PRIVACY DISCLOSURE AND DIGNITY POLICY AND PROCEDURE

Passion Home and Disability Care Services will manage and ensure that our organization provides the participant access to services and supports that respect and protect their dignity and right to privacy.

This policy applies to all Staff and contractors.

POLICY

Passion Home and Disability Care Services is committed to protecting and upholding all stakeholders right to privacy and dignity; including participants, staff, management and representatives of agencies, we deal with.

We are committed to protecting and upholding the participants right to privacy and dignity as we collect, store and handle information about them, their needs and the services provided to them.

Passion Home and Disability Care Services is subject to NDIS (Quality and Safeguards) Commission rules and regulations. Passion Home and Disability Care Services will follow the guidelines of the Australian Privacy Principles in its information management practices.

We will ensure that each participant understands, and agrees to, what personal information will be collected and informed of the reason for the collection. The participant will be informed and agree to this information is being recorded material in an audio and/or visual format.

We will advise each participant of privacy policies using the language, mode of communication and terms that the participant is most likely to understand. (Easy Read documents are made available to all participants).

We will ensure that:

- It meets its legal and ethical obligations as an employer and service provider in relation to protecting the privacy of participants and organizational personnel.
- The participants are provided with information about their rights regarding privacy and confidentiality.
- The participants and organizational personnel are provided with privacy, and confidentiality is assured when they are being interviewed or discussing matters of a personal or sensitive nature.
- All staff, management and volunteers understand what is required in meeting these obligations.
- Participants are advised of Passion Home and Disability Care Services confidentiality policies using the language, mode of communications and terms that are most likely to be understood.
- We will attempt to locate interpreters and will use easy access materials.

This policy conforms to the Federal Privacy Act (1988) and the Australian Privacy Principles, which govern the collection, use and storage of personal information.

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.

PROCEDURES

Dealing with personal information

In dealing with personal information, Passion Home and Disability Care Services staff will:

- Ensure privacy for the participants, staff, or management 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 organization and its activities.

- Use fair and lawful ways to collect personal information.
- Collect personal information only with consent from the individual.
- Ensure that people know of the type of personal information being held, the purpose of keeping the information and the method 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 the individual to review information or correct wrong information about themselves.
- Take reasonable steps to protect all personal information from misuse and loss and from unauthorized access, modification or disclosure.
- Destroy or permanently de-identify personal information no longer needed and/or after legal requirements for retaining documents have expired.
- Ensure that participants understand and agree with what personal information will be collected and why.
- Ensure participants are informed when any recordings occur in either audio and/or visual format. The participant's involvement in any recording must be agreed to in writing.

Participant Records

Participant records will be kept confidential and only handled by staff directly engaged in the delivery of service to the participant. Information about participants may only be made available to other parties with the consent of the participant, or their advocate, guardian or legal representative. A written agreement giving permission to the recording must be maintained in the participant's file.

All hard copy files of participant records will be kept securely in a locked filing cabinet, in the office space.

Responsibilities for Managing Privacy

All staff is responsible for the management of personal information to which they have access. Director is responsible for the content in Passion Home and Disability Care Services publications, communications and on the website and must ensure the following:

- Appropriate consent is obtained for the inclusion of any personal information about any individual, including Passion Home and Disability Care Services personnel (Consent Policy and Procedure)
- Information being provided by other agencies or external individuals conforms to privacy principles
- That the website contains a Privacy Statement that makes clear the conditions of any collection of personal information from the public through their visit to the website.

The Director is responsible for safeguarding personal information relating to Passion Home and Disability Care Services staff, management and contractors. The Director will be responsible for:

- Ensuring that all Staff is familiar with the Privacy Policy and administrative procedures for handling personal information.
- Ensuring that participants and other relevant individuals are provided with information about their rights regarding privacy and dignity.
- Handling any queries or complaints about a privacy issue.

Privacy Information for Participants

At the first interview, participants will be notified of the type of information is being collected about them, how their privacy will be protected, and their rights in relation to this data. Information sharing is part of our legislative requirements. Participants must give consent to any information sharing between our organisation and government bodies. The participant is offered to opt-out of any NDIS information sharing during audits.

Privacy for Interviews and Personal Discussions

To ensure privacy for participants or Staff when discussing sensitive or personal matters, Passion Home and Disability Care Services will only collect personal information which is necessary for the provision of supports and services and which:

- Is given voluntarily; and
- Will be stored securely on the Passion Home and Disability Care Services database.

When in possession or control of a record containing personal information, Passion Home and Disability Care Services will ensure that the record is protected against loss, unauthorised

sed access, modification or disclosure, by such steps as it is reasonable in the circumstances to take. If it is necessary for that the record be given to a person in connection with the provision of a service to Passion Home and Disability Care Services, everything reasonable will be done to prevent unauthorised use or disclosure of that record Passion Home and Disability Care Services will not disclose any personal information to a third party without the individual's consent unless that disclosure is required or authorised by or under law.

CONFIDENTIALITY POLICY AND PROCEDURE

The purpose of this policy and procedure is to ensure Passion Home and Disability Care Services upholds each participant's individuality, dignity and privacy. The policy sets out Passion Home and Disability Care Services responsibilities relating to the collection and protection of participant's information.

Definition

Health information – Any information or an opinion about the physical, mental or psychological health or ability (at any time) of an individual.

Personal information – Recorded information (including images) or opinion, whether true or not, about a living individual whose identity can reasonably be ascertained.

Sensitive information – Information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political party, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preference or practices, or criminal record.

POLICY

Privacy and confidentiality of participant's information are of paramount importance to Passion Home and Disability Care Services. We will only collect information necessary for effective service delivery. We will only use information collected for the purpose it was collected and secure it appropriately.

We will collect, use and disclose information in accordance with relevant state and Federal privacy legislation.

PROCEDURES

- Passion Home and Disability Care Services will keep participants informed of their rights.
- We will ensure participant and or their authorised representative has access to participant personal information.
- We will keep participant information secure.
- Computers and laptops will be protected by user access credentials.
- We will not release information related to participants to other individuals or services without the consent of the participant or their representative.
- We will respect participant's right to withdraw from consent at any time.
- We will collect, use and disclose information in accordance with relevant state and Federal privacy legislation.
- All staff are responsible for upholding Company's privacy and confidentiality responsibilities.
- Management will make arrangements for participants with special needs to assist with protecting their privacy and dignity.
- We will give due consideration to individuals and groups with special needs when upholding their privacy, dignity and confidentiality.
- We will capture participant information the privacy of their home or in our office and ensure that it is in an area that prevents other people from hearing their personal details.
- Participant privacy will be respected, and assistance will be given in a dignified and appropriate manner during social outings or in their own home.

- Staff will ensure time and space for participant privacy, respecting and encouraging participant independence.
- Individual choice will be respected in regard to clothing and grooming, taking into account various factors such as the weather to ensure warmth if cold or to avoid overheating during hot seasons.
- Employees will show respect for the participant's home and participant belongings.
- Company will collect, use and disclose information in accordance with relevant state and Federal privacy legislation.
- Participant Information will not be collected or released to other individuals or services without informed consent from the participant or their representative, or in exceptional circumstances i.e., where legislation requires, in case of life threating emergency.
- Clinical records to be kept in a locked filing cabinet when not being used in the office; if a home file is kept this is to be kept discretely and privately in the participant's home where the participant wishes to keep it.
- Company will not provide participant information over the phone as it is difficult to determine the identity of the caller(s).
- Company will ensure improvements identified through staff and participant feedback, are actioned through the company's Continuous Improvement Plan.
- Company will monitor staff knowledge and application of confidentiality and privacy principles on-the-job and through yearly Performance Reviews.
- Company will provide additional on-the-job and formal training to staff where required.

Staff Privacy and Confidentiality

Staff information Passion Home and Disability Care Services collects include, but is not limited to tax declaration form; employment / engagement contract; personal details; emergency contact details; medical details; Police and Working with Children Check records; Qualifications; First Aid, CPR and Anaphylaxis certificates; medical history; personal resume; payroll information; and Superannuation details

Staff information may be accessed the Management Team.

Staff have the right to request access to personal information Passion Home and Disability Care Services holds about them, without providing a reason for requesting access; access this information; and make corrections if they consider the information is not accurate, complete or up to date.

If an individual requests access to or the correction of personal information, within a service benchmark of 2 working days (and no more than 45 days after receiving the request), staff will provide access, or reasons for the denial of access; correct the personal information, or provide reasons for the refusal to correct the personal information; or provide reasons for the delay in responding to the request for access to or correction of personal information.

Staff personal and health information will only be disclosed for medical treatment or emergency; with written consent from the staff member; or when required by Commonwealth Law, or to fulfil legislative obligations such as mandatory reporting.

Monitoring and Review

Passion Home and Disability Care Services Management Team will review this policy and procedure at least annually. This process will include a review and evaluation of current practices and service delivery types, contemporary policy and practice in this clinical area, the Incident Register and will incorporate staff, participant and another stakeholder feedback. Feedback from service users, suggestions from staff and best practice developments will be used to update this policy.

Passion Home and Disability Care Services Continuous Improvement Plan will be used to record and monitor progress of any improvements identified and where relevant feed into Passion Home and Disability Care Services service planning and delivery processes.

MANAGEMENT OF DATA BREACH POLICY AND PROCEDURE

To meet legislative compliance requirements as a mandatory reporter of eligible data breaches to both the Office of the Australian Information Commissioner (OAIC) and any individuals who may be potentially affected by a data breach; to inform relevant authorities of any breach, and to limit and reduce risks to the business and ensure continuous improvement in maintenance of data held by our organisation.

All Staff are required to maintain the confidentiality of all data relating to participants and other Staff members. This policy relates to all personal data regarding both participants and team members.

POLICY

Passion Home and Disability Care Services views data breaches as having serious consequences, so the organisation must have robust systems and procedures in place to identify and respond effectively.

Passion Home and Disability Care Services will delegate relevant staff members with the knowledge and skills required to become a Response Team member.

Staff are required to inform the Director or their delegate of the potential, or suspected, data breach immediately. Within forty-eight (48) hours, the Director is to complete a Data Breach Process Form and ensure that, as a regulated entity, they notify the particular individuals and the Commissioner about eligible data breaches as soon as practicable (no later than thirty (30) days after becoming aware of the breach or suspected breach).

If a staff member becomes aware that there are reasonable grounds to believe that there has been an eligible data breach, Passion Home and Disability Care Services is required to promptly notify any individuals at risk of being affected by the data breach and the OAIC.

Passion Home and Disability Care Services will undertake the following when an eligible data breach has occurred:

1) Prepare a statement that, at a minimum, contains:
    a) Passion Home and Disability Care Services contact details:
        i) If relevant, the identity and contact details of any entity that jointly or simultaneously holds the same information, in respect of which the eligible data breach has occurred, e.g., due to outsourcing, joint venture or shared services arrangements. If information of this sort is included in the statement, the other entity will not need to report the eligible data breach separately.
    b) A description of the data breach.
    c) The kinds of information concerned.
    d) The steps it recommends individuals take to mitigate the harm that may arise from the breach (while the entity is expected to make reasonable efforts to identify and include recommendations, it is not expected to identify every recommendation possible following a breach).
2) Provide a copy of the prepared statement to the OAIC using online Notifiable Data Breach Form.
3) Undertake such steps, as are reasonable in the circumstances, to notify affected or at-risk individuals of the contents of the statement. Individuals will be notified by email, telephone or post, depending on the situation; if direct notification is not practicable Passion Home and Disability Care Services will publish the statement on its website and take reasonable steps to publicize its contents.

Definition

Data breach (Eligible Data Breach) Unauthorised access to or unauthorised disclosure of personal information or personal information is lost in circumstances where unauthorised access to, or unauthorized disclosure of the information is likely to occur.

Likely (likely to result in serious harm) To be interpreted to mean more probable than not

Reasonable person A person in Passion Home and Disability Care Services who is properly informed, based on information immediately available or following reasonable enquiries, or an assessment of the data breach.

Likely to result in serious harm

OAIC Office of the Australian Information Commissioner

Likely to result in serious harm

An assessment as to whether an individual is likely to suffer 'serious harm' because of an eligible data breach depends on, among many other relevant matters:

- the kind and sensitivity of the information subject to the breach
- whether the information is protected and the likelihood of overcoming that protection
- if a security technology or methodology is used in relation to the information to make it unintelligible or meaningless to persons not authorised to obtain it - the information or knowledge required to circumvent the security technology or methodology
- the persons, or the kinds of persons, who have obtained, or could obtain, the information
- the nature of the harm that may result from the data breach.

Potential forms of serious harm Could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation.

Remedial action There are a number of exceptions to the notification obligation, including importantly where an entity is able to take effective remedial action to prevent unauthorised access to, or disclosure of, information when it is lost or to prevent any serious harm resulting from the data breach. Where such remedial action is taken by an entity, an eligible data breach will not be taken to have occurred, and therefore an entity will not be required to notify affected individuals or the OAIC

Suspicion of an eligible data breach If Passion Home and Disability Care Services merely suspects that an eligible data breach has occurred, but there are no reasonable grounds to conclude that the relevant circumstances amount to an eligible data breach, the entity must undertake a "reasonable and expeditious assessment" of whether there are in fact reasonable grounds to believe that an eligible data breach has occurred

Assessment time frame Within 30 days after the day, it became aware of the grounds that caused it to suspect an eligible data breach.

Personal Information Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is identifiable in the circumstances.

For example, personal information may include:

- an individual's name, signature, address, phone number or date of birth
- sensitive information
- credit information

- staff member record information
- photographs
- internet protocol (IP) addresses
- voiceprint and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)
- location information from a mobile device (because it can reveal user activity patterns and habits)

PROCEDURE

Stage 1. Assess and determine the potential impact

- Once notified of the potential data breach, the Director must consider whether a privacy data breach has (or is likely to have) occurred and then make a preliminary judgement as to its possible severity. Advice on how to manage the data breach should be sought from appropriate managerial Staff.
- Criteria for determining whether a privacy data breach has occurred:
    - Is personal information involved?
    - Is the personal information of a sensitive nature?
    - Has there been unauthorised access to personal information, or unauthorised disclosure of personal information or loss of personal information, in circumstances where access to the information is likely to occur?
- Criteria for determining the severity of the breach:
    - Type and extent of personal information involved.
    - The number of individuals that have been affected.
    - If information is protected by any security measures (password protection or encryption).
    - Type of person/s who now have access.
    - Whether there is (or could be) a real risk of serious harm to the affected individuals.
    - If there could be media or stakeholder attention due to the breach/suspected breach.
- With respect to the above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in Section 26WG of the National Data Breach Act.

The Director and relevant staff will take a preliminary view as to whether the breach (or suspected breach) may constitute a Notifiable Data Breach. Accordingly, the Director will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team); this will depend on the nature and severity of the breach.

Stage 2. Select appropriate data breach management option

Data breach managed at a local level by managerial Staff

1. The Director will ensure implementation of immediate corrective action if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
2. A Data Breach Process Report is to be completed within 48 hours of receiving instructions. The report will contain a:
    - description of the breach or suspected breach

- summary of action taken
- summary of outcomes from the action taken
- outline of processes implemented to prevent a repeat situation
- recommendation outlining why no further action is necessary.

3. The Director will sign-off, confirming that no further action is required.

Data breach managed by the Data Breach Response Team

1. When the Director instructs that the data breach be escalated to the Response Team, the Director will convene the Response Team and notify any relevant managerial staff.

2. The Response Team will consist of:

   - Director
   - Human Resource nominee
   - Information Technology nominee
   - Marketing and external relations nominee
   - Other people nominated by the Director.

Primary role of the Data Breach Response Team

There is no single method of responding to a data breach. Each incident must be dealt with, on a case by case basis, by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team, as appropriate:

1. Immediately contain the breach, if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.

2. Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach, having regard for the information outlined above.

3. Call upon the expertise of, or consult with, relevant Staff in specific circumstances.

4. Engage independent cybersecurity or a forensic expert, as appropriate.

5. Assess whether serious harm is likely (with reference above and to Section 26WG of the National Data Breach Act).

6. Make a recommendation to the Director whether this breach constitutes an NDB for mandatory reporting to the OAIC, and the practicality of notifying affected individuals.

7. Consider developing a communication or media strategy including the timing, content and method of any announcements to participants, Staff or the media.

8. The Response Team must undertake its assessment within 48 hours of being convened.

Secondary role of the Data Breach Response Team

Once the data breach has been dealt with appropriately, the Response Team should turn its attention to the following steps:

1. Identify lessons learnt and remedial action that can be taken to reduce the likelihood of a recurrence; this may involve a review of policies, processes and refresher training.

2. Prepare a report for submission to senior management.

3. Consider conducting an audit to ensure that necessary outcomes are affected and effective.

Stage 3. Notify the Office of the Australian Information Commissioner

- Taking into consideration the Response Team's recommendation, the Director will determine whether there are reasonable grounds to suspect that a Notifiable Data Breach has occurred.
- If there are reasonable grounds, the Director must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

If you would like more information about our Privacy Policy or the way we manage your personal information, you can contact the Privacy Officer by:

Email: submit enquiry/feedback: NDIS Commission using the following contact details: contactcentre@ndiscommission.gov.au

Telephone:1800 035 544 OR By Post: NDIS Commission Feedback, PO Box 210, Penrith. NSW 2750,

For complaints about a breach of your privacy: Email: internalintergrity@ndiscommission.gov.au

Post: (Same address as above)

Alternatively, additional information on the Australian Privacy Principles can be obtained from the Office of the Australian Information Commissioner website