POLICY AND PROCEDURE MANUAL

Policy 4.2 Privacy and Information Management

Reference Documents

- Participant Registration Form
- Customer Consent Form
- Australian Privacy Principles
- Privacy Act 1988 (Cth)
- NDIS (Quality Indicators) Guidelines 2018

Date of CEO Endorsement: 19/10/2023

Last Review Date: 19/10/2023

Next Review Date: 18/10/2025

Policy Statement

1. Participants and carers right to privacy and confidentiality is recognised, respected and protected in all aspects of their contact with Thrive365.
2. Thrive365 will at all times operate according to the requirements of applicable privacy legislation.
3. Thrive365 will only request and retain information that is necessary to:
   - assess a potential Participant's eligibility for a service;
   - provide a safe and responsive service;
   - monitor the services received;
   - fulfil our duty of care responsibilities; and
   - fulfil contract requirements to provide non-identifying data and statistical information to a funding body.
4. Thrive365 is committed to ensuring the confidentiality of all Participant information, in all the forms in which it might be stored. All Participant service records are to be kept up to date and stored securely.
5. Participants will have access on request, to the information that Thrive365 holds about them, and have the right to have any inaccurate information corrected.
6. Participant information will generally not be disclosed to a third party without the prior knowledge and consent of the Participant or their appointed guardian, attorney or advocate. However, there are occasions where Thrive365 must release personal information to a third party such as:-

- There are reasonable grounds to believe that the participant is a risk to themselves or to others or that the participant is at imminent risk of harm from others.
- Fulfilling legal obligations such as mandatory reporting
- In situations where Thrive365 is legally obligated to make documentation available such as when subpoenaed by a court or tribunal.

7. Personal information may include the following:
   - medical conditions and health status;
   - racial or ethnic background;
   - political opinions and membership of political organisations;
   - religious and philosophical beliefs and/or affiliations;
   - employment, qualifications and/or industrial affiliations;
   - sexual preferences or practices;
   - Government identifiers such as Medicare numbers, NDIS participant numbers
   - Bank account details

Procedures

Participant and Carer Information

As part of their onboarding to Thrive365 participants are provided with:-

- A service agreement which outlines how Thrive will manage personal information.
- A participant consent form for release of any information to Thrive365.
- Access to Thrive365 privacy policy via our website.
- Access to the website terms and conditions via website
- An image consent form (in the ***Appendix***)

Staff Office Practices

- All Thrive365 staff sign a confidentiality agreement and code conduct as part of their onboarding.
- Thrive365 gradates access to its IT systems according to staff member delegation.
- Access to IT systems are password protected.
- Paper files are maintained in locked filing cabinets. Staff offices located in each house are locked.
- Staff are provided with Thrive365 devices such as phones and tablets. No information of any form of media relating to Thrive365 including images of participants or staff, can be taken off the premises without prior permission of CEO.

- Staff are not to use their own media devices to take photographs of participants or other staff.
- Staff are not to use their own devices to access participants' files e.g. in CTARs.
- Archived documents are only accessible to staff with the delegated authority to access the record, or to others as are required by law.

Privacy Officer

Thrive365's privacy officer is the CEO.

Requests for Information from Third Parties

Thrive365 direct support staff must seek advice from their line supervisor before releasing any information to a third party about a participant.

All requests for information from the media must be referred to the CEO.

Release of information regarding a participant in emergency circumstances

All staff are authorised to release information regarding a participant in emergency situations where the health and wellbeing of the participant or another person is at risk. This may include:-

- Release of medical records or medication summaries to hospital, ambulance or GP
- Release of an image or information about a participant to police e.g. if the person is missing
- A report is required to the NDIS Quality and Safeguards Commission e.g. to notify of a notifiable incident.
- Release of information to a tribunal such as NCAT or QCAT
- If a staff member is in a situation where they believe that they need to disclose information about a Participant that they ordinarily would not disclose, they should seek the advice of the Program Manager before making the disclosure.

Additional Practices

- Computer screens must not be visible to members of the public
- Participant files are not to be left on unattended desks.
- Staff must log off their computer when they leave their desk and must not reveal their access password to another person.
- Hard copies of information regarding service users will be stored in a filing cabinet that is kept locked when the office is unattended, with keys only available to authorised staff.

- Participant files, or individual sections or pages of files, are not to be removed from Thrive365 premises in any format, unless Thrive365 is so directed by an authority with the legal mandate to give the direction to do so.
- Information from a Participant file is not to be copied, except as part of a backup procedure, without the express permission of the Participant.
- Organisational arrangements for maintaining Participant privacy and confidentiality will be reviewed annually as part of a privacy audit.

Thrive365 Information Management Procedures

Thrive365 utilises the CTARs client management system as its key information storage device for participants. CTARS is password protected with gradated access according to staff delegation level.

CTARS is a cloud-based system.

Thrive365 is committed to ensuring that the information it collects, creates and stores about participants is :-

- Accurate
- Recorded appropriately i.e. case notes are constructed professionally and based on fact, not opinion.
- Recorded observations are within the skill set and delegation of the worker making the observation.

Information stored in CTARS is routinely reviewed by senior staff.