1.1. PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

1.2. Purpose and Scope

This policy and procedure lays out the duties of employees to collect, use, protect and disclose private data in accordance with the legislation on privacy.

It applies to all:
• Perfect Care Pty Ltd employees;
• Aspects of activities of Perfect Care Pty Ltd; and
• Private and health data of employees and clients

It should be read in combination with the Records and Information Management Policy and Procedure of Perfect Care Pty Ltd. It includes the policies and processes set out in the General Privacy and Privacy Policy and Procedure of Perfect Care Pty Ltd. It complies with applicable laws, regulations and standards.

1.3. Definitions

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. This is also considered to be personal information.

1.4. Policy

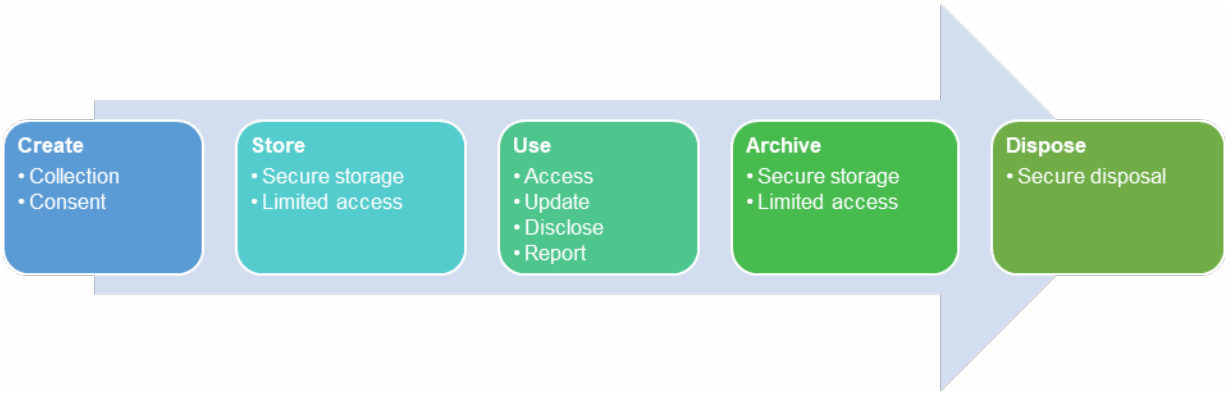
Confidentiality and privacy are of Perfect Care Pty Ltd primary significance.

Perfect Care Pty Ltd protects the privacy of everyone, including the privacy of their participants and employees. All persons (or their legal agents) are entitled to decide who has access to their private data.

Perfect Care Pty Ltd collects, uses and discloses data in accordance with appropriate state/territory laws and Federal Privacy Act.
Perfect Care Pty Ltd promotes and supports privacy and confidentiality procedures through its documents and information management procedures (see Records and Information Management Policy and Procedure).

Perfect Care Pty Ltd 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.

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



All employees are liable for preserving [Clients], other employees and [Organization's] privacy and confidentiality

1.5. Procedures

General

The Director is accountable for ensuring that Perfect Care Pty Ltd 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:
• Why and how Perfect Care Pty Ltd collects, uses and discloses personal data;
• What information Perfect Care Pty Ltd gathers about individuals and their source;
• Who has access to data;
• Collection, storage, access, use, disclosure and disposal of data;
• How people can consent to the collection, withdrawal or alteration of private data;
• Their approval and modification of data retained by Perfect Care Pty Ltd;
• How Perfect Care Pty Ltd safeguards and manages private data, including how it handles privacy queries and complaints; and
• How it manages data that needs to be updated, demolished or deleted.

These procedures are frequently reviewed by the Services Manager through annual Privacy Audits (See Perfect Care Pty Ltd Privacy Audit Form and Schedule)

All employees are accountable for 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 participants, 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.

Under the Human Resources Policy and Procedure of Perfect Care Pty Ltd, all employees must undergo Induction, which involves instruction in privacy, confidentiality and management of data. Workers ' understanding and implementation of procedures to manage confidentiality, privacy and data is tracked on a daily basis and through annual performance reviews. Workers will receive additional formal and on - the-job training where necessary.

Perfect Care Pty Ltd Privacy Statement must be prominently exhibited in the premises of Perfect Care Pty Ltd and included in the Client Handbook of Perfect Care Pty Ltd.

It is necessary to provide a complete copy of this policy and procedure upon request.

Photos and Videos

Photos, videos and other recordings are a form of personal information. Workers 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 Perfect Care Pty Ltd 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; and
- Fulfil government non-identification and statistical data demands. Personal participant data that Perfect Care Pty Ltd collects involves but is not restricted to:
- Clients and their parents and guardians contact details.
- Emergency contact details and individuals authorized to collect participants.
- 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 participants or their agents, employees must clarify:
• That Perfect Care Pty Ltd 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.

Participants and their relatives must receive a Privacy Statement from Perfect Care Pty Ltd and notify them that a copy of this policy and procedure is accessible on request.

Workers 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]. Workers 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, workers must use a Consent Form to:
• Confirm and explain the above-mentioned data; and
• Obtain permission from participants 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***

Perfect Care Pty Ltd 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 participants at any moment for an interview or for their participant 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 the Services Manager. Their choice will be respected and recorded in their Client file by Perfect Care Pty Ltd. Perfect Care Pty Ltd shall notify its Approved Quality Auditor of participants who have refused to participate in the audit upon commencement of any audit process.

Workers Information Collection and Consent

Personal worker’s information that Perfect Care Pty Ltd 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 Perfect Care Pty Ltd safely stores and protects private data to employees and clients, see the Records and Information Management Policy and Procedure.

Access

Personal information of the worker must only be accessed by the Services Manager, who can access the data only if it is necessary to fulfil their responsibilities.
Workers only have to access the private data of Clients if it is necessary to carry out their responsibilities.

Workers and Clients have the right to:
• Request access to private data Perfect Care Pty Ltd 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 Services Manager 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 Perfect Care Pty Ltd or any other individual.
• It may be the topic of investigations.

Any applications for Client access or correction denied by the Services Manager must be approved and recorded in the Client's file.
Any employees who are denied access or correction demands must be endorsed by the Director and recorded in the file of the worker member.

Disclosure

Personal data of the client or employee may only be revealed:
• For emergency medical therapy;
• To external organizations with the permission of the 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 Services Manager before disclosing the data.

International Disclosure

Under the Privacy Act 1988, Perfect Care Pty Ltd 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 Services Manager 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.

Reporting

Notifiable Data Breaches Scheme

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; and
• 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 Perfect Care Pty Ltd.

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 Perfect Care Pty Ltd 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
• Perfect Care Pty Ltd 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 Services Manager, who will determine the reaction of Perfect Care Pty Ltd and whether the violation must be recorded under the NDB Scheme.

If Perfect Care Pty Ltd 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 Services Manager 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 Services Manager considers the data breach to be notifiable under the NDB Scheme, they must notify the Data Breach Response Team of Perfect Care Pty Ltd.
• Services Manager as Team Leader, accountable for guiding the reaction team and reporting to the Director;
• Director as Project Manager, coordinating the team and supporting its participants;
• Director to introduce privacy knowledge to the team;
• Director as legal assistance, identifying legal commitments and providing guidance;
• Director as support for risk leadership, assessing danger from infringement;
• Director as support for information and communication technology (ICT) or forensics, helping to define the cause and effect of infringement involving ICT technologies;
• Director 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;
• Director supporting human resources where the infringement was caused by the worker's actions; and
• Director 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 of [Organization] and registered in the Incident Register of Perfect Care Pty Ltd, 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:

• Step 1: contain data infringement;
• Step 2: assess information breach and related hazards;
• Step 3: notify people and the Australian Information Commissioner; and
• Step 4: Prevent future infringements.

See Perfect Care Pty Ltd'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 Services Manager 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 Perfect Care Pty Ltd;
• The police or other law enforcement agencies;
• The Australian Securities and Investment Commission (ASIC);
• Australian Prudential Regulation Authority (APRA)
• Australian Tax Office (ATO);
• Australian Reporting and Analysis Center (AUSTRAC);
• Australian Cyber Security Center (ACSC);
• Australian Digital Health Agency (ADHA);
• Government Departments of the Federal, State or Territory;
• Professional and regulatory associations; and
• providers of insurance.

Victorian Protective Data Security Standards

• establish an initial cybersecurity baseline, consider implementing the Australian reporting arrangements.
You can find more details at: https:/www.asd.gov.au/publications/protect/eight-explained.htm;
• Assess the compliance of Perfect Care Pty Ltd with the Essential Eight and correct any recognized gaps;

• subscribe to the' Stay Smart Online ' website at: https:/www.staysmartonline.gov.au. This website offers guidance on intelligent internet behaviour and how to react to internet threats; and
• Assess Perfect Care Pty Ltd against Question 13 of the Organization Compliance Checklist (protective information safety) of the Department of Health and Human Services. On http:/fac.dhhs.vic.gov.au/organization-compliance-checklist you can find the checklist.

Archiving and Disposal

Refer to the Records and Information Management Policy and Procedure for details on how Perfect Care Pty Ltd archives and disposes of Clients' personal information.

1.6. Supporting Documents

Documents relevant to this policy and procedure include:
- Consent Form
- Records and Information Management Policy and Procedure
- Perfect Care Pty Ltd Information Sharing Guidelines [It is a South Australian Government requirement that businesses have an Information Sharing Guidelines (ISG) Appendix, based on the state government's ISG.]
- Data Breach Response Plan
- Continuous Improvement Register
- Client Handbook
- Privacy Statement
- Privacy Audit Form

Policy review

Perfect Care Pty Ltd may make changes to this policy and procedures from time to time to improve the effectiveness of its operation. Generally, this entire policy will be reviewed in consultation with people using the service, their families and carers and workers annually. All service planning, delivery and evaluation activities will include workers, client and other stakeholders and their feedback. Perfect Care Pty Ltd's annual service delivery and satisfaction surveys will include questions regarding:

- Satisfaction with Perfect Care Pty Ltd's privacy and confidentiality processes;
- Whether stakeholders have received adequate information about privacy and confidentiality; and
- The extent to which clients and their supporters feel their privacy and confidentiality has been protected.

Perfect Care Pty Ltd's Continuous Improvement Plan will be used to record and monitor progress of any improvements identified and where relevant feed into Perfect Care Pty Ltd's service planning and delivery processes.

By signing this document, I acknowledge that I have read and understand the Privacy and confidentiality Policy and Procedure. I need to comply with this policy and procedure and that Perfect Care Pty Ltd can change or update the policy at any time.

Signed: _____

Version	Endorsed	Endorsee	Reason/Section Update	Next Review
1.0		<Manager's Name>	Initial Release	