Privacy and Confidentiality Policy and Procedure

Purpose

This purpose of this policy and procedure is to outline the duties of employees to collect, use, protect and disclose private data in accordance with the legislation on privacy. This policy should be read in combination with the Records and Information Management Policy and Procedure.

Scope

This policy and procedure applies to all

- Thrive Disability Services & Carer Support employees;
- Aspects of activities of Thrive Disability Services & Carer Support; and
- Private and health data of employees and clients

Statement

Thrive Disability Services & Carer Support protects the privacy of everyone, including the privacy of their clients and employees. All persons (or their legal agents) are entitled to decide who has access to their private data.

Thrive Disability Services & Carer Support collects, uses and discloses data in accordance with appropriate state/territory laws and Federal Privacy Act.

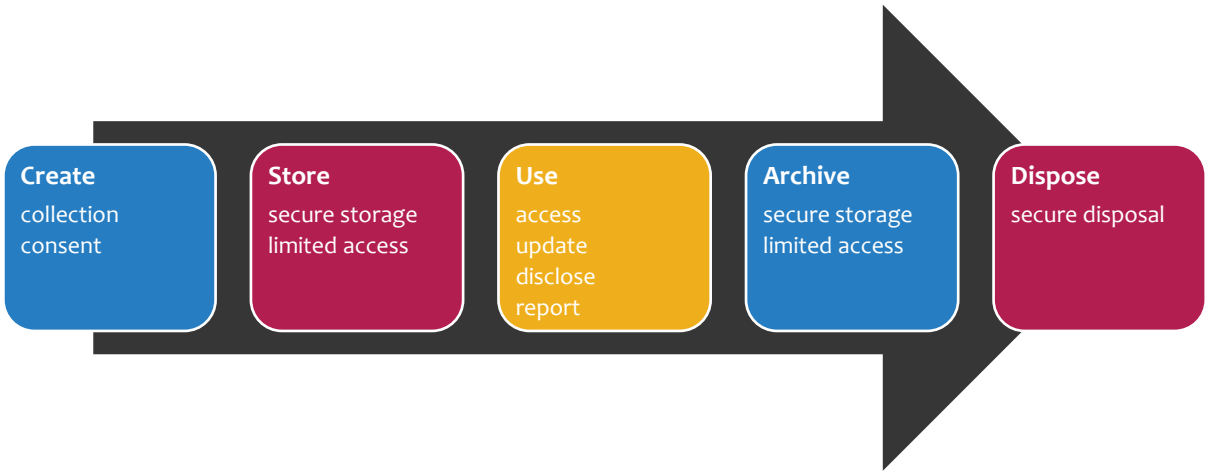
Thrive Disability Services & Carer Support promotes and supports privacy and confidentiality procedures through its documents and information management procedures (see Records and Information Management Policy and Procedure).

Thrive Disability Services & Carer Support shall obtain only the data needed for the secure and efficient provision of the service. It will only use collected data for the purpose it has been gathered and properly secure it.

All employees are liable for preserving Clients, other employees and the organisations privacy and confidentiality.

Thrive Disability Services & Carer Support Privacy Statement must be prominently exhibited in the premises of Thrive Disability Services & Carer Support and included in the Client Handbook of Thrive Disability Services & Carer Support. It is necessary to provide a complete copy of this policy and procedure upon request.

The procedures of privacy and confidentiality communicate with the lifecycle of data as follows:



Responsibilities

Managing Director	• ensuring that Thrive Disability Services & Carer Support meets the criteria of the 1988 (Cth) Privacy Act as well as all other relevant state/territory laws and requirements. This involves the development, implementation and review of procedures addressing: o Why and how we collect, uses and discloses personal data o What information is gathered about individuals and their source o Who has access to data o Collection, storage, access, use, disclosure and disposal of data o How people can consent to the collection, withdrawal or alteration of private data o Their approval and modification of data o How information is safeguarded and how we manage private data, including how it handles privacy queries and complaints o How we manage data that needs to be updated, demolished or deleted. • Privacy Policy and procedures are frequently reviewed through annual Privacy Audits. • Employees ' understanding and implementation of procedures to manage confidentiality, privacy and data is tracked on a daily basis and through annual performance reviews.
Employee	• reading and acting in compliance with this policy and

	procedure and their duties for data protection, confidentiality and data management. • Collection, processing, storage, use, disclosure and disposal of private and health information from clients, other employees or stakeholders in accordance with state and federal legislation and this policy and procedure. • Information from other employees and other stakeholders must be held in accordance with the confidentiality requirements of their jobs or contract of commitment. • undergo Induction, which involves instruction in privacy, confidentiality and management of data. • Undertake additional formal and on - the-job training where necessary.

Photos and Videos

Photos, videos and other recordings are a form of personal information. Employees must respect people's choices about being photographed or videoed and only use images of people when informed consent has been obtained. This includes being aware of cultural sensitivities and the need for some images to be treated with special care.

Information Collection and Consent

Client Information Collection and Consent Thrive Disability Services & Carer Support will only ask for private data required to:

- Assess the eligibility of a prospective client for a service
- Provide a secure and responsive service
- Monitor the services supplied
- Fulfil government non-identification and statistical data demands. Personal client data that Thrive Disability Services & Carer Support collects involves but is not restricted to:
    - Clients and their parents and guardians contact details.
    - Emergency contact details and individuals authorized to collect clients.
    - Health status of clients and medical documents.
    - Records of immunization.
    - Records of medicines.
    - Information about the external agency.
    - Reports of incidents.
    - Arrangements for custody.
    - Permit/Forms of consent.
    - Intake of service delivery, evaluation, review of data.
    - Records of development, plans, portfolios and observations.

Before gathering private data from clients or their agents, employees must clarify:

- That Thrive Disability Services & Carer Support only collects private data needed for

the secure and efficient delivery of services • that private data kept safely is used only for the purpose of obtaining it;
- What data is needed;
- Why the data is being gathered and how it will be stored and used;
- Occasions when it may be necessary to disclose the data and who or where the data may be revealed;
- The right of the Client to refuse to disclose the data;
- The rights of the Client to supply, access, update and use private data and to give and withdraw their permission; and
- the implications (if any) if all or part of the necessary data is not supplied.

Clients and their relatives must receive a Privacy Statement from Thrive Disability Services & Carer Support and notify them that a copy of this policy and procedure is accessible on request.

Employees must provide Clients and their families with data on privacy in ways that match their individual communication requirements. Written data can be given or clarified verbally by employees in [distinct languages and easy English]. Employees can also assist clients when needed to access interpreters or advocates. What languages does the company provide data in distinct languages? Easy English formats are becoming more of a necessity and auditors are beginning to look more actively for data in this format to be supplied.

After providing the above information, employees must use a Consent Form to:
- Confirm and explain the above-mentioned data; and
- Obtain permission from clients or their legal agents to collect, store, access, use, disclose and dispose of their private data.

Clients and their representatives or families are responsible for:
- Provide precise data when required;
- Complete and return consent forms in a timely way;
- be delicate and respectful to others who do not wish to be photographed or videotaped;
- Be sensitive and respectful of other people's privacy in the use and disposal of photographs and videos.

NDIS Audits

Thrive Disability Services & Carer Support fulfils the criteria of the 2018 National Disability Insurance Scheme (Approved Quality Auditors Scheme) Guidelines whereby Clients are automatically included in NDIS Practice Standards audits. A NDIS Approved Quality Auditor may contact clients at any moment for an interview or for their client file and plans to be reviewed.

Clients who do not wish to engage in audits may notify any employee who is required to provide written notification to Managing Director. Their choice will be respected and

recorded in their Client file by Thrive Disability Services & Carer Support. Thrive Disability Services & Carer Support shall notify its Approved Quality Auditor of clients who have refused to participate in the audit upon commencement of any audit process.

Employees Information Collection and Consent

Personal employees information that Thrive Disability Services & Carer Support collects includes, but is not limited to:

- Details about professional registration
- Forms of tax returns
- Details of superannuation
- Payroll information
- Contracts for employment/engagement
- Personal information
- Details of emergency contact
- Medical details
- NDIS Worker Screening Checks, Police Checks and Child Checks
- Qualifications
- First aid, CPR, anaphylaxis and other certificates
- Personal resumes
- Forms of permission

Where applicable, forms used to collect the above information will also obtain the consent of the employee member to collect, store, access, use, disclose and dispose of their personal information.

Storage

For details on how Thrive Disability Services & Carer Support safely stores and protects private data to employees and clients, see the Records and Information Management Policy and Procedure.

Access

Personal information of the employee must only be accessed by the [Position Title], who can access the data only if it is necessary to fulfil their responsibilities.
Employees only have to access the private data of Clients if it is necessary to carry out their responsibilities.

Employees and Clients have the right to:

- Request access to private data Thrive Disability Services & Carer Support holds about them, without offering a reason to request access;
- access this data; and
- make corrections if they think the data is not precise, complete or up-to-date.

All requests for Client access or correction must be addressed to the employee responsible for maintaining the personal information of the Client. All employees have access to or demands for correction
The [Position Title] must be addressed. Within [2 working days] of obtaining a request for access or correction, the answering member will:

- provide access or clarify why access is refused;
- correct private data or give reasons for not correcting it; or
- provide explanations for any expected delay in responding to the request.

An application for access or correction may be rejected in whole or in portion where:

- The application is frivolous or vexatious;
- It would have an unfair effect on the privacy of other persons;
- It would pose a severe danger to any person's life or health; or
- It would bias any investigation conducted by Thrive Disability Services & Carer Support or any other individual.
- It may be the topic of investigations.

Any applications for Client access or correction denied by the Managing Director must be approved and recorded in the Client's file.

Any employees who are denied access or correction demands must be endorsed by the Managing Director and recorded in the file of the Employee.

Disclosure

Personal data of the client or employee may only be revealed:

- For emergency medical therapy;
- To external organizations with the permission of the person [or of the child Clients, parents or guardians];
- With the written consent of the authorized person;
- To fulfil parliamentary responsibilities such as compulsory reporting when needed by legislation.

If an employee is in a position where they think they need to reveal data about a Client or other employee that they would not normally disclose, they must consult the Managing Director before disclosing the data.

International Disclosure

Under the Privacy Act 1988,Thrive Disability Services & Carer Support must take appropriate measures to guarantee that the foreign recipient does not infringe Australian Privacy Principles (APPs) Principle 8 before disclosing private data to an overseas recipient. The Managing Director is liable for carrying out these inquiries.

This requirement does not apply if:

- the foreign recipient is subject to a legislation or binding system which has the

impact of protecting the data in a manner significantly comparable to that provided by the APPs, and
- Mechanisms are accessible to implement that protection.

Notifiable Data Breaches

Under the Privacy Act 1988 (Cth), the Notifiable Data Breaches (NDB) Scheme is a federal scheme. Organizations are needed to report certain infringements of information to those affected by the infringement, as well as the Australian Information Commissioner. A violation of data occurs when private information retained by organizations is lost or unauthorized access to it. A data breach may happen as a result of malicious action, human error, or management or security system failure.

Examples of data breaches include:
- Loss or robbery of devices (such as phones, laptops and storage systems) or paper documents containing private data
- Unauthorized access by an employee to private information
- inadvertent disclosure of private information owing to' human mistake,' such as an email sent to the incorrect individual
- Disclosure of private data to a scammer as a consequence of insufficient processes for verifying identity

Besides the harm caused to individuals who are the topic of information breaches, such an event can also cause reputational and economic damage to Thrive Disability Services & Carer Support.

The Data Breach Preparation and Response — A Guide to Managing Data Breaches under the Privacy Act 1988 (Cth), released by the Office of the Australian Information Commissioner (OAIC), provides further details on the NDB Scheme.

The Data Breach Response Plan of Thrive Disability Services & Carer Support describes its approach to contain, assess and manage incidents of data breach.

Identifying a Notifiable Data Breach

A Notifiable Data Breach, occurs when:
- Access to or disclosure of private data is unauthorized or data is lost in conditions in which unauthorized access or disclosure is likely to happen;
- Disclosure or loss is likely to cause severe damage to any of the persons concerned by the data. Serious harm may involve severe physical, psychological, emotional, economic or reputational damage in the context of an information violation; and
- Thrive Disability Services & Carer Support was unable to avoid the probable danger of severe harm through remedial action.

All possible or actual breaches of information must be reported to the Managing Director who will determine the reaction of Thrive Disability Services & Carer Support and whether the violation must be recorded under the NDB Scheme.

If Thrive Disability Services & Carer Support reacts rapidly to mitigate a data breach and is therefore unlikely to cause severe damage, it is not regarded to be a notifiable data breach.

Responding to a Data Breach

If the Managing Director suspects that, under the NDB Scheme, a data breach is notifiable, they must create an evaluation to determine whether this is the case.

If the Managing Director considers the data breach to be notifiable under the NDB Scheme, they must notify the Data Breach Response Team. Responsibilities of Managing Director include:

- Accountable for guiding the reaction team who report to the Managing Director;
- Coordinating the team and supporting its clients;
- Introducing privacy knowledge to the team;
- Provide legal assistance, identifying legal commitments and providing guidance
- Provide support for risk leadership, assessing danger from infringement;
- Provide support for information and communication technology (ICT) or forensics, helping to define the cause and effect of infringement involving ICT technologies;
- Providing information and documents management knowledge, assisting in the review of breach-related safety and tracking checks (e.g. access, authentication, encryption, audit logs) and providing guidance on recording data breach reaction;
- Supporting human resources where the infringement was caused by the Employee's actions; and
- Providing media/communications knowledge and helping to communicate with impacted people and deal with media and external stakeholders.

The Data Breach Response Team must notify the breach as quickly as practicable to all affected people.

All incidents of information violation (whether notifiable or not) must be addressed in accordance with the Data Breach Response Plan and registered in the Incident Register, where appropriate, with relevant actions tracked in its Continuous Improvement Register.

Where a violation is referred to the Data Breach Response Team, its reaction will be based on the following steps:

1. contain data infringement;
2. assess information breach and related hazards;
3. notify people and the Australian Information Commissioner; and

4. Prevent future infringements.

See Thrive Disability Services & Carer Support's Data Breach Response Plan for further detail.

Notifiable Data Breaches Involving More Than One Entity

The NDB Scheme recognizes that more than one entity often holds private data together. For instance, one entity may possess the information physically, while another may have legal control or ownership of the information.

Examples include:

- Where cloud service supplier holds data;
- Agreements for subcontracting or brokering; and
- Joint ventures.

In these conditions, the liability of both companies under the NDB Scheme is regarded to be an eligible information violation. However, only one organization requires to take the measures that the NDB Scheme requires, and this should be the organization with the most direct connection with the individuals impacted by the data breach. Where responsibilities under the Scheme (such as evaluation or notification) are not fulfilled, both organizations will be in violation of the demands of the Scheme.

Other Reporting Requirements

The Managing Director must immediately notify the NDIS Commission and if they become conscious of an infringement or possible infringement of privacy law.

Infringements of data may also cause reporting commitments outside the Privacy Act 1988, such as:

- The financial services provider of Thrive Disability Services & Carer Support
- The police or other law enforcement agencies
- The Australian Securities and Investment Commission (ASIC)
- Australian Tax Office (ATO)
- Government Departments of the Federal, State or Territory
- Professional and regulatory associations
- providers of insurance

Archiving and Disposal

Refer to the Records and Information Management Policy and Procedure for details on how Thrive Disability Services & Carer Support archives and disposes of Clients' personal information.

Supporting Documents

Documents relevant to this policy and procedure include:

- Consent Form
- Records and Information Management Policy and Procedure
- Data Breach Response Plan
- Continuous Improvement Register
- Client Handbook
- Privacy Statement