Privacy and Confidentiality

Purpose

This document defines ConnectAbility policy and procedure for handling personal and confidential information to ensure this information is protected from unauthorised disclosure. ConnectAbility will adhere to the guidelines of the *Australian Privacy Principles* in its information management practices.

Policy Statement

ConnectAbility is committed to ensuring the capture, storage, disposal and use of information is effectively managed in accordance with legislative requirements. ConnectAbility will uphold the rights of our service users to privacy and confidentiality in relation to:

- Gaining informed consent from its service users in the use of management of their information held by ConnectAbility;
- Providing information regarding consent and service user information management to service users in a meaningful and understandable format;
- Handling and transferring information, whether written or verbal, within ConnectAbility;
- Communication of service user information to other agencies/individuals;
- Storage of information and service user files;
- Obtaining informed consent from service users; and
- Informing service users of the limitations of confidentiality and consent.

ConnectAbility is also committed to operating in a transparent manner and to freedom of information, and to the rights of service users to access information held about them in a proficient and professional manner.

Scope

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

Contents

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 business.
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.
notifiable data breach	Under the Notifiable Data Breaches (NDB) scheme any organisation the *Privacy Act 1988* covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.
personal information	• Any information or an opinion about an identified individual, or an individual who is reasonably identifiable. Personal information collected by ConnectAbility 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.
sensitive information	Sensitive information includes health information and information about religious beliefs, race, gender and others.
service user (i.e. Customers)	Any individual who engages with ConnectAbility services. Includes all prospective, current, and past (until the legislated requirements for record keeping are passed) Customers of ConnectAbility.
Office of the Australian Information Commissioner (OAIC)	The independent national regulator for privacy and freedom of information.

Responsibilities

Position	Responsibilities
The Board of Directors and CEO	The Board is responsible for oversight of this policy, and via the CEO: • Ensure adequate governance arrangements, authority and resources are provided to ensure the safe delivery of supports and services.
Leaders	Ensuring workers: • are trained in the appropriate management of personal and confidential information, and • adhere to the requirements of this policy.
ConnectAbility Employees and volunteers	All employees are responsible for management of personal information and ensuring that confidentiality is maintained for all information that they have access to.

Process and Requirements

1 Privacy and confidentiality policy

All personal information, including sensitive information, collected by ConnectAbility, is collected in accordance with the *Privacy Act 1988* and the *Australian Privacy Principles (Privacy Amendment (Enhancing Privacy Protection) Act 2012)*, the *Privacy Amendment (Notifiable Data Breaches) Act 2017,* and *Health Records and Information Privacy Act 2002*. This policy also ensures compliance with the *NDIS Practice Standards* and Article 22 of the United Nations Convention of the Rights of Persons with Disabilities.

Personal information – ConnectAbility 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.

Corporate information – ConnectAbility is committed to protecting the confidentiality of commercially sensitive information regarding its business activities (see section Confidentiality of corporate information). Confidential information must never be used for personal gain.

ConnectAbility 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.

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

1.1 Dealing with personal information

In dealing with personal information, ConnectAbility employees will:

- ensure privacy for service users, employees, or volunteers when they are being interviewed or discussing matters of a personal or sensitive nature;
- only collect and store personal information that is necessary for the functioning of the organisation and its activities;
- use fair and lawful ways to collect personal information;
- collect personal information only by consent from an individual;
- ensure that people know what sort of personal information is held, what purposes it is held it for and how it is collected, used, disclosed and who will have access to it;
- ensure that personal information collected or disclosed is accurate, complete and up-to-date, and provide access to any individual to review information or correct wrong information about themselves;
- take reasonable steps to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure;
- destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired; and
- notify individuals and the Office of the Australian Information Commissioner (OAIC) when there has been a data breach (or suspected breach) of personal information, if it is likely to result in serious harm to individuals whose privacy has been breached.

1.2 Confidentiality

ConnectAbility employees will:

- retain all confidential information in the strictest confidence and not disclose any confidential information to any person other than for purposes directly related to their position at ConnectAbility.
- not use any confidential information which they have acquired in relation to the activities of ConnectAbility for their own interests or the interests or purposes of others not associated with ConnectAbility.
- not make copies of any confidential information for any other reason other than those essential to and directly related to their position and responsibilities with ConnectAbility.
- upon the request, and in any event upon the cessation of their engagement or employment with ConnectAbility return or destroy materials containing confidential information which are in their possession.

This will not prevent an individual from:

- disclosing information to proper authorities in relation to concerns about improper conduct, breaches of laws or breaches of duty of care.
- providing access for external reviewers to non-identified information for the purposes of formal audit processes.

- making a formal complaint to appropriate authorities about an aspect of the organisation's operation (see *Whistleblowing Policy*).
- disclosing any information that they may be required to disclose by any court or regulatory body or under applicable law.

2 Application of the Australian Privacy Principles

2.1 Consideration of personal information privacy

Open and transparent management of personal information (APP 1)

- ConnectAbility has a clearly expressed and up-to-date Privacy Policy detailing how we manage personal information.
- Our policy is freely available on the ConnectAbility website, alternatively a hard copy can be sent free of charge by request.
- ConnectAbility has procedures for handling privacy-related inquiries and complaints.

Anonymity and pseudonymity (APP 2)

- ConnectAbility will allow people from whom the personal information is being collected to not identify themselves or use a pseudonym.
- ConnectAbility is not required to provide those options where:
    - the organisation is organisation is required or authorised by law or a court or tribunal order to deal with identified individuals, or
    - it is impracticable for the organisation to deal with individuals who have not identified themselves.

2.2 Collection of personal information

Collection of solicited information (APP 3)

- ConnectAbility will:
    - only collect information that is reasonably necessary or directly related to one or more primary functions or activities of ConnectAbility.
    - collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
    - notify stakeholders about why we collect the information and how it is administered.
    - notify stakeholders that this information is accessible to them.
    - collect personal information from the person themselves wherever possible.
    - collect sensitive information only with the person's consent or if required by law.
- ConnectAbility will also collect sensitive information about an individual if such collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
    - is physically or legally incapable of giving consent to the collection; or
    - physically cannot communicate consent to the collection; or
    - if at or before the time of collecting the information, inform the individual whom the information concerns that ConnectAbility will not disclose the information without the individual's consent.
- ConnectAbility will collect health information about an individual if:
    - the information is necessary to provide a health service to the individual; and

- the information is collected as required or authorised by or under law and in accordance with rules established by competent health or medical bodies that have obligations of professional confidentiality.

Unsolicited information (APP 4)

- Where unsolicited personal information is received, ConnectAbility must decide within a reasonable period of time whether that personal information about an individual could have been lawfully collected by ConnectAbility itself, and:
  - If so, the information will be dealt with in accordance with the treatment of solicited information documented in this *Privacy Policy*, or,
  - If not, and the information is not contained within a Commonwealth record, ConnectAbility 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 (APP 5)

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

2.3 Dealing with personal information

Use and Disclosure (APP 6)

- ConnectAbility will only use or disclose information for the primary purpose for which it was collected or a directly related secondary purpose. For other uses, ConnectAbility will obtain consent from the affected person.
- ConnectAbility may use personal information about an individual for a secondary purpose if:
    - the individual has consented to a secondary use or disclosure
    - the individual would reasonably expect ConnectAbility to use or disclose the information for the secondary purpose, and that secondary purpose is:
        - if the information is personal information, it is related to the primary purpose of collection, or,
        - in the case of sensitive information, it is directly related to the primary purpose, or
        - or disclosure is required to prevent serious and imminent threat to life, health or safety, or
        - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order.
- 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 will comply with the relevant Australian Privacy Principle or Rules made by the Privacy Commissioner. Some of these special situations are:
    - where ConnectAbility 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;
    - ConnectAbility has reason to suspect an individual may have done something unlawful or engaged in serious misconduct that relates to ConnectAbility functions or activities, and ConnectAbility needs to disclose the information so that it can take appropriate action; or
    - ConnectAbility reasonably believes that the use or disclosure is reasonably necessary to assist another person to locate a person reported as missing, or
    - ConnectAbility reasonably believes that the use or disclosure of the information is reasonably necessary for an enforcement body's enforcement related activities
        - ConnectAbility will make a written note that ConnectAbility has used the information for that purpose.
    - A complete list of these 'special situations' is defined in subsections 16A and 16B of the Privacy Act.
- Whether or not an individual has consented to the use or disclosure, in the case of any obligation ConnectAbility has under a Commonwealth contract, ConnectAbility 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 (APP 7)

- In relation to personal information which has been collected from a person, ConnectAbility may use or disclose the personal information (other than sensitive information) for direct marketing if:
    - ConnectAbility collected the information from the individual and:
        - the individual would reasonably expect ConnectAbility to use or disclose the information for direct marketing; and
        - ConnectAbility has provided a simple means so the individual can easily request not to receive direct marketing communications from ConnectAbility (an 'opt out'); and

        - the individual has not made a prior request to ConnectAbility to not receive direct marketing communications from ConnectAbility.
    - ConnectAbility collected the information from someone other than the individual and:
        - either the individual has consented to the use or disclosure for the purpose, or it is impracticable to obtain the individual's consent; and
        - in each direct marketing communication with the individual, ConnectAbility includes a prominent statement that the individual can ask not to receive further direct marketing communications from ConnectAbility; or
        - ConnectAbility otherwise draws the individual's attention in some other way to the fact that the individual may make that request; and
        - the individual has not made a request asking ConnectAbility to stop sending direct marketing communications.
- ConnectAbility may use or disclose sensitive information about an individual for the purpose of direct marketing only if the individual has consented to the use or disclosure of the information for that purpose.
- If ConnectAbility uses or discloses personal information about an individual for:
    - direct marketing, an individual may ask ConnectAbility to stop sending direct marketing communications from ConnectAbility and ConnectAbility must give effect to the request within a reasonable period after receiving the request unless exceptional circumstances apply; or
    - where the personal information is used for the purpose of facilitating direct marketing by other organisations on behalf of ConnectAbility, an individual may request ConnectAbility not to use or disclose the individual's information for direct marketing by other organisations and ConnectAbility must act on that request within a reasonable period after receiving the request (unless exceptional circumstances apply).
- The individual may request ConnectAbility to provide details of where his or her personal information came from (e.g. which other organisation) and ConnectAbility must do so within a reasonable period after receiving the request (except in exceptional circumstances) unless it is impractical or unreasonable to do so.
- ConnectAbility will not charge any individual for the making of, or to giving effect to, these requests.

Cross border disclosure (APP 8)

- ConnectAbility 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. This is detailed in Australian Privacy Principle 8.

Adoption, use or disclosure of government related identifiers (APP 9)

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

- some of the 'special situations' under the law allow the use or disclosure. A complete list of these 'special situations' is defined in subsections 16A and 16B of the Privacy Act. In each case, if it does this, ConnectAbility will comply with the relevant APP or Rules made by the Privacy Commissioner.
- ConnectAbility reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (and ConnectAbility will make a written note that ConnectAbility has used the information for that purpose).

2.4 Integrity of personal information

Quality of personal information (APP 10)

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

Security of personal information (APP 11)

- ConnectAbility 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.
- ConnectAbility data handling practices are regularly reviewed. All sensitive information is separately stored and shared among employees on a need to know basis only.
- Service user records (that include personal, sensitive and health information) are stored on a central database:
  - each service user's records are assigned to a particular team depending on their service/program
  - service user information can only be accessed by employee working on that team (team based security)
  - within each team, employee have different levels of access to service user information, this is determined by their role within the team.
- Access and guidance to ConnectAbility personnel has been established to support this Privacy Policy and Procedure.
- ConnectAbility 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 to keep the information.
  - Customer information held by ConnectAbility will be destroyed or archived in accordance with the *Customer Record Management Policy*.
- Customer records on the database are not able to be deleted or removed. Where a service user leaves the program/service or is deceased their records are archived or made inactive.

2.5 Access to, and correction of, personal information

Access to personal information (APP12)

- If ConnectAbility holds personal information about an individual, and the individual wants access to that information, ConnectAbility will provide the individual with access to that information.
- ConnectAbility will provide to the individual its reasons for denial of access or a refusal to correct personal information.

- ConnectAbility can withhold the access of an individual to the individual's information if:
  - providing access would pose a serious and imminent threat to the life or health of any individual; or
  - providing access would have an unreasonable impact upon the privacy of other individuals; or
  - the request for access is frivolous or vexatious; or
  - the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
  - providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
  - providing access would be unlawful; or
  - denying access is required or authorised by or under an Australian law or a court/tribunal order; or
  - providing access would be likely to prejudice an investigation of possible unlawful activity, or misconduct of serious nature that relates to ConnectAbility' functions or activities that have been, is being or may be engaged in.
- Where providing access would reveal evaluative information generated within ConnectAbility in connection with a commercially sensitive decision-making process, ConnectAbility may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.
- ConnectAbility 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 may, in appropriate circumstances, charge the individual an appropriate (and not excessive) fee for giving access to the personal information and will not apply to lodging a request for access.
- If ConnectAbility refuses to give access to personal information in the manner requested by the individual or if one or more of the abovementioned reasons apply, ConnectAbility 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. ConnectAbility will also consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

Correction of personal information (APP 13)

- ConnectAbility will ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, irrelevant, misleading, or not up-to-date.
- ConnectAbility 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:
  - ConnectAbility 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
  - the individual requests ConnectAbility to correct the personal information.
- APP 13 sets out the following minimum procedural requirements in relation to correcting personal information:
  - take reasonable steps to notify other APP entities of a correction to an individual's personal information;
  - respond to a request for correction or to associate a statement, and
  - not charge an individual for making a request, correcting personal information or associating a statement.

- If ConnectAbility refuses to correct the personal information when requested to do so by an individual:
    - ConnectAbility 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.
    - An individual can request ConnectAbility to attach a statement to information saying that the information is inaccurate, out of date, incomplete, irrelevant or misleading. ConnectAbility 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.
- Special considerations apply to Commonwealth records, which can only be destroyed or altered in accordance with the *Archives Act 1983* (Archives Act).

3 Confidentiality of corporate information

- This section applies to the confidentiality of corporate information.
- 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):
    - Any information about, and any documents relating to, our commercial customers and/or our customers.
    - Any information about and any documents relating to our employees.
    - All confidential deliberations of the ConnectAbility Board and Committees of the Board.
    - 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.
    - The investigation of any matter and the materials contained in any investigation reports.
    - Any of ConnectAbility' trade secrets and business processes.
    - Any information and documents relating to our strategy, business plans, budgets and/or financial position.
    - Any information about our suppliers and/or or price lists of such suppliers.
    - Any information from any supplier listing services, goods or products used by ConnectAbility.
    - Any information about the method of presentation or supply of services.
    - Any information, research programs, concepts or results connected with any proposed or new services that may be supplied by ConnectAbility before the general introduction or availability to the public of that service.
    - 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.
    - Any information maintained in any database maintained by the organisation in connection with its business.
    - Any information, 'know how' or expertise relating to the business of the organisation, including knowledge, and whether or not it is the product of any research concerning investment opportunities.
    - Any information about any plans or proposals to improve or develop ConnectAbility business.
    - 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 employees.
    - Any information about any new or proposed trademark, service mark, patent or copyrighted work that it intends to introduce for use the business prior to the lodging of any relevant application.

    - Any information about any mergers/acquisitions for business development.
- Confidential corporate information must be securely stored in a manner that protects the confidentiality of the information.
- Permission for Customer or employee participation in research programs must be referred to the CEO for consideration and approval.

4 Notifiable Data Breach Scheme

4.1 What is a data breach?

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

The Notifiable Data Breaches 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.

4.2 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 OAIC must also be notified as soon as practicable through a statement about the eligible data breach.

4.3 How to notify

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

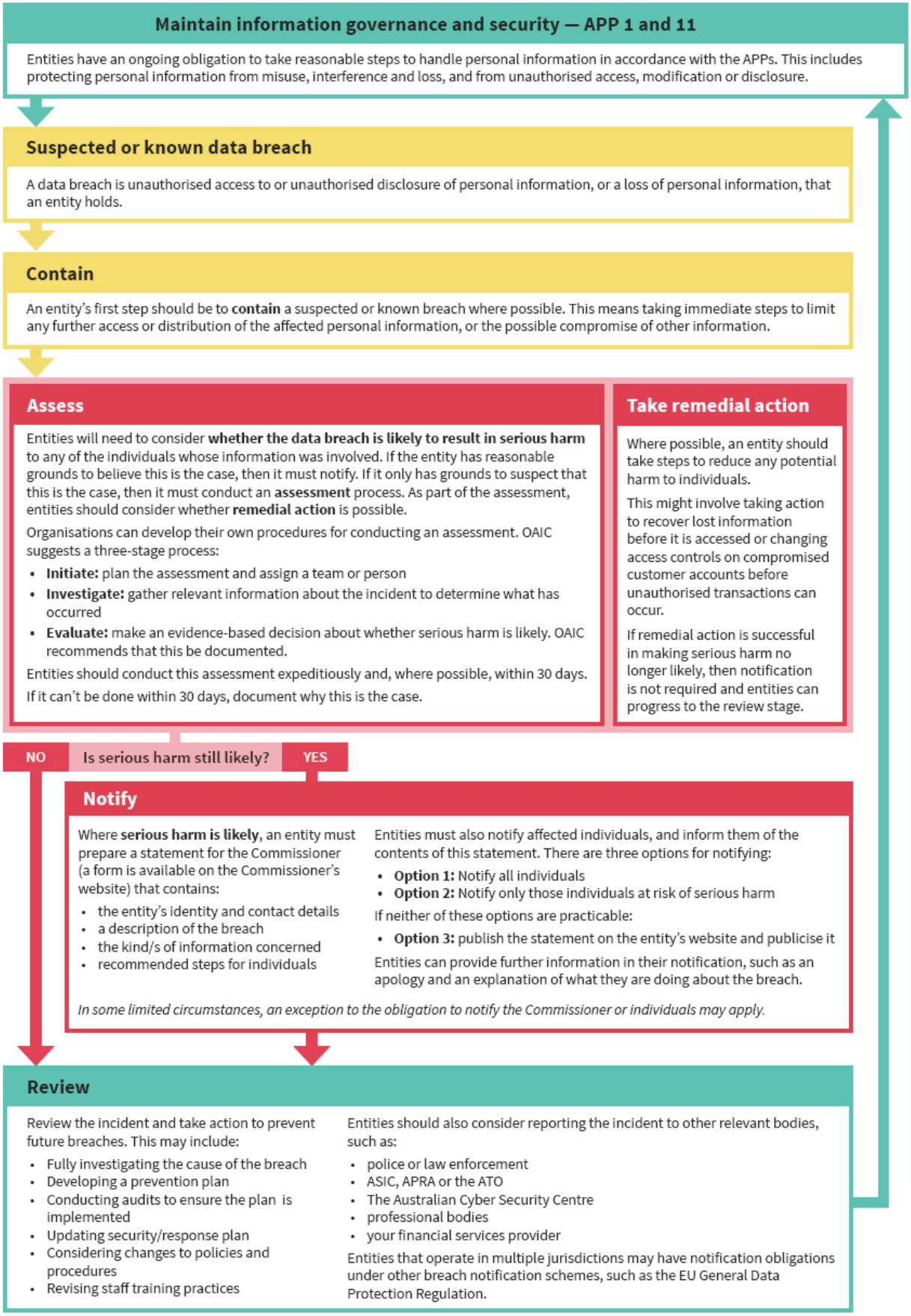
- the identity and contact details of the organisation.
- a description of the data breach.
- the kinds of information concerned.
- recommendations about the steps individuals should take in response to the data breach.

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.

4.4 Data breach response summary diagram

The following diagram provides an overview of the data breach response, including the requirements of the Notifiable Data Breach scheme (coloured red).



Training

ConnectAbility will:

- Ensure stakeholders are aware of ConnectAbility's *Privacy and Confidentiality Policy* and its purposes.
- Make this information freely available in relevant publications and on the organisation's website.

This policy will be:

- communicated to the key internal and external stakeholders of ConnectAbility;
- communicated to ConnectAbility employee through professional development opportunities;
- accessible through ConnectAbility's internal information systems.

Records management

- Service user records will be retained and destroyed in accordance with the *Customer Record Management Procedure*.
- On request by a person, ConnectAbility will take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

Resource and Reference Links

Type	Description
Legislation	*Archives Act 1983*
Legislation	*Australian Privacy Principles (Privacy Amendment (Enhancing Privacy Protection) Act 2012)*
Legislation	*Health Records and Information Privacy Act 2002 (NSW)*
Legislation	*NDIS Practice Standards and Quality Indicators 2021*
Legislation	*Privacy Act 1988 (Cth)*
Legislation	*Privacy and Personal Information Protection Act 1998 (NSW)*
Procedure	*Feedback and Complaints Policy CORPO-008*
Procedure	*Customer Record Management CORPO-025*
Procedure	*Whistleblower Policy CORPO-023*
Guide	*Emergency Management Plan: Data Breach*
Guide	*Privacy Policy (public version)*
System	CAZoom
System	NDS etrainu
External Resource	Notifiable Data Breach Form - Office of the Australian Information Commissioner (OAIC)

Version Control

Version	Date	Author	Reason/Changes	Sections
7	07/12/2023	Compliance & Quality	Revised content for legislative requirements	All
6	05/2019	Donna Vallette	Changes made to incorporate data breaches	All
5	07/2016	Michelle Holcombe	Policy made more generic to cover all services	All

4	08/2014	Scott Harvey	Reviewed in line with introduction of new DSS. In consultation with participants, families/carers and staff	All
3	09/2008	Scott Harvey	Reviewed in line with Standards. Approved by CoM	All
2	03/2006	Shelley Williams	Reviewed in line with Standards. Approved by CoM	All
1	08/2001	Christina Morris	Policy created to reflect DSS	All