Policy 15	PRIVACY AND CONFIDENTIALITY

Record of policy development		
Version	**Date approved**	**Date for review**
1.4	December 2020	December 2022
1.3	May 2019	May 2021
1.2	January 2018	January 2021

Policy purpose: COASTLINK respects each client's right to privacy, dignity and confidentiality including the collection, use and disclosure of personal information.

Policy:

COASTLINK is committed to protecting and upholding the right to privacy of clients, staff, volunteers, Board members and representatives of agencies we deal with. In particular COASTLINK is committed to protecting and upholding the rights of our clients to privacy in the way we collect, store and use information about them, their needs and the services we provide to them.

COASTLINK requires staff, volunteers and Board members to be consistent and careful in the way they manage what is written and said about individuals and how they decide who can see or hear this information.

COASTLINK will follow the guidelines of the *Australian Privacy Principles* in its information management practices as well as the NDIS (Protection and Disclosure of Information – Commissioner) Rules 2018

COASTLINK will ensure that:

- it meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of clients and organisational personnel
- clients are provided with information about their rights regarding privacy
- clients and organisational personnel are provided with privacy when they are being interviewed or discussing matters of a personal or sensitive nature
- all staff, Board members and volunteers understand what is required in meeting these obligations

This policy conforms to the *Federal Privacy Act (1988)* and *the Australian Privacy Principles* which govern the collection, use and storage of personal information in addition to the NDIS (Protection and Disclosure of Information – Commissioner) Rules 2018

(Note: The *Federal Privacy Act* applies to organisations with an annual turnover over $3m or organisations that are health service providers, operators of a residential tenancy database, a contractor that provides services under a Commonwealth contract, an organisation that is related to a larger

organisation or one which trades in personal information.

Many funding contracts may require that funded organisations comply with the Australian Privacy Principles).

This policy will apply to all records, whether hard copy or electronic, containing personal information about individuals, and to interviews or discussions of a sensitive personal nature.

Principles:

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth legislation) outlines thirteen Australian Privacy Principles.

Principle 1: open and transparent management of personal information
Principle 2: anonymity and pseudo-anonymity
Principle 3: collection of solicited personal information
Principle 4: dealing with unsolicited personal information
Principle 5: notification of the collection of personal information
Principle 6: use or disclosure of personal information
Principle 7: direct marketing
Principle 8: cross –border disclosure of personal information
Principle 9: adoption, use or disclosure of government related identifiers
Principle 10: quality of personal information
Principle 11: security of personal information
Principle 12: access to personal information
Principle 13: correction of personal information

Relevant Standards

NDIS Practice Standards:

1. Rights and Responsibilities
2. Provider Governance and Operational Management
3. Provision of Supports
4. Support Provision Environment
5. High Intensity Daily Personal Activities
6. Specialist Behaviour Support
7. Implementing Behaviour Support Plans
8. Early Childhood Supports
9. Specialised Support Coordination
10. Specialist Disability Accommodation

Aged Care Quality Standards

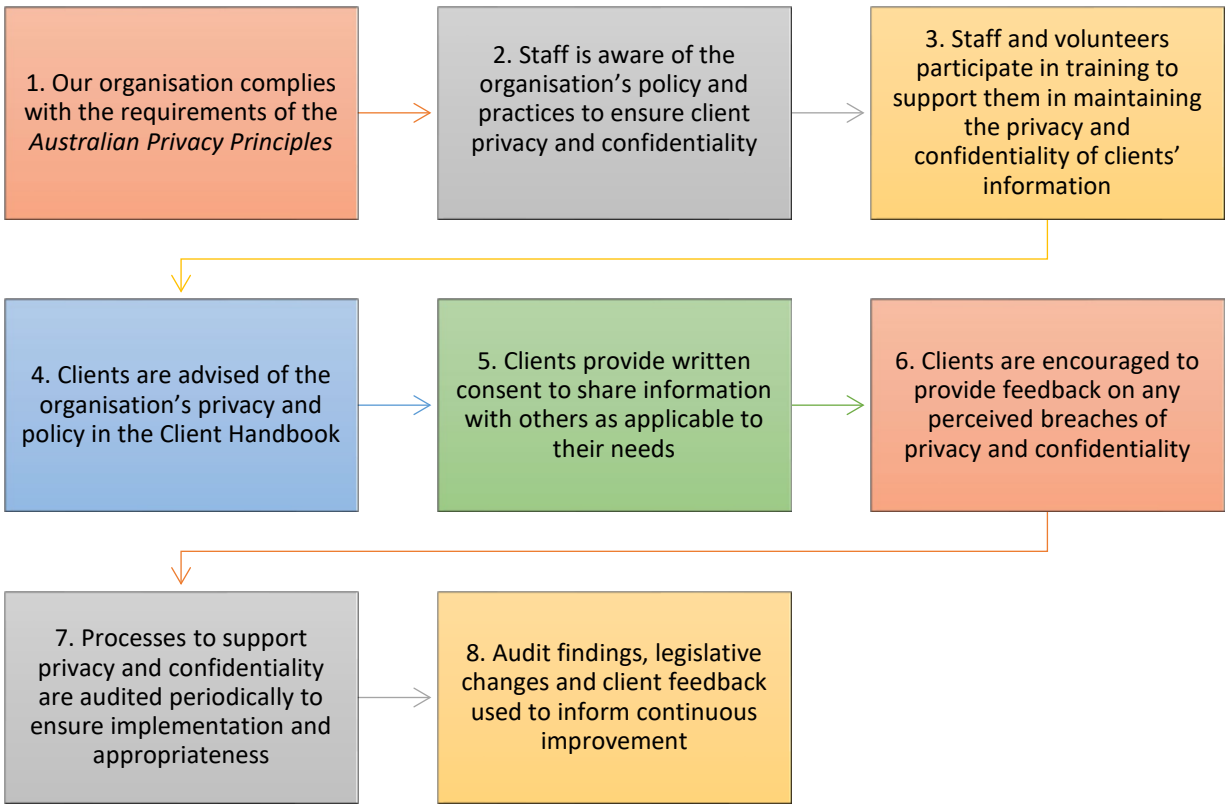
1. Consumer dignity and choice
2. Ongoing assessment and planning with consumers
3. Personal care and clinical care
4. Services and supports for daily living
5. Organisation's service environment
6. Feedback and complaints
7. Human resources
8. Organisational governance

Related Legislation & References
Aged Care Act 1997 (Cth), Schedule 2 User Rights Principles 2014. Charter of Rights and Responsibilities – Home Care Aged Care Quality & Safety Commission Archives Act 1983 Australian Privacy Principles Children and Young Persons (Care and Protection) Act 1998 Commonwealth Home Support Programme Guidelines Commonwealth Privacy Act 1988 *Crime Commission Act 2012* *Independent Commission Against Corruption Act 1988* *Mental Health Act 2007* *National Disability Insurance Scheme (Protection and Disclosure of Information - Commissioner) Rules 2018* National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018 National Disability Insurance Scheme Act 2013 National Disability Insurance Scheme Code of Conduct NDIS Quality and Safeguards Commission *Ombudsman Act 1974* Privacy Amendment (Enhancing Privacy Protection) Act 2012 *Privacy and Personal Information Protection Act 1998* Privacy and Personal Information Protection Act 1998 *Public Interests Disclosure Act 1994* *State Records Act 1998* United Nations Convention on the Rights of Persons with Disabilities *Work Health and Safety Act 2011* *Workers Compensation Regulation 2010* *Workplace Injury Management and Workers Compensation Act 1998*

Related Procedures	
Policy 3 – Information Management Policy 7 – Human Resource Management Policy 10 – Assessment Policy 11 – Support Planning and Delivery Policy 15 – Complaint and Feedback	
Documents/Forms	
Client Handbook	Shared Drive
Client Consent Form	Client records

Responsibilities and delegations	
This policy applies to: Clients Employees/volunteers	**It will be distributed through:** Client handbook, Coastlink website, Coastlink brochures Employee/volunteer handbook, shared drive
Policy approval	Board

15.1 PRIVACY AND CONFIDENTIALITY PROCEDURE OVERVIEW



15.1.1 PRIVACY AND CONFIDENTIALITY PROCEDURES
Introduction COASTLINK will conform to both State and Commonwealth privacy legislation requirements regarding the collection, use and protection of personal information of our Clients and Team Members. COASTLINK staff and volunteers must respect the right to privacy and confidentiality of all clients in the collection and management of their information.
Learning and development Management, staff and volunteers are provided with training and information on the rights of clients to privacy and confidentiality and the processes to support this. All staff, volunteers and contractors will sign a Confidentiality Agreement thereby demonstrating their commitment to maintaining confidentiality in the Organisation.

15.1.2 Principles for the Collection of Client Information

The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Commonwealth legislation) outlines thirteen Australian Privacy Principles which COASTLINK conforms to.

Principle 1: open and transparent management of personal information

Manage personal information in an open and transparent way.

Principle 2: anonymity and pseudo-anonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym.

Principle 3: collection of solicited personal information

The entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

Principle 4: dealing with unsolicited personal information

The entity receives personal information and the entity did not solicit the information, the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 and as soon as practicable but only if lawful to do so, destroy the information or ensure that the information is de-identified.

Principle 5: notification of the collection of personal information

Take steps to notify the individual of information collected, the circumstances of that collection and the purposes of that collection of information. Notify how to access personal information held by the entity and how to correct that information. Notify how to complain about a breach of the Australian Privacy Principles and how the entity will deal with such a complaint. Notify if the entity is likely to disclose information to overseas recipients.

Principle 6: use or disclosure of personal information

Information about an individual collected by an entity for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: the individual has consented to the use or disclosure.

Principle 7: direct marketing

If any entity holds personal information about an individual, the entity must not use or disclose the information for the purpose of direct marketing.

Principle 8: cross –border disclosure of personal information

Before disclosing information about an individual to a person (the overseas recipient): the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Principle 9: adoption, use or disclosure of government related identifiers

An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless: it is required or authorised by or under Australian law.

Principle 10: quality of personal information

An entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

Principle 11: security of personal information

If an entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss and from unauthorised access, modification or disclosure.

Principle 12: access to personal information

If an entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Principle 13: correction of personal information

If the information the entity holds is inaccurate, out-of-date, incomplete, irrelevant or misleading or the individual requests the entity to correct the information then the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

15.2 PRIVACY AND CONFIDENTIALITY MANAGEMENT PROCESS

15.2.1 Principle 1: Open and transparent management of personal information

- We only collect information about clients that is relevant to the provision of support and we explain to clients why we collect the information and the purpose for which it is used.
- Client consent to collect information is provided when signing a Service Agreement with COASTLINK.
- We seek written consent from clients to disclose personal information to other health or community care service providers as appropriate to provide emergency care or services, when signing Service Agreements.
- We seek consent from clients when signing Service Agreements to provide access to client records to government officials (or their delegates) in the conduct of quality reviews or the investigation of complaints. We advise clients that these individuals are required to keep all information accessed through this process confidential.
- Information collected in relation to a client is subject to internal audits for quality and safeguarding, and to ensure that only that information relevant to the delivery of quality services is retained by the organisation.

15.2.2 Principle 2: Anonymity and pseudo-anonymity

- Information provided to government bodies regarding service provision does not identify the client or carer, unless required.
- If any information is provided to outside government agencies for data purposes, we ensure that the information is de-identified.
- Any references to individual clients in meeting minutes refer to the client by initials only or another unique identifier, such as their client number.
- Information provided in reports, case studies, or other documents that may be accessible by a third party, are not to contain information that may identify the client unless the client has consented to this.
- COASTLINK does not use unique identifiers issued by another agency or government department as the client number

15.2.3 Principle 3: Collection of solicited personal information

- When completing an intake form, client profile, or other COASTLINK form, staff are to ensure that they are only recording that information which is required for service delivery, or the safety of clients and/or staff.
- Staff should not ask clients for information that does not relate to their role in the delivery of services to the client.

15.2.4 Principle 4: Dealing with unsolicited personal information

- Information recorded by COASTLINK in relation to a client should be provided by the client, or a person nominated by them, wherever possible.
- Information received from a third party, including other agencies, that is not relevant to the health, safety and wellbeing of the client, others clients or staff, and/or the delivery of services by COASTLINK, should not be retained by the organisation.

- As soon as practicable, and only if it does not contravene State or Federal laws or legislation, information that is unsolicited and not required should be destroyed or de-identified.

15.2.5 Principle 5: Notification of the collection of personal information

- Clients are to be informed of what information has been recorded by COASTLINK and how this information will be used. This is to be completed at the time of signing a Service Agreement.
- Clients are to be informed of how information about them can be accessed by them.
- Clients are to be informed that COASTLINK is a mandatory reporter, and circumstances in which it is required to inform government agencies of their information (refer Section 7B.7 Reporting Accountabilities and Complaints).
- Client are to be informed of their right to correct any information about them held by COASTLINK.
- Clients are informed of their right make a complaint should they believe a breach of the Australian Privacy Principles has occurred, and how COASTLINK will manage that complaint.
- Clients are to be advised if COASTLINK is likely to disclose information to overseas recipients, and seek their consent prior to such disclosure.

15.2.6 Principle 6: Use or disclosure of personal information

- All information relating to clients is confidential and is not disclosed to any other person or organisation without the client's permission.
- Consent to share personal information can be withdrawn at any time by the client.
- We only share information when it is necessary to ensure appropriate support is delivered and only with the client's permission/consent beforehand.
- The provision of information to people outside the service is authorised by the Operations Manager or CEO.
- We do not discuss clients or their support with people not directly involved in supporting them, including other COASTLINK staff or volunteers.
- If a client is accessing more than one program or service within COASTLINK, their consent should be provided to share relevant information between programs or services, and staff.
- Clients have a right to request that individual staff members not be provided access to their personal information. The Operations Manager or CEO should be advised of this, and measures should be taken to address this.

15.2.7 Principle 7: Direct marketing

Written permission is obtained before images of any services users and their family members are used in any form of media including but not limited to photographs, DVDs, promotional or other material.

Younger people with disabilities will be requested to agree to media use as part of their annual profile renewal. Where this box is not ticked the images will not be used.

In cases where the image of a client is to be used for a media release, promotional DVD or other media platforms we will:

- Seek permission from clients who have not already agreed on the annual profile. Where written permission is not possible, permission will be sought from a person who is involved in the client's life, such as family members, carers, guardians or others with a close and continuing relationship with the client.
- The client should be involved in the decision making to their fullest extent.
- Where a client is the subject of an order made by the Guardianship Tribunal or the subject of an application for guardianship, the consent of the Guardianship Tribunal must be sought and given before any material containing the image or name of the person is broadcast or published.
- Seek permission on each activity where video, photograph or other media is used.
- Only use the material for the purposes for which it was intended.
- Provide clients with a free copy of the video, photograph or other media.
- Inform clients of where the video, photograph or other media will be distributed or seen.
- Where media such as Radio, Newspaper or Television Networks are present at activities organised by COASTLINK we will ensure clients in those situations are aware of their right to choose whether they be interviewed or photographed or taped.
- Where possible, Coastlink will advise media representatives of the right of people with disabilities to give their informed consent prior to being interviewed, photographed or videotaped

15.2.8 Principle 8: Cross –border disclosure of personal information

- COASTLINK does not support the disclosure of client information to overseas recipients, unless for training or service delivery purposes.
- COASTLINK is to obtain written consent from clients prior to the release of their information to an overseas recipient.
- If a client requests that information be shared with a nominee who resides or is travelling overseas, staff should obtain written consent where possible. A second nominee who is in Australia may be provided by the client if the first nominee is to be out of Australia. It is the clients right to choose that their information be provided to a nominee outside of Australia, and COASTLINK staff should work with the client to ensure that they are aware of any potential risks, and agree on how information is to be shared.
- COASTLINK staff and volunteers are to inform the CEO immediately if they suspect, or become aware, that client information may have been disclosed to an overseas recipient.
- The CEO is to inform the Board if client information may have been disclosed to an overseas recipient without the written consent of the client or their nominee.
- The Board will ensure the security of information held by COASTLINK through rigorous information technology maintenance which includes monthly health checks of the system (audits) which provide for a high level of security *(Refer Section 3.3.2).*

15.2.9 Principle 9: Adoption, use or disclosure of government related identifiers

- COASTLINK does not use unique identifiers issued by another agency or government department as the client number
- Unique identifiers, such as a clients NDIS number, may be recorded on the information held by COASTLINK and used for the purposes intended by the issuing agency.
- COASTLINK staff are not permitted to disclose unique identifiers without the consent of the client.

15.2.10 Principle 10: Quality of personal information

- Any information recorded in relation to a client should be accurate and factual
- Information should be verified by the client, their nominee, or the informing agency as being accurate and factual when provided.
- All information recorded should be objective. Staff are not to include their personal views or opinions on a client, their health or wellbeing, but should present the facts that may provide for an informed opinion by those qualified to do so.
- Clients are to be provided information about how and when they may update their information. This can occur by letter, email, phone or informing a staff member of any changes to their information.
- Information should be verified, as being accurate and factual, annually when undertaking the client profile review.
- Any information that is not accurate should be updated as soon as practicable by the Coordinator.

15.2.11 Principle 11: Security of personal information

- Client files and other information are securely stored.
- Client files are only to be accessed by those staff needing to do so in the delivery of services, or for the purpose of internal audits for quality and safeguarding.
- All requests for access to client files by a third party are to be approved by the Operations Manager or CEO.
- Third parties requiring access to client files for the purpose of audits, accreditation, compliance, and legal matters, are to provide a written request as to the reason for access, what information they require, the intended use of the information, and (if any) the relevant legislation or law that allows them to request such access.
- COASTLINK is to obtain written consent from the client or their nominee prior to the release of information to a third party, unless there is reasonable belief that to inform the client of such a request may cause a risk of harm to the client or others, and is permitted within the relevant legislation or law. In such cases, the CEO is to be advised prior to any staff member providing information to a third party.
- COASTLINK will take reasonable steps to restrict access to client files between programs or services unless the client has consented to such access, and it is appropriate for the delivery of quality services.
- Staff are not permitted to keep client information on desks, notice boards, walls or other areas where it might be seen by others, without the consent of the client. Management will undertake periodic checks to ensure that client information if being appropriately managed in working environments.
- Clients who consent to their photo or personal information being on display in the working environment, have the right to withdraw that consent at any time.

15.2.12 Principle 12: access to personal information

Clients of COASTLINK have a right to read any personal information kept about them. A request from a client (or their advocate) to access information is referred to the CEO who confirms the request with the Coordinator and then arranges for the client to view their information.

- Clients can ask to see the information that we keep about them and are supported to access this information if requested. The client can nominate a representative to access the client's records held by us.
- Access is provided to the client within two weeks from the date of the request.

- The Coordinator is available to assist the client in understanding the information and to explain terminology or other assistance.
- Client files should not leave the COASTLINK offices and should be viewed within the office wherever possible.
- If a client requests to view their files outside of the COASTLINK office the CEO is to be informed. The original files should remain in the office, and a copy to be made available for viewing. Two staff, including either a Coordinator or the Operations Manager, should be present when the client is viewing files outside of the office.
- COASTLINK reserves the right to request payment for the photocopying of any files in excess of 50 pages, if the client is requesting a hard copy of files be provided.

15.2.13 Principle 13: correction of personal information

- The client or their advocate or representative can request any changes to their personal information they believe to be incorrect. COASTLINK retains the right to leave the original information in the file if the CEO believes it to be factual. This will be explained with a file note placed within the file and on ProSIMS.
- Any changes made to a client file should include the name of the person providing the information (and their delegation and organisation if required) and the date the changes were provided to COASTLINK.
- The Coordinator is responsible for ensuring that the relevant staff have updated, accurate and factual, information to provide quality services. This should be provided in an email, and confirmation that the staff member has the updated information should be provided.

15.2.14 Client assessments

- Assessments and reviews are always conducted in private with the client and the Coordinator/Assessor unless the client consents to their carer, advocate or other person being present.
- During client assessments, the Coordinator asks the client about any particular privacy requirements they have such as their preference for a male or female support worker. These are noted on their assessment form and on the support plan,
- Any discussions between staff about clients are held in a closed office

15.2.15 Mandatory reporting and risk of harm

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.
- where there is a risk of harm to self or others, including real, perceived or potential risk.

15.2.16 Providing and requesting information under Chapter 16A

Chapter 16A in the Children and Young Persons (Care and Protection) Act 1998 allows information to be exchanged between prescribed bodies despite other laws that prohibit or restrict the disclosure of personal information, such as the Privacy and Personal Information Protection Act 1998, the Health Records and Information Privacy Act 2002 and the Commonwealth Privacy Act 1988.

Previously this information exchange was generally only possible where the information was sent to or received from Community Services.

Chapter 16A allows for the exchange of information between prescribed bodies without Community Services involvement. In this Chapter, the term "organisation" applies to all "prescribed bodies", whether they are government or an NGO.

15.2.16.a Objectives and principles

Chapter 16A establishes a scheme for information exchange between prescribed bodies and requires organisations to take reasonable steps to co-ordinate the provision of services with other organisations.

The four key principles to consider are:

- organisations that have responsibilities for children or young persons should be able to provide and receive information that promotes the safety, welfare or wellbeing of children or young persons
- organisations should work collaboratively and respect each other's functions and expertise
- organisations should be able to communicate with each other to facilitate the provision of services to children and young persons and their families
- the needs and interests of children and young persons, and of their families, in receiving services relating to the care and protection of children or young people takes precedence over the protection of confidentiality or of an individual's privacy.

15.2.16.b Information Sharing

- Information may only be provided under Chapter 16A by the CEO or with written approval of the CEO. Denial of information may also only be provided by the CEO or with written approval of the CEO.
- The CEO will maintain a register, and provide a de-identified report to the Board, on any reports made under Chapter 16A where a real or perceived risk is identified.
- Only information pertaining to the health, safety and wellbeing of the children or young persons that is necessary for the recipient to be able to facilitate the provision of services should be shared.
- Where appropriate, the client and/or their carer should be informed of the exchange of information and its purpose.
- Information received from other organisations in relation to a child or young person should be documented and include the name, delegation and organisation providing the information. The CEO or Operations Manager should be advised of this exchange to ensure it is consistent with the intentions Chapter 16 and not a breach of the Privacy and Confidentiality of the client.

15.2.17 Confidentiality of complaints and disputes

As far as possible, the fact that a client has lodged a complaint and the details of that complaint are kept confidential amongst staff directly concerned with its resolution. Similarly, information on disputes between a client and a staff member or a client and a carer is kept confidential. The

client's permission is obtained prior to any information being given to other parties whom it may be desirable to involve in the resolution of the complaint or dispute.

15.2.18 Destruction of information

- Client information is to be retained for a period of seven (7) years
- Client information will be securely stored in accordance with legislative and legal requirements.
- Client information to be destroyed will be done so in a manner to ensure no risk of release of client information to a third party.
- Client information may be shredded by COASTLINK or by a contracted third party authorised to do so.