Community Living & Respite Services	Policy No.	AD P5	**	
	Issue No. 8		Issue Date: May 2005	
	Revised Date		Nov 2019, Nov 2022	
	Authorised By		Reviewed by Director of Operations	

PRIVACY

POLICY

Community Living & Respite Services (CLRS) will use all reasonable efforts to protect the privacy of individuals' personal information and to comply with the obligations imposed by the *Privacy Act 1988* (Cth) (*Privacy Act),* the Australian Privacy Principles (APP) and all relevant legislation.

SCOPE

This police applies to all clients, employees, labour hire staff, volunteers and students of CLRS.

Purpose of Policy

The purpose of this policy is to:

- Ensure personal information is managed in an open and transparent way;
- Protect the privacy of personal information including Health Information of clients and staff;
- Provide for the fair collection and handling of personal information;
- Ensure that personal information we collect is used and disclosed for relevant purposes only;
- Regulate the access to and correction of personal information;
- Ensure the confidentiality of personal information through appropriate storage and security; and
- Ensure reporting requirements under Department of Health and Human Services Client Incident Management System are met.

DEFINITIONS

Staff/ Staff Member refers to employees, labour hire staff, volunteers and Students of CLRS.

Employment refers to employment, volunteering or placement.

Personal Information refers to information or an opinion, wheth.er true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sensitive Informationrefers to information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, biometric information, biometric templates, health information about an individual and genetic information.

Health Information refers to information or an opinion about:

- the health or a disability (at any time) of an individual; or
- an individual's expressed wishes about the future provision of health services to him or her; or
- a health service provided, or to be provided, to an individual that is also personal information; or
- other personal information collected to provide, or in providing, a health service;
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Likely refers to more probable than not (rather than a possibility), under the judgment of a reasonable person in the entity's position.

Responsible person refers to a parent, a child or sibling, a spouse, a relative, a member of the individual's household, a guardian, an enduring power of attorney, a person who has an intimate personal relationship with the individual, or a person nominated by the individual to be contacted in case of emergency, provided they are at least 18 years of age.

Serious harm refers to physical, psychological, emotional, financial and reputational harm (being upset is insufficient). Three main factors affect whether harm is serious:

- the type(s) of information involved;
- the circumstances of the breach; and
- the nature of harm that might arise.

Staff / Employee Record refers to a record of personal information relating to the employment of the staff member. Examples of personal information relating to the employment of the staff member are all or any of the following:

- The engagement, training, disciplining or resignation of the employee;
- The termination of the employment of the employee;
- The terms and conditions of employment of the employee;
- The staff member's personal and emergency contact details;
- The staff member's performance or conduct;
- The staff member's hours of employment;
- The staff member's salary or wages;
- The staff member's membership of a professional or trade association;
- The staff member's trade union membership;
- The staff member's recreation, long service, sick, personal, maternity, paternity or other leave; and
- The staff member's taxation, banking or superannuation affairs.

Unsolicited Information refers to all personal information received from an individual that we did not actively seek to collect.

PROCEDURE

Collection of personal information

We will only collect Personal Information about an individual by fair and lawful means and only if the information is necessary for one or more of our functions as an aged care provider and collection of the Personal Information is necessary to:

- Comply with the provisions of state or commonwealth law;
- Provide data to government agencies in compliance with state or commonwealth law;
- Determine eligibility to entitlements provided under any state or commonwealth law;
- Provide appropriate services and care;
- Enable contact with a nominated person regarding a client's health status; and
- Lawfully liaise with a nominated representative and to contact family if requested or needed.

Some individuals may not want to provide information to us. The information we request is relevant to providing them with the care and services required. If the individual chooses not to provide us with some

or all of the information we request, we may not be able to provide them with the care and services they require.

We will not collect your Sensitive Information (including Health Information) unless the collection of the information is reasonably necessary for or directly related to one or more of our functions and:

- You have consented to the collection of this information; or
- The collection of the information is required as authorised by or under an Australian law or a court/tribunal order; or
- A permitted general situation exists to the collection of the information; or
- A permitted health situation exists in relation to the collection of the information.

Methods of collection

Personal Information and Sensitive Information (including Health Information), may be collected:

- From a client or resident;
- From any person or organisation that assesses health status or care requirements;
- From the health practitioner of a client or resident;
- From other health providers or facilities;
- From family members or significant persons of a client or resident; and
- From a legal advisor of a client or resident.

We won't collect Personal Information from the client or resident unless:

- We have the consent of the client or resident to collect the information from someone else; or
- We are required or authorised by law to collect the information from someone else; or
- It is unreasonable or impractical to do so.

When engaging with a potential client or resident, the individual should identify any parties from whom they do not wish Personal Information accessed or to whom they do not wish Personal Information provided. This should be recorded in the file of the client or resident and complied with to the extent permitted by law.

Unsolicited Information

If we receive Personal Information from an individual that we have not solicited and we could not have obtained the information by lawful means, we will destroy or de-identify the information as soon as practicable and in accordance with the law.

Staff records

We must keep a record in respect of staff about:

- Basic employment details such as the name of the employer and the staff member and the nature of their employment (eg part-time, full-time, permanent, temporary, casual, volunteer, agency or student);
- Pay;
- Overtime hours;
- Averaging arrangements;
- Leave entitlements;
- Superannuation contributions;
- Termination of employment (where applicable); and
- Individual flexibility arrangements and guarantees of annual earnings.

We may also collect Personal Information about a staff member relating to their employment being Staff/ Employee Records as defined above.

Notification

We will at or before the time or as soon as practicable after we collect Personal Information from an individual take all reasonable steps to ensure that the individual is notified or made aware of:

- Our identity and contact details;
- The purpose for which we are collecting Personal Information;
- The identity of other entities or persons to whom we usually disclose Personal Information to;
- That our Privacy Policy contains information about how the individual may complain about a breach of the APPs and how we will deal with a complaint;
- Whether we are likely to disclose Personal Information to overseas recipients and if so, the countries in which such recipients are likely to be located and if practicable, to specify those countries.

Use and disclosure of information

a) Permitted disclosure

We may not use or disclose Personal Information for a purpose other than the primary purpose of collection, unless:

- the secondary purpose is related to the primary purpose (and if Sensitive Information directly related) and the individual would reasonably expect disclosure of the information for the secondary purpose;
- the individual has consented;
- the information is Health Information and the collection, use or disclosure is necessary for research, the compilation or analysis of statistics, relevant to public health or public safety, it is impractical to obtain consent, the use or disclosure is conducted within the privacy principles and guidelines and we reasonably believe that the recipient will not disclose the Health Information;
- we believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety;
- we have reason to suspect unlawful activity and use or disclose the Personal Information as part of our investigation of the matter or in reporting our concerns to relevant persons or authorities;
- we reasonably believe that the use or disclosure is reasonably necessary to allow an enforcement body to enforce laws, protect the public revenue, prevent seriously improper conduct or prepare or conduct legal proceedings; or
- the use or disclosure is otherwise required or authorised by law.

b) Cross border disclosure

If we disclose an individual's Personal Information to an overseas recipient, we will take all steps that are reasonable in the circumstances to ensure that the overseas recipient does not breach the APP, unless:

- the overseas recipient is subject to laws similar to the APP and the individual has mechanisms to take action against the overseas recipient;
- we reasonably believe the disclosure is necessary or authorised by Australian Law; or
- the individual has provided express consent to the disclosure.

c) Disclosure of Health Information

We may disclose Health Information about an individual to a person who is responsible for the individual if:

- the individual is incapable of giving consent or communicating consent;
- the services manager is satisfied that either the disclosure is necessary to provide appropriate care or treatment or is made for compassionate reasons or is necessary for the purposes of undertaking a quality review of our services (and the disclosure is limited to the extent reasonable and necessary for this purpose); and
- the disclosure is not contrary to any wish previously expressed by the individual of which the services manager is aware, or of which the services manager could reasonably be expected to be

aware and the disclosure is limited to the extent reasonable and necessary for providing care or treatment.

ACCESS

You have a right to request that we provide you access to the Personal Information we hold about you (and we shall make all reasonable attempts to grant that access) unless the request for access:

- is frivolous or vexatious;

OR

- poses a serious threat to the life or health of any individual;
- unreasonably impacts upon the privacy of other individuals;
- jeopardises existing or anticipated legal proceedings;
- prejudices negotiations between the individual and us;
- is unlawful or would be likely to prejudice an investigation of possible unlawful activity;
- denied by an enforcement body performing a lawful security function which asks us not to provide access to the information:
- giving access would reveal information we hold about a commercially sensitive decision making process.

Requesting access

Requests for access to information can be made orally or in writing and addressed to the Senior Manager of the relevant service. We will respond to each request within a reasonable time.

Declining access

An individual's identity should be established prior to allowing access to the requested information. If unsatisfied with the individual's identity or access is requested from an unauthorised party, we can decline access to the information.
We will provide in writing the reasons for declining access to the requested information.

Granting access

On request (and after determining an individual's right to access the information) we should provide access to Personal Information.

Charges

If we charge for providing access to Personal Information, those charges will not be excessive.

PERSONAL INFORMATION QUALITY

We aim to ensure that the Personal Information we hold is accurate, complete and up-to-date. Please contact us if any of the Personal Information you have provided to us has changed or you believe that the information we have about you is not accurate or complete.

CORRECTION

If an individual establishes the Personal Information held about them is inaccurate, incomplete, out-of-date, incomplete, irrelevant or misleading we must take reasonable steps to correct the information.
If we disagree with an individual about whether information is accurate, complete and up- to-date, and the individual asks us to associate with the information a statement claiming that the information is inaccurate, incomplete, out-of-date, incomplete, irrelevant or misleading we must take reasonable steps to do so.

If we refuse to correct the Personal Information as requested by the individual, we will give the individual written notice that sets out:

- the reasons for the refusal, except to the extent that it would be unreasonable to refuse;
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by the regulations.

DIRECT MARKETING

Personal Information
We will not use or disclose Personal Information about an individual for the purposes of direct marketing, unless the information is collected directly from you and:

- you would reasonably expect us to use or disclose your Personal Information for the purpose of direct marketing; and
- we have provided you a means to 'opt-out' and you have not opted out.

Sensitive Information
We will not use or disclose Sensitive Information about an individual for the purposes of direct marketing, unless the individual has consented to the information being used for direct marketing.

An individual's rights in relation to direct marketing activities
If we use information for the purposes of direct marketing the individual may ask us

- not to provide direct marketing communications to us;
- not to disclose or use the information; and
- to provide the source of the information.

PERSONAL INFORMATION SECURITY
We are committed to keeping secure the Personal Information you provide to us. We will take all reasonable steps to ensure the Personal Information we hold is protected from misuse, interference, loss, from unauthorised access, modification or disclosure.

Information of a Client

- We must keep the records of a client in a secure storage area.
- If the records are being carried while providing care only the staff member carrying the records will have access to them.
- Records of previous clients and earlier unused records of current clients shall be archived and stored in a locked service away from general use.
- Only Direct Support Professionals attending to the care of a client are to have access to information of the client. A client record shall only be used for the purpose it was intended.
- A client, or their representatives shall be provided access to records as requested and after consultation with the service manager. At these times, a qualified staff member is to remain with a client or representative to facilitate the answering of any questions raised.
- Details of a client are not to be provided over the phone, unless the staff member is sure of the person making the inquiry..
- No staff member shall make any statement about the condition or treatment of a client to any person not involved in the care except to the immediate family or representative of the client and then only after consultation with the Services Manager.
- All staff must be discrete with their comments at all times, protecting and respecting the privacy, dignity and confidentiality of all clients and residents.
- Handovers shall be conducted in a private and confidential manner.

Security measures
Our security measures include, but are not limited to:

- training our staff on their obligations with respect to your Personal Information;

- use of passwords when accessing our data storage system; and
- the use of firewalls and virus scanning tools to protect against unauthorised interference and access.

This applies to staff (including contracted staff) who are required to have up-to-date virus protection software and firewalls installed on any device used to access documents containing Personal Information. Contractors working on our behalf are required to:

- comply with the APP;
- notify us of any actual or potential breaches of security;
- indemnify us in relation to any loss suffered by a breach.

We will, as soon as practicable and in accordance with the law, destroy or de-identify any Personal Information that is no longer required for our functions.

Client Privacy Incidents

Privacy breaches that impact out-of-home care clients or Victorian based NDIS clients may need to be reported as a client incident under DHHS Client Management System in accordance with the *Out of Home Care Incident Reporting Procedure.*

DATA BREACH

From February 2018 the Notifiable Data Breach Regime (NDBR) came into effect, introducing mandatory data breach notification obligations for all organisations subject to the *Privacy Act.*

The regime requires us to:

- conduct an assessment into a security incident if it has reasonable grounds to suspect that an 'eligible data breach' occurred; and
- notify the Privacy Commissioner and affected individuals if it has reasonable grounds to believe that it suffered an 'eligible data breach'.

What is an 'eligible data breach'?

A data breach occurs if there is unauthorised access to, unauthorised disclosure of, or loss of information (e.g. Personal Information). However, the NDBR does not impose obligations on all types of data breaches.

For the regime to apply, a data breach must be an 'eligible data breach'. A data breach is only an eligible data breach if a reasonable person would conclude that it is likely that an affected individual would suffer serious harm because of the breach.

A data breach would not be considered an eligible data breach if the data is protected to a high standard. For example, if personal information stored on a laptop is encrypted to a high standard and the laptop was stolen, the breach would not be an eligible data breach.

If a data breach occurs, the Office of the Australian Information Commissioner (OAIC) and any affected individuals must be notified in accordance with the *Data Breach Notification Procedure*.

MEDIA

No staff member of staff shall make any statement to the press, radio or television station or to any reporter for the media. If a staff member is approached to make a statement or comment they must refer the person to our Chief Executive Officer.

GRIEVANCE PROCEDURE

How to make a complaint

If you wish to make a complaint about the way we have managed your Personal Information you may make that complaint verbally or in writing by setting out the details of your complaint to any of the following:

Privacy Officer	**Director of Operations**	**Chief Executive Officer**
Phone: 03 5480 2388	Phone: 03 5480 2388	Phone: 03 5480 2388
Email: hr@clrs.org.au	Email: ldavy@clrs.org.au	Email: ceo@clrs.org.au

Further information regarding complaints management can be found in our *Complaints Policy*

Monitoring and Evaluation

Security audits are conducted annually to ensure staff are compliant with securing of information.

Complaints are recorded on a Complaints Register and monitored by the Senior Management, or Board. Client input and comments are sought through the annual client survey.

CLRS is obliged to provide information to the following external agencies:

- Department of Health and Human Services
- Disability Complaints Commissioner
- Office of the Australian Information Commissioner
- Office of the Senior Practitioner
- Quarterly Data Collection