of the individual for the purposes of the ConnectAbility Australia' activities or functions; or
    b. the use or disclosure of the identifier is reasonably necessary for ConnectAbility Australia to fulfil its obligations to an agency or a state or territory authority; or
    c. the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

d. some of the 'special situations' under the law allow the use or disclosure. In each case, if it does this, ConnectAbility Australia will comply with the relevant APP or Rules made by the Privacy Commissioner. Some of these 'special situations' are:
    i. where ConnectAbility Australia reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety;
    ii. ConnectAbility Australia has reason to suspect an individual may done something unlawful or engaged in serious misconduct that relates to ConnectAbility Australia functions or activities, and ConnectAbility Australia needs to disclose the information so that it can take appropriate action; or
    iii. ConnectAbility Australia reasonably believes that the use or disclosure is reasonably necessary to assist another person to locate a person reported as missing; or
    iv. ConnectAbility Australia reasonably believes that the use or disclosure of the information is reasonably necessary for an enforcement body's enforcement related activities (and ConnectAbility Australia will make a written note that ConnectAbility Australia has used the information for that purpose).

24. The complete list of these special situations is contained in the law.

Part 4 — Integrity of personal information (APPs 10 and 11)

Quality of personal information

25. ConnectAbility Australia will take all reasonable steps to ensure that the personal information it collects is accurate, complete and up-to-date and relevant, having regard to the purposes of the use or disclosure of the personal information that is collected.

Security of personal information

26. ConnectAbility Australia will take all reasonable steps to protect the personal information it holds from misuse, interference (which may include measures to protect against computer attacks), loss and unauthorised access, modification or disclosure.
27. ConnectAbility Australia data handling practices are regularly reviewed. All sensitive information is separately stored and shared among employees on a need to know basis only.
28. Customer management records (that include personal, sensitive and health information) are stored on a central database.
    a. each customer's records are assigned to a particular team depending on their service/program
    b. customer information can only be accessed by staff working on that team (team based security)
    c. within each team, staff have different levels of access to customer information, this is determined by their role within the team
29. Education and guidance to ConnectAbility Australia personnel has been established to support this Privacy Policy.
30. ConnectAbility Australia will take all reasonable steps to destroy or permanently de-identify personal information about an individual that it holds, if the information is no longer needed for any purpose for which it is able to be used or disclosed, and where there is no law or Court/tribunal or Commonwealth contract that requires ConnectAbility Australia to keep the information.

31. Customer records on the on the database are not able to be deleted or removed. Where a customer leaves the program/service or is deceased their records are made inactive.

Part 5 - Access to, and correction of, personal information (APPs 12 and 13).

Access to personal information

32. If ConnectAbility Australia holds personal information about an individual, and the individual wants access to that information, ConnectAbility Australia will provide the individual with access to that information.
33. This principle lists ten grounds on which ConnectAbility Australia can refuse to give access to personal information. ConnectAbility Australia need not to rely on any such ground and provide access upon request, unless disclosure is prohibited. Before relying on any of these grounds ConnectAbility Australia should consider whether redacting some information would enable access to be provided (for example, redacting personal information about another person).
34. The ten grounds are:
    a. ConnectAbility Australia reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
    b. giving access would have an unreasonable impact upon the privacy of other individuals; or
    c. the request for access is frivolous or vexatious; or
    d. the information relates to existing or anticipated legal proceedings between ConnectAbility Australia and the individual, and the information would not be provided by the process of discovery in those proceedings; or
    e. providing access would reveal the intentions of ConnectAbility Australia in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
    f. providing access would be unlawful; or
    g. denying access is required or authorised by or under an Australian law or a court/tribunal order; or
    h. both of the following apply:
        i. ConnectAbility Australia has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates the ConnectAbility Australia functions or activities has been or is being or may be engaged in; and
        ii. giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
    i. providing access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
    j. giving access would reveal evaluative information generated within ConnectAbility Australia in connection with a commercially sensitive decision-making process.
35. ConnectAbility Australia will respond to an access request within a reasonable period after the request is made and will give access to the personal information in the manner requested by the individual, if it is reasonable and practicable to do so. ConnectAbility Australia may, in appropriate circumstances, charge the individual an appropriate (and not excessive) fee for giving access to the personal information.
36. If ConnectAbility Australia refuses to give access to personal information in the manner requested by the individual or because one or more of the exceptions referred to in this policy apply, ConnectAbility Australia will give the individual a written notice about the refusal that complies with

the regulations to the Law and includes information about how a person can complain about the refusal.

Correction of personal information

37. ConnectAbility Australia will take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. This requirement applies where:
    a. ConnectAbility Australia is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or
    b. the individual requests ConnectAbility Australia to correct the personal information.
38. APP 13 sets out the following minimum procedural requirements in relation to correcting personal information:
    a. take reasonable steps to notify other APP entities of a correction to an individual's personal information
    a. respond to a request for correction or to associate a statement, and
    b. not charge an individual for making a request, correcting personal information or associating a statement.
39. If ConnectAbility Australia refuses to correct the personal information when requested to do so by an individual:
    a. ConnectAbility Australia will give the individual a written notice about the refusal that complies with the regulations to the Law and includes information about how a person can complain about the refusal.
    b. An individual can request ConnectAbility Australia to attach a statement to information saying that the information is inaccurate, out of date, incomplete, irrelevant or misleading. ConnectAbility Australia will answer that request within a reasonable period after it is made and will take reasonable steps as are to ensure the statement is able to be seen by the users of the information.
40. Special considerations apply to Commonwealth records, which can only be destroyed or altered in accordance with the *Archives Act 1983* (Archives Act).

Part 6 – Confidentiality of corporate information

41. While Parts 1-5 above have been written with a focus on the privacy of personal information, the intent of each of these points applies to the confidentiality of corporate information.
42. Confidential information includes, but is not limited to, the following stored in any form or manner (except where is or has been made generally known by the organisation to the public or is otherwise already in the public domain):
    a. Any information about, and any documents relating to, our commercial customers and/or the people we support.
    b. Any information about and any documents relating to our employees.
    c. All confidential deliberations of the ConnectAbility Australia Board and Committees of the Board.
    d. Information in any personnel or employment manuals, policy documents and/or quality assurance manuals (or similar documents) developed from time to time by the organisation.
    e. The investigation of any matter and the materials contained in any investigation reports.

f. Any of ConnectAbility Australia trade secrets and business processes.
g. Any information and documents relating to our strategy, business plans, budgets and/or financial position.
h. Any information about our suppliers and/or or price lists of such suppliers.
i. Any information from any supplier listing services, goods or products used by the organisation.
j. Any information about the method of presentation or supply of services.
k. Any information, research programs, concepts or results connected with any proposed or new services that may be supplied by ConnectAbility Australia before the general introduction or availability to the public of that service.
l. Any information in connection with any advertising and promotional activities proposed to be undertaken by or for the organisation prior to the general introduction of that advertising or promotional material to the public or prior to such advertising and promotional activity first being undertaken.
m. Any information maintained in any database maintained by the organisation in connection with its business.
n. Any information, know how or expertise relating to the business of the organisation, including knowledge, whether or not it is the product of any research concerning investment opportunities.
o. Any information about any plans or proposals to improve or develop ConnectAbility Australia business.
p. Any information about the contents of any training programs or materials used in any training proposed or undertaken by us relating to training of ConnectAbility Australia People.
q. Any information about any new or proposed trademark, service mark, patent or copyrighted work that it is intended to introduce for use the business prior to the lodging of any relevant application.
r. Any information about any mergers/acquisitions for business development.

43. Confidential corporate information must be securely stored in a manner, which protects the confidentiality of the information.

Permission for customers or employee participation in research programs must be referred to the CEO for consideration and approval.

Notifiable Data Breach Scheme

44. **What is a data breach?**

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.

The scheme only applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'. Examples of data breaches include:

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

45. **Consequences of a data breach**

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, whether that is 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.

When an agency or organisation is aware of reasonable grounds to believe an eligible data breach has occurred, they must promptly notify individuals at likely risk of serious harm. The Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

46. **How to notify**

The notification to affected individuals and the Commissioner must include the following information:

- the identity and contact details of the organisation
- a description of the data breach
- the kinds of information concerned
- recommendations about the steps individuals should take in response to the data breach.

The notification to the Commissioner should be made through the **Notifiable Data Breach form.**

ConnectAbility will manage data breaches in accordance with the *Data breach notification — A guide to handling personal information security breaches* released in 2014, the *Guide to developing a data breach response plan* released in 2016, and the resources published to assist entities in complying with the Notifiable Data Breaches (NDB) scheme.

Data breach response summary diagram

The following diagram provides an overview of the data breach response, including the requirements of the NDB scheme.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — Is serious harm still likely? — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Version control

Version	Date	Author	Reason	Sections
6	May 2019	Donna Vallette	Changes made to incorporate data breaches	**All**
5	July 2016	Michelle Holcombe	Policy made more generic to cover all services	**All**
4 (draft 1)	August 2014	Scott Harvey	Reviewed in line with introduction of new DSS. In consultation with participants, families/carers and staff.	**All**
3	September 2008	Scott Harvey	Reviewed in line with Standards. Approved by CoM	**All**
2	March 2006	Shelley Williams	Reviewed in line with Standards. Approved by CoM	**All**
1 (draft 1)	August 2001	Christina Morris	Policy created to reflect DSS	**All**